LANDesk® Management Suite 9.0

User's Guide

LANDesk®
An Avocent® Company

LANDesk and Avocent do not warrant that this document is error free and each retains the right to make changes to this document or related product specifications and descriptions at any time without notice. LANDesk and Avocent do not assume any obligation to update the information contained herein. This document is provided “AS IS” and without any guaranty, warranty, or license, express or implied, including but not limited to: fitness for a particular purpose, merchantability, non infringement of intellectual property, or other rights of any third party. Any LANDesk or Avocent products referenced in this document are not intended for use in medical, life saving, or life sustaining applications. Third parties may have intellectual property rights relevant to this document and the technologies discussed herein.

Contents

Introduction to LANDesk® Management Suite 9

LANDesk® Management Suite consists of tools you can use to help manage your Windows, Macintosh, Linux, and UNIX devices. Use these tools to distribute software packages, monitor software usage, deploy OS images and migrate profiles, remote control devices, detect and remediate security risks, and complete many other management tasks.

In this chapter, you'll learn more about Management Suite 9, including:

- What you can do with Management Suite 9
- Where to go for more information

What you can do with Management Suite 9

With Management Suite 9, you can:

- Use the LANDesk® Management Suite console to configure and manage your network. See Using the LANDesk® Management Suite console.
- Create and manage queries on inventory data and LDAP directories. See Using queries.
- Manage inventories, track inventory changes, create forms to gather custom data from devices, and view detailed reports. See Managing inventory and Using reports.
- Diagnose and troubleshoot problems on remote devices from the console. You can remote control, reboot, execute files, and transfer files to devices. See Administering remotely.
- Quickly distribute software to all of your network users. See Using software distribution.
- Use a Web-based console to access key Management Suite features from anywhere you have a browser. See Using the Web console.
- Monitor software licenses and compliance, and track software usage trends. See Using software license monitoring.
- Deploy OS images and migrate user profiles. See Using OS deployment and Using profile migration.
- Create application policies based on core database queries. Devices targeted by policies automatically receive application sets. See Using policy-based distributions.
- Use the Patch and Compliance tool to download the latest security content (definitions and patches) and create security scans, compliance scans, and remediation tasks. You can configure security scanner behavior and end-user interactive options with customized settings, and even create your own custom security definitions to scan devices for specific potentially threatening conditions. See "Patch and Compliance" on page 296.
- Protect your managed devices from other harmful security risks with a wide-ranging set of security tools, including: LANDesk Antivirus, HIPS, Firewall, Device Control, Security Activity, 802.1X NAC support, and more. See Introduction to 9.

Where to go for more information

The LANDesk User Community at http://community.landesk.com has user forums and best known methods for using many Management Suite features. Also, the community Web site is your main resource for Management Suite installation and deployment information, such as:

- Finding out system requirements
- Installing Management Suite
- Activating the core server
- Upgrading from previous versions of Management Suite
- Installing LANDesk add-on products

Using the console

LANDesk Management Suite provides a full range of system management tools that let you view, configure, manage, and protect devices on your network. All of these tasks can be performed via a single console. This chapter introduces the console interface and describes how to configure and navigate the console's network view and tool windows.

Read this chapter to learn about:

Console overview

The power of the console is that you can perform all critical network management functions from one convenient location, freeing you from the need to go to each managed device to perform routine maintenance or to troubleshoot problems. From a single console, you can distribute and update software or configuration settings, diagnose hardware and software issues, deploy OS images and migrate user profiles, use role-based administration to control user access to both features and devices, use remote control features to train end users or resolve problems, and more.

You can have multiple core servers and databases to accommodate your specific network management needs. For information on installing a core server and console, additional consoles, Web console, and managing multiple core servers and databases, refer to the *Installation and Deployment Guide* (this guide is available as a printable PDF document).

This chapter describes how to navigate and use the console to view and organize devices; and how to access the various management tools. (Each tool, such as software distribution and remote control, are described in-depth in their own separate chapters in this guide.)

Console wizards

Wizards are available for several areas of LANDesk Management Suite. Most wizards automatically increment based upon the user following the steps outlined by the wizard.

Getting started wizard

The Getting Started wizard helps the user configure LANDesk Management Suite to perform the following functions:

- Schedule tasks on your managed devices
- Manage Intel® vPro and IPMI devices
- Remote control managed devices
- View domain users in the Web Console

You can choose to work through the wizard, or click to place a checkmark in the **Don't show this wizard again** checkbox to prevent the wizard from being shown.

Discovering and installing agents

The Discovering and Installing Agents wizard helps the user configure LANDesk Management Suite to perform the following functions:

- Discovery: Looks for devices on the network that are unknown to the LANDesk Management Suite. IP address ranges can be specified to scan on the network.
- Deploying an agent: Installs the LANDesk Management agent on devices to be managed.

Security updates

The Download Patch Updates wizard assists the user in downloading and managing security and patch vulnerability definition files from the LANDesk content servers. The wizard helps in configuring tasks to download updates, starting the task, and scheduling future downloads.

Creating roles and groups

The Creating Roles and Groups wizard assists you in performing the steps necessary to manage who can access devices on the network and what tools or specific features can be used on those devices. It takes you through the process of creating a scope, a role, and a user group permission.

Starting the console

To start the console

1. Click **Start** > **Programs** > **LANDesk | Management Suite**. (The actual program name may be different depending on the LANDesk product that's installed and the license used to activate your core server.)
2. Enter a valid user name and password.

   If you're connecting to a remote core server, follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).
3. Select the core server you want to connect to. The user must have proper authentication credentials to that core server.
4. Click **OK**.

The console opens with the layout (size, position, open tool windows, etc.) that was being used the last time this user logged out.

For additional consoles, the credentials you use to log into Management Suite must match the credentials used for any drives you have mapped to the core server. Otherwise, you might see a "Multiple connections" error in the console login dialog.

About the Login dialog

Use this dialog to launch the console and connect to a core server.

- **Username:** Identifies a LANDesk user. This might be an administrator user or some other type of user with restricted access (see "Role-based administration" on page 44). The user must be a member of one of the LANDesk groups on the core server. Follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).
- **Password:** The user's password. (**Note:** If a LANDesk Administrator changes the password of another user, for example an additional console user, the new password does not take effect until that user reboots their console. At that point, the user would enter their new password to log into the console.)
- **Authentication source:** The source that the core should use to authenticate the credentials you provide. This source can either be a local group on the core server (Windows Local) or an active directory.
- **Core server:** Specifies the core server you want to connect to. This drop-down list is the same as the core server drop-down list available on the console toolbar.

Changing the core server connection

The console lets you view and manage the contents of any database associated with a core server that you can connect to on your network. This allows you to create databases for different sites, organizational units, or logical internal networks.

You can only be connected to one core server at a time.

To change core server connections

1. Select a core server from the **Core** drop-down list located on the console toolbar. Or, enter a core server name in the **Core** text box and press **Enter**.

   The server is searched for on your network. If found, you're prompted to log in at the standard Login dialog.

2. Enter a valid user name and password.

Follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name.

Once you've connected to a core server, its name is automatically added to the **Core** drop-down list in the toolbar.

You can also quickly log in as another user to the current core by clicking the **Core** drop-down list and without changing the core name, pressing Enter.

Understanding the network view

The network view is the main window of the console and is the starting point for most administrative tasks. This is where you view device's inventory data, create queries to search for and group devices, select devices to remote control, and so on.

The network view window is always open and contains two panes. The left-hand pane shows a hierarchical tree view of the core server\database you're currently connected to and its **Devices**, **Queries**, and **Configuration** groups. You can expand or collapse the tree objects as needed. The right-hand pane in the network view displays a detailed list of the selected group's items.

You can resize the network view window and its panes and columns, but you can't close it. The network view window is not dockable like the tools windows.

Role-based administration
The devices you can view and manage in the network view, and the management tools you can use, are determined by the access rights and device scope assigned to you by the administrator. For more information, see "Role-based administration" on page 44.

The **Network View** contains the following groups and subgroups:

Core

The **Core** object identifies the core server you're currently connected to. The **Core** object is located directly under the network view root and can be collapsed and expanded.

Core object name syntax

The syntax for the core object name is:

Server Name\Database Instance

Devices

The **Devices** group contains the following device subgroups.

- **My devices:** Lists devices for the currently logged-in user, based on the user's scope. A user can create device subgroups only under **My devices**. Users can add devices to their **My devices** group, or any of its subgroups, by copying them from the **Public devices** and **All devices** groups. Users can also click and drag devices from **Public devices** and **All devices** into their **My devices** group.

Dragging and dropping items in the network view
When you click an item in order to drag it to another group in the network view, the cursor indicates where you can and can't drop the item. As you move the cursor over a group object, a plus-sign (+) indicates that you can add the item to that group; and a cross-out sign indicates that you can't add the item to that group.

- **Public devices:** Lists devices an administrator (a user with the LANDesk Administrator right) has added from the **All devices** group. An administrator sees all of the devices in this group, while other users see only the devices allowed by their scope. Also, only an administrator can create a subgroup under **Public devices**.
- **All devices:** Lists all devices that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). For an administrator, **All devices** lists all managed devices that have been scanned into the core database. Devices configured with the standard LANDesk agent automatically appear in the **All devices** group when they are scanned into the core database by the inventory scanner.

For regular users, All Devices is a composite of their user's **My devices** and **Public devices** groups.

Administrators and users can run asset reports on the devices in this group.

You can also manually add computers to the network view by right-clicking the **All devices** group, selecting, clicking **Insert new computer**, filling in the device and network information, and clicking **OK**. These computers also appear in the User added computers subgroup under the Configuration group.

Virtual OS Hosts

The Virtual OS Hosts group shows managed devices, which are virtual hosts stored in the database. The Virtual OS Hosts group contains the following configuration groups:

- **My virtual OS hosts:** Lists virtual OS hosts for the currently logged-in user, based on the user’s scope. A user can create device subgroups only under My virtual OS hosts. Users can add devices to their My virtual OS hosts group, or any of its subgroups, by copying and pasting them from the Public virtual OS hosts and All virtual OS hosts groups. Users can also click and drag virtual OS hosts from public virtual OS hosts and All virtual OS hosts into their My virtual OS hosts group.
- **Public virtual OS hosts:** Lists devices a Management Suite administrator has added from the All virtual OS hosts group. Users with the LANDesk administrator right see all of the devices in this group, while other Console users see only the devices allowed by their scope. Only an administrator can create a subgroup under Public virtual OS hosts.
- **All virtual OS hosts:** Lists all virtual OS hosts that can be seen by the currently logged-in user, based on the user’s scope, in a flat list (no subgroups). For an administrator, All virtual OS hosts lists all managed virtual OS hosts that have been scanned into the database. Virtual OS hosts configured with the Standard LANDesk Agent automatically appear in the All virtual OS hosts group/folder when they are scanned into the database by the inventory scanner.

Queries

The **Queries** group contains the following query subgroups.

- **My queries:** Lists queries either created by the currently logged-in user, or added to the user's **User queries** group by an administrator. A user can create, modify and delete query groups and queries under their **My queries** group. They can also copy queries to this group from the **Public queries** group.

Any query a user runs is limited to the range of devices defined by the user's scope. For example, if a user's scope is **All machines**, the query will search all devices in the core database, but if the user's scope is restricted to 20 machines, only those 20 machines will be searched by the query. For more information on creating queries, see "Creating database queries" on page 105.

- **Public queries:** Lists queries that an administrator, or a user with the Public Query Management (PQM) right, has added. Only users with the LANDesk Administrator right or the PQM right can add, modify, or delete query groups or queries in the **Public queries** group. However, all users can see the queries in this group, and can copy them to their own **My queries** group.
- **All queries:** Lists all queries that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). **All queries** is a composite of the user's **My queries** and **Public queries** groups.

Administrators can use this group to run a user's queries against that user's scope, as if they were that user. In this way, an administrator can preview exactly the results a user will see when they run a query.

Configuration

The **Configuration** group contains the following configuration groups.

- **PXE holding queue:** Lists PXE holding queues and the devices that are waiting in the PXE holding queue. For more information, see "Using the PXE holding queue" on page 215.
- **Bare Metal Server:** Lists bare metal devices that have been created for provisioning tasks.
- **PXE Provisioning (Windows PE):** Lists devices targeted for Microsoft Windows PE provisioning tasks.
- **PXE Provisioning (Linux PE):** Lists devices targeted for Linux PE provisioning tasks.
- **Multicast domain representatives:** Lists configured multicast domain representatives that can be used for software distribution load balancing. For more information, see "Using Targeted Multicast with software distribution" on page 159.
- **PXE representatives:** Lists devices configured as PXE representatives that can deploy OS images to devices in their subnet. For more information, see "Using PXE representatives" on page 211.
- **Pending unmanaged client deployments:** Lists devices that have been discovered by the Unmanaged Device Discovery tool, and are waiting for an agent configuration task. For more information, see "Unmanaged device discovery" on page 191.
- **User added computers:** (Administrator only) Lists computers that have been added manually to the network view via the Insert new computer dialog (right-click the **All devices** group).

Fast Find

The Fast Find feature appears in a toolbar wherever it makes sense for the user to search for a specific item in a corresponding list. For example, any time a list of items is displayed in either the upper or lower portion of the console, the Fast Find field accompanies that view to facilitate locating a specific item in the corresponding list.

An example of when this can be helpful is if an organization has 10,000 nodes listed in the database. A user calls for assistance, and the helpdesk team member needs to find the device in the console. The helpdesk member can ask for the caller’s login name, or machine name, or any other user and device specific information, and (as long as the view includes the column with the specific information) the Fast Find can find the exact entry among the 10,000 entries in a second or two.

Creating groups

Groups help you organize devices and queries in the console's network view. You can create groups to organize network devices based on function, geographic location, department, device attribute or any other category that meets your needs. For example, you could create a marketing group for all devices in the marketing department or a group that includes all devices running a specific OS.

Rules for creating groups

- **My devices and My queries:** Administrators and all other users can create groups under **My devices** and **My queries**.
- **Public devices:** Only administrators can create groups under **Public devices**.
- **Public queries:** Only administrators or users with the "Public query m Management" right can create groups under **Public queries**.
- **All devices and All queries:** There are no subgroups in **All devices** or **All queries**. Users, including administrators, cannot create groups under **All devices** or **All queries**.

To create a group

1. In the console's network view, right-click the parent group (such as **My devices**), and then click **New group**. Or, select the parent group, and then click **Edit** > **My Devices** > **New Group**.
2. Type in a name for the new group, and then press the **Enter** key.

You can right-click groups to perform various tasks, based on the type of group. For example, if you created a device subgroup, its shortcut menu lets you:

- Add devices
- Create a new subgroup
- View as a report
- Cut
- Copy
- Paste
- Delete
- Rename

For more information on right-click features, see "Shortcut menus" on page 19.

Device icons

Device icons display in the console's network view and show the current agent and health status of a device.

You can update the agent and health status for devices one at a time as you select them in the network view, or for all of the visible devices in the network view at the same time. You can also update a device's status by selecting it and clicking the Refresh toolbar button. For information on configuring how agent discovery is handled, see "Configuring agent discovery" on page 26.

Icon display quality
These are high-color icons and require at least a 16-bit color-depth setting. If the icons in your console appear out of focus, change your color settings in the Windows Display Properties.

If your firewall blocks UDP packets
If you manage devices through a firewall that blocks UDP packets, you won't be able to use these device shortcut menu features: **Wake Up**, **Shut Down**, **Reboot**, and **Inventory Scan**.

Viewing managed devices in the All Devices group

Devices running LANDesk agents automatically appear in the **All devices** group when they are scanned into the core database by the inventory scanner. Typically, this scan takes place for the first time during a device's initial agent configuration. Once a device is scanned into the core database it is considered to be a managed device. In other words, it can now be managed by that core server. For more information on setting up devices, see "Configuring device agents" on page 75.

Because the **All devices** group is populated automatically, via an inventory scan, you may never need to manually discover devices. However, to discover devices not already in the core database, you can scan the network for devices with the unmanaged device discovery tool. For more information, see "Unmanaged device discovery" on page 191.

When connected to a particular core server, the administrator can see every device managed by that core server. Regular users, on the other hand, are restricted and can only see the devices that reside within their assigned scope (a scope is based on either a database query or a directory location). For more information, see "Role-based administration" on page 44.

Shortcut menus

Shortcut (context) menus have been significantly expanded for all items in the console, including groups, devices, queries, scheduled tasks, scripts, reports, and so on. Shortcut menus provide quick access to an item's common tasks and critical information.

To view an item's shortcut menu, select and right-click the item.

Available options in the shortcut menu
Options that appear in a device's shortcut menu, as well as options that are disabled or dimmed, may differ depending upon the device platform and upon which LANDesk agents are installed on the device.

For example, when you right-click a managed device in the network view, its shortcut menu will typically display the following options:

- **Inventory:** Displays all of the device's inventory data scanned in the core database.
- **Inventory history:** Displays inventory data changes for the attributes you've selected for tracking. You can print the inventory history or export it to a .CSV file.
- **Remote control:** Opens a remote control session with the device.
  - **Chat:** Opens a remote chat session with the device.
  - **File transfer:** Opens the file transfer dialog where you can transfer files to and from the device.
  - **Remote execute:** Lets you browse to and execute a batch file or application on the device.
- **Wake up:** Remotely wakes up a device whose BIOS supports Wake on LAN* technology.
- **Shut down:** Remotely shuts down the device.
- **Reboot:** Remotely reboots the device.
- **Inventory scan:** Runs an inventory scan on the device.
- **Scheduled tasks and policies:** Displays the device's current scheduled tasks and application management policies.
- **Add to new group:** Adds a copy of the device to a new user-defined group under the **My Devices** group. You're prompted to enter a name for the new group.
- **Add to existing group:** Lets you select the group where you want to add a copy of the device.
- **Group membership:** Displays all of the groups where the device is currently a member.
- **Run inventory report:** Opens the Reports dialog where you can select from a list of reports to run on the device. Double-click the report name to run it.
- **Update Agent Watcher settings:** Opens the Update Agent Watcher settings dialog where you can enable/disable real-time monitoring of specific LANDesk agents and services, choose an Agent Watcher settings or configure a new one, and specify a time interval to check for changes in the selected setting.
- **Security and patch information:** Opens the Security and patch information dialog that displays detailed vulnerability scan and remediation data for the device: including detected vulnerabilities and other security risks, installed patches, and repair history.
- **Security/compliance scan now:** Opens a dialog that lets you select a scan and repair settings, and then click **OK** to perform an immediate security scan on the device.
- **Antivirus scan now:** Opens a dialog that lets you select antivirus settings, and then click **OK** to perform an immediate antivirus scan on the device.
- **Manage local users and groups:** Opens the Local users and groups dialog that lets you remotely manage a Windows device's local users and groups.

- **Cut:** Removes items from a user-defined group. You can't cut items from the "All" groups.
- **Copy:** Creates a copy of the item that you can add to a another group.
- **Paste:** Places the item you've cut or copied into a user-defined group.
- **Remove:** Removes the item from a user-defined group.
- **Delete:** Deletes the item from the "All" group AND from any other group it's a member of at the time.
- **Properties:** Displays the device's inventory summary, device information, agent status, and remote control settings.

This guide does not cover every item type's possible shortcut menu. We recommend that you right-click any item to see the options that are available.

Configuring the network view with column sets

Column sets allow you to customize the inventory data that displays in the right pane of the network view, for both device lists and query results lists. Each column in a column set represents a unique attribute (or component) from the scanned inventory. For example, the default column set that displays in the network view is comprised of the Device Name, Type, and OS Name attributes.

Use the Column Set Configuration tool (**Tools > Administration > Column Set Configuration**) to create as many column sets as you like. Then, to apply a column set, drag the desired column set to device groups and query objects in the network view tree.

Column sets tool

The Column sets tool organizes column sets into three categories:

- **My column sets:** Column sets created by the currently logged-in user.
- **Public column sets:** Column sets created by an administrator, or predefined column sets.
- **All column sets** (only visible to an administrator): Column sets created by all LANDesk users.

A user can copy a column set from the Public Column Sets group into their own My Column Sets group and then modify the column set properties.

You can create subgroups under the **My column sets** object to further organize your column sets.

Creating column sets

The **Column configuration** dialog is where you create column sets. Each column represents a single inventory attribute or component that has been scanned into the core database. Columns appear from left to right in the network view in the order that they appear in the Columns list.

To create a column set

1. Click **Tools > Administration > Column Set Configuration**.
2. Select the **My column sets** object (or the **Public column sets** object), and then click the **Create a new column set** toolbar button.
3. In the **Column Configuration** dialog, enter a name for the new column set.
4. Select inventory attributes from the list and add them to the Columns list by clicking **Add to columns**. Remember to select attributes that will help you identify the devices in the device list or returned by the query.

5. (Optional) You can customize how and where the columns appear in the network view by directly editing a component's heading, alias, and sort order fields; or by removing or moving the selected component up or down in the list with the available buttons.
6. (Optional) You can specify more precise qualifying data for software components. Select the software component, click the **Qualify** button, and then select a primary key value from the list of available values. For more information, see "Using the qualify option with software components" on page 21.
7. Click **OK to save the column set.**

Restoring the original default columns
To restore the default columns in the network view, simply create a custom column set that includes the Device Name, Type, and OS Name attributes, and then apply it to device groups and query objects. Or, you can use the predefined column set named Original in the My column sets group.

Applying column sets to device groups and queries

Once you've created a column set, you can drag it to a devices group or subgroup, or to a specific query object in a queries group or subgroup. The device list, or query results list, displays the inventory data specified by the selected column set in the right pane of the network view.

Note that for device lists, once a column set is applied to a group it persists even when you select different device groups. However, for query results lists, the column set must be reapplied when changing between various queries.

You can also right-click a column set to access its shortcut menu and perform common tasks, as well as view and edit its properties. The shortcut menu includes the following options:

- Add to new group
- Add to existing group
- Group Membership
- Set as default
- View as
- Cut
- Copy
- Delete
- Rename
- Properties
- Info
- Export
- Copy to other core(s)
- Auto sync

Using the qualify option with software components

When creating column sets that include software components, you can specify a qualifier for those software components by choosing a specific primary key value. A software qualifier lets you more precisely identify the data you want a query to search for and display in that software component's column. For example, you can configure the column set to display version information for only one specific application by selecting that application's executable file name as the qualifier.

To specify a software component's qualifier, select the software component in the Columns list, click the **Qualify** button, and then select a value from the list of available primary key values.

As with the Alias field, once you select a primary key value and add it to the software component's Qualifier field, you can manually edit it by clicking in the field.

About the Column Configuration dialog

Use this dialog to create a new column configuration.

- **Name:** Identifies the column configuration.
- **Inventory attributes:** Lists each of the inventory objects and attributes scanned into the core database. Expand or collapse objects by clicking the box to the left of the object.
- **Add to columns:** Moves the selected inventory attribute into the columns list. If you select an entire inventory component, all of the inventory attributes contained in that component are added to the columns list.
- **Columns:** Lists the inventory attributes in the order they will appear, from left to right, in the network view.
- **Qualify:** Lets you specify a precise data qualifier for the selected software component. For more information, see "Using the qualify option with software components" on page 21.
- **Remove:** Removes the selected attribute from the list.
- **Move up:** Moves the selected attribute up one position.
- **Move down:** Moves the selected attribute down one position.
- **OK:** Saves the current column configuration and closes the dialog.
- **Cancel:** Closes the dialog without saving any of your changes.

Toolbar options

The console includes a toolbar that provides one-click access to common network view operations and some basic console configuration options. The toolbar buttons are dimmed when an item in the network view is selected that does not support that operation.

You can enable text descriptions for toolbar buttons by clicking **View > Show toolbar text**.

The console toolbar includes the following buttons:

- **Cut:** Removes items from the network view and stores them temporarily on the clipboard. If you accidentally cut an item, use the paste command to restore it. You must restore the deleted item before you perform any other command.
- **Copy:** Copies items from one location in the network view to another.
- **Paste:** Pastes items you've cut or copied.
- **Delete:** Permanently removes the item. You can't restore items you delete from the network view.
- **Refresh:** Updates the selected group or item in the network view. You can also collapse and expand a group to update its items. You can also click **View > Refresh** to update the currently selected item in the network view.
- **Refresh scope:** Updates the selected group or item in the network view, based on the currently logged-in user's scope (as defined in the Users tool). Scopes are updated when users log in or when a console user with administrative privileges clicks this button.
- **Layout:** Lists your saved window layouts. Select a layout from the drop-down list to restore the console to that layout configuration. If you want to save your current layout, click the **Save the current layout** button.
- **Core:** Lists core servers you have connected to before (which makes them appear in this list). You can select a core server from the list, or type the name of a core server

and press **Enter**. That core server is searched for on your network, and if found you're prompted to log in with a valid user name and password.

Using console tools

Tools are available through both the Tools menu and the Toolbox. To enable the **Toolbox**, click **View > Toolbox**.

A Management Suite administrator sees all of the tools in both the Tools menu and the **Toolbox**. Other Management Suite users will see only the tools (features that are allowed by their assigned rights). Tools dependent on rights that a user hasn't been granted don't appear at all in the Tools menu or in the **Toolbox** when that user is logged in to the console. For example, if a user doesn't have the "Power management" right, the Power management tool does not appear in either the **Tools** menu or the **Toolbox**.

When you click a tool name, the tool's window opens in the console. Tool windows can be resized, docked, floating, hidden, and closed. You can have multiple tool windows open at the same time, docked or floating. See the next section for more information on manipulating tool windows.

Dockable tool windows

Dockable windows is a console feature that lets you open as many of the tools as you want and move them in and out of the main console window.

Note: You can save console layouts you've designed and prefer for certain management tasks, and restore a saved layout whenever you need it. For more information, see "Saving window layouts" on page 24 later in this chapter.

When you open multiple tool windows, they're tabbed in a single window. The active tool window displays on top, with a tab for each open tool running along the side or bottom. Click a tab to display that tool window. You can dock the tabbed tools window or drag it so that it is floating outside of the console window.

Docking a tool window means attaching it to one of the edges of the console. The window is said to be in a docked state if it is currently attached to an edge of the console. You can also undock the tools window and have it free-floating outside of the console. You can dock windows horizontally or vertically in the console.

To dock a tool window

1. Click the window's title bar and drag the window to an edge of the console
2. When the docking rectangle (dim outline of the window appears indicating that the window will be docked), release the mouse button. The window attaches to that edge of the console.

Note that only tool windows (those windows accessible from the **Tools** menu or **Toolbox**) can exist as docked windows, floating windows, or tabbed windows. The network view window can be resized but can't be tabbed with other windows, floated outside the console, or closed.

If you minimize and then restore the main console window, then all docked and floating windows, including tabbed windows, are also minimized and restored with it.

Auto hide

The tool windows also support the auto hide feature. Auto hide is a push pin button in the upper right-hand corner of a window that lets you hold a window in place or hide it.

When the push pin is in (i.e., the pin points down), the window is pinned in place and auto hide is temporarily disabled. When the push pin is out (i.e., the pin points to the left) the window goes into auto hide mode when the cursor moves off of the window. Auto hide minimizes and docks the window along one of the edges of the console and displays a tab in its place.

The **Toolbox** also supports auto hide.

Saving window layouts

Layouts are saved console configurations, meaning the position and size of the network view, the **Toolbox**, and all open tool windows. You can use window layouts to save and restore customized console configurations that are especially useful for certain tasks or users.

To change the layout of the console, select a saved layout from the **Layout** drop-down list on the main toolbar.

To save your current layout

1. Configure the console interface the way you want it.
2. Click the **Disk** button next to the **Layout** drop-down list on the toolbar.
3. Enter a unique name for the layout.
4. Click **OK**.

About the Manage window layouts dialog

Use this dialog to manage saved window layouts and to reset the console window to the previous layout.

- **Saved layouts:** Lists all of your saved layouts.
- **Reset:** Returns the console window to the previous layout.
- **Delete:** Removes the selected layout.
- **Rename:** Lets you change the name of the selected layout.

Find bar

Find lets you search for items in a list containing a specific word or phrase. The **Find** bar is available in the network view and tool windows that contain flat lists of items. For example, the **Find** bar appears when you're viewing the:

- All Devices group
- All Queries group
- Pending Unmanaged Client Deployments group
- Unmanaged Device Discovery tool window

To search for an item with the Find bar

1. Select the **All devices** group. The **Find** bar appears at the top of the list.
2. In the **Find** text box, type any text you want to search for.
3. From the **In column** drop-down list, select the column you want to search
4. Click the **Search** toolbar button.

The resulting list displays only those items that matched your search criteria.

Status bar

The status bar at the bottom of the console displays the following information (from left to right):

- Number of selected items in a listing
- Current job name and status
- Name of the currently logged-in user
- Days until the core server will attempt to contact the licensing server

The status bar is always visible.

Viewing device properties

In the console's network view, you can quickly view information about a device by right-clicking the device in the device list and selecting **Properties**.

More detailed information about the device is available in its inventory data. You can view inventory data in the network view columns (which are configurable), or by right-clicking the device and selecting **Inventory** to open the full **Inventory** window.

About the Device properties dialog

Use this dialog to view useful information about the selected device. The dialog includes three tabs: **Inventory**, **Device**, and **Agents**. Click each one to view related information.

Inventory tab

The **Inventory** tab contains a summary of the device's inventory data. For more details, see "Viewing a summary inventory" on page 96.

Device tab

The **Device** tab contains basic information about a device, including its location and identity on the network. This tab also appears when you manually insert a device (from the **All devices** group's shortcut menu, click **Insert new computer**).

- **Device:**
  - **Name:** The name that appears in the core database and network view for the device.
    If you are manually inserting a device, you can make this a user-friendly name. If you enter nothing here, the default device name will be the Windows computer name.
  - **Type:** The type of device, such as Windows 2000 Server or XP Workstation.
- **Network:**
  - **IP Name:** The Windows computer name for the device.
  - **IP address:** The IP address assigned to the device.
  - **Physical address:** The physical address of the device.

Agents tab

The **Agents** tab contains information about the current status of agents and remote control settings for the device.

- **Common Base Agent status:** Indicates whether the standard LANDesk agent (Common Base Agent is loaded on the device.

- **Real-time inventory and monitoring status:** Indicates whether the real-time inventory and monitoring agent is loaded on the device.
- **Remote control agent status:** Indicates whether the remote control agent is loaded on the device. If this agent is not loaded on the device, remote control operations (such as file transfer and chat are not available.
- **Security type:** Indicates the remote control security model used for the device. Options include: Local template, Windows NT security/local template, and Certificate-based/local template.
- **Allow:** Shows the remote control operations that are allowed on the device. These operations were enabled by the device agent configuration.
- **Settings:** Indicates how remote control operates when you attempt to interact with the device.

Configuring agent discovery

Agent discovery is the process used to find managed devices that have the standard LANDesk agent or remote control agent installed. These two agents provide the following capability:

- **The standard LANDesk agent:** Enables the PDS (ping discovery service). If the standard LANDesk agent is installed on a device, you can schedule software distributions and device setup configurations.
- **Remote control:** Lets you remotely access and control a device.

Agent discovery uses TCP/IP to verify agents running on the devices.

IP addresses are used as search criteria in order to perform standard LANDesk agent discovery with TCP/IP. Management Suite looks for the standard LANDesk agent and remote control agent on devices within a specific range of IP addresses. This range of addresses is implied by the IP network address you supply.

If you don't designate subnet network addresses when searching on TCP/IP, discovery is performed only on the network segment where the console initiating the discovery resides. For example, if you've installed four consoles, each residing on a different network segment, you would have to initiate four scans, one from each of the four consoles.

On network segments where consoles don't exist, you MUST use subnet network addresses to access the information on that network segment.

Note on firewalls: If you have one or more firewalls on your network, agent discovery can't be used to search outside firewalls, because firewalls generally limit the flow of packet traffic to designated ports.

To configure agent discovery options

1. Click **Configure** > **Agent status options**.
2. Select whether you want agent discovery to update agent status for only the selected item in the network view, or all visible items in the network view.
3. Specify the agent status refresh rate.
4. Configure how you want to discover the remote control agent, and prioritize the address resolution methods.
5. Specify how long agent discovery will attempt to discover the remote control agent on the device before timing out.
6. Click **OK**.

About the Agent status options dialog

Use this dialog to configure the following agent discovery options.

- **Gather agent status:**

    - **For selected items only:** Specifies that a device's agent status is updated as the device is selected in the network view. This option generates the least amount of network traffic and is the default.
    - **For visible items in network view:** Specifies that all visible devices in the network view will have their agent status updated according to the refresh rate. As new devices become visible, their agent status (and health) are updated.
- **Agent and health status refreshes every < > minutes:** Indicates whether agent status is automatically updated. You can specify the refresh rate.
- **Communication method:** Indicates how the agent is discovered.
    - **IP address:** Uses the core database to retrieve the computer's stored IP address.
    - **Domain Name Service (DNS):** Resolves the computer's ID name with the DNS server when verifying the remote control agent. If you do not have a DNS server, clear this option.
    - **Move up and Move down:** Moves the selected method up or down in the Discover agent using list. Methods are tried in the order they appear in the list.
- **Timeout:** Sets the timeout value before the remote control agent discovery fails for each checked address resolution method.

Monitoring devices for network connectivity

Device monitoring lets you regularly monitor the connectivity of any of your managed devices.

Ping settings are specific to the device you've selected. When a device stops responding to a ping (when it goes offline), an alert notification is added to the log on the core server. If you want to be notified with another alert action, such as receiving an e-mail when a device goes offline, you can configure an alert in the core alert ruleset.

To monitor connectivity for managed devices

1. Click **Configure > Device monitoring**.
2. Click **Add**. Select one or more devices that you want to monitor, and then click **Add**.
3. Specify the **Ping frequency** setting, the number of retries, and the timeout limit.
4. Click **OK**.

About the Configure device monitoring dialog

Use this dialog to configure the following device monitoring options.

- **Monitor these devices:** Lists the devices that are currently being monitored.
- **Add:** Opens the **Add monitored devices** dialog where you can search for and select managed devices that you want to monitor.
- **Remove:** Deletes the selected device from the list.
- **Ping frequency:** Control when and how the ping operation occurs. These settings can be applied to each device individually.
    - **Ping every:** Schedules a periodic ping at the specified minute interval.
    - **Schedule daily at:** Schedules a daily ping at a specific time.
    - **Retries:** Specifies the number of ping retries.
    - **Timeout:** Specifies the number of seconds until ping retries will timeout.
- **OK:** Saves your changes and closes the dialog.
- **Cancel:** Closed the dialog without saving your changes.

Configuring device monitoring alerts

If you want device monitoring to notify you when managed devices come online or go offline, you have to first configure an alert ruleset that has additional actions (such as receiving an e-mail when the alert is sent).

To configure device monitoring alert settings

1. Click **Tools > Configuration > Alerting**.
2. In the **Alerts** tree, expand the **Alert rulesets** item.
3. Right-click **Core alert rulesets** and click **Edit**.
4. In the **Ruleset** window's **Alert ruleset** pane on the left, click **Alerts**.
5. In the **Alerts** pane, under the **Standard** folder, click **Device monitor**.
6. In the right pane, click **Rules > Add**.
7. Drag the **Device monitor system connectivity** alert to the **Alerts** well at the bottom of the page.
8. In the **Ruleset** window's **Alert ruleset** pane on the left, click **Actions** and drag any additional actions that you want down to the **Actions** well. By default the core alert log handler configuration is the action. You can choose to send an e-mail or an SNMP trap, or run an executable on the core when the alert is received. (You may need to define an action, such as specifying where to send e-mail alerts.)
9. In the **Ruleset** window's **Alert ruleset** pane on the left, click **Time** and drag **Always** down to the **Time** well.
10. Click the **OK** button next to the wells.
11. In the **Actions** pane on the right, click **Publish**.
12. In the **Alert ruleset** pane on the left, click **Rules summary** and double-click the rule you created.
13. In the dialog that appears, check the **Health** box if you want a device's health status in the console to change when it is online/offline, then click **OK** to close the dialog.
14. Click **Publish** to publish any changes you made in the dialog and close the **Ruleset** window.

Note: When you configure alert settings, they apply to all of the devices you're monitoring.

Management Suite port usage

When using Management Suite in an environment that includes firewalls (or routers that filter traffic), information on which ports need to be opened at the firewalls is crucial. The following table lists the ports used by the Management Suite components. This information focuses on required router and firewall configurations. Ports used only locally and ports used only to communicate with devices running legacy versions of Management Suite are not included.

Feature	TCP Ports	Inbound / Outbound
Alert management system	38292	In
Inventory	5007	in
Management Gateway using HTTPS	443 HTTPS	In/Out
Management Gateway using HTTP	80 HTTP 443 HTTPS	In Out
Management Web services	80 HTTP	In

Feature	TCP Ports	Inbound / Outbound
Remote control	9535, 9595	Out
Secure inventory/Web console	443 HTTPS	In
Software distribution (policy)	12175, 12176	In
Software distribution (push)	9594, 9595	Out
Software distribution (targeted multicasting)	33354	Out
LANDesk trusted access	4444, 7777	In
Avocent Management Platform (RBA, licensing, reporting)	8443, 8092	In/Out

The table summarizes the ports that need to be opened at the firewall in order to enable specific product features. Inbound and outbound are based on the assumption that the core server / console is inside the firewall, and the devices to be managed are outside the firewall. Inbound means that a service on the core server is listening at the indicated port and that devices will open connections to it. Outbound means that the device outside the firewall is listening at the indicated port and the core server (or console in the case of remote control) will open connections to it.

If certificate-based security is used for remote control, the TCP 9594 port needs to be enabled (core server to managed device and console to core server). When a computer is chosen in the Network View, a ping discovery is sent to the device on UDP port 9595. If the port is blocked, there will be no response and the remote control option will be grayed on the shortcut menu.

Setting up additional Management Suite consoles

The Management Suite console is automatically installed on the core server. This console should be installed on LANDesk administrator’s machines that need full functionality or access to all the Management Suite tools. The console is used to interact with the various Management Suite features; e.g., to distribute software, remotely control managed devices, view inventory information, and perform other management functions.

For additional utility and functionality, consoles can be installed throughout the network. (LANDesk Software doesn't charge extra for additional consoles.)

To install an additional console

1. From your Management Suite installation media, launch the autorun.
2. Click the **Remote console** button.
3. Click **Continue**.
4. If the prerequisite check passes, click **Continue**. Otherwise, fix the missing prerequisites.
5. Click **Run setup**.
6. Follow the installation prompts.

Supported console operating systems

The following is a list of supported console operating systems:

- Windows Vista Business/Ultimate/Enterprise SP1 (32-bit)
- Windows XP Professional SP1 or SP2 or SP3
- Windows Server 2003 (32-bit) with SP1 or SP2

- Windows Server 2003 R2 (32-bit) with or without SP2
- Windows Server 2008 R2

Console computer Requirements

The following is a list of console computer requirements:

- Supported Windows OS using NTFS
- Microsoft Internet Explorer 6.x SP1 or later
- Microsoft Data Access Components (MDAC) 2.8

Setting up the Web console

The Web console offers a subset of the Management Suite console functionality from the convenience of a Web browser. Once installed on a Web server, designated users can access the Web console through Microsoft Internet Explorer*, or other supported Web browsers. This setup (installed by default on the core server) allows Web console access to users without additional installation at their local PCs.

By default, Setup places the Web Console files in the \Inetpub\wwwroot\remote folder.

Setup also creates Web console file shares with the necessary permissions on the core server.

The Web console and managed devices require the following shares and permissions to work correctly:

- **ldmain:** Server applications (\Program Files\LANDesk\ManagementSuite). The Administrators group must have Full Control. For Microsoft Windows 2003, the Network Service group must have Read and Execute, List Folder Contents, and Read rights.
- **ldlog:** Logs (\Program Files\LANDesk\ManagementSuite\log).
- **ldlogon:** Managed device applications and agents (\Program Files\LANDesk\ManagementSuite\ldlogon). The Administrators group must have Full Control and the Everyone group must have Read Only rights.
- **scripts:** Software distribution scripts (\Program Files\LANDesk\ManagementSuite\Scripts).

If the Web console is being installed on a server other than the core server, the logged-in user must be a domain administrator, and the domain administrator account must be in one of the Core Server's LANDesk user groups. The core server and Web console servers must be in the same domain, and any users needing to use the Web console must be added to one of the LANDesk user groups on both the core server and Web console servers.

The Management Suite 9 Web console can't be run on an older core server or console. Only the Management Suite 9 Web console can be run on a Management Suite 9 Core server or console computer.

Earlier versions of Management Suite will not work.

If the Web console is being installed on a Microsoft Windows 2003 server, Internet Information Server (IIS) disables active server pages by default. They must be enabled for the Web console to work correctly.

To enable active server pages on Microsoft Windows 2003 servers

1. Click **Start|Administrative Tools|Internet Information Services (IIS) Manager**.
2. Click to expand <CoreServerName>.
3. Click **Web Service Extension**.
4. Click **Active Server Pages**.
5. Click **Allow**.

6. Close the Internet Information Services (IIS) Manager window.

In order to verify the installation of the Web Console, a Web browser can be opened and the Web server URL can be entered. By default, the URL is:

- http://<WebServerName>/remote

The installation was successful if the browser prompts for login credentials and opens the Console.

The first time the Console is launched, it may take up to 90 seconds to display. This delay happens because the server has to do a one-time compile of Console codes. The Console launches much faster after the first time.

If a permission denied error occurs when the Web Console is being accessed, Integrated Microsoft Windows authentication must be enabled as the authentication method for the Web Console's site.

How to verify the authentication method

1. Click **Start|Administrative Tools|Internet Information Services (IIS) Manager**.
2. Click to expand **<CoreServerName>|Web Sites| Default Web Site**.
3. Click **Properties** from the **Remote** folder's drop-down menu.
4. Click the **Directory Security** tab.
5. Click **Edit** in the **Anonymous access and authentication control** field.
6. Clear the **Enable Anonymous Access** checkbox.
7. Check the **Integrated Windows authentication** checkbox.
8. Click **OK** to exit the **Authentication Methods** window.
9. Click **OK** to exit the **Remote Properties** window.
10. Close the Internet Information Services (IIS) Manager window.

Console and Web console functionality comparison

The following table lists the capabilities of the Management Suite console and the Management Suite Web console.

Capability	Console	Web Console	Notes
Agent Configuration	Yes	Minimal	Scheduled Agent Deployments and Update tasks are visible and controllable by Web Console users with rights to Agent Configuration.
Alerting	Yes	No	
Antivirus	Yes	No	
Column Set Configuration	Yes	Yes	In the Web Console access under Preferences on the Custom Columns tab.
Configure Services	Yes	No	Vastly different behavior: Inventory Service, Scheduler Service, Management Gateway, PXE behavior, OSD validation, and many other features must be configured in the Console.
However, licensing status can be viewed in either.			

Capability	Console	Web Console	Notes
Connection Control Manager	Yes	Minimal	Scheduled deployments are visible and controllable by Web Console users with rights to CCM.
Custom Data Forms	Yes	No	
Delivery Methods	Yes	Yes	Tab located under Distribution in Web Console.
Device right-click	Yes	Yes	Vastly different behavior – the only overlapping function is to run an inventory scan (on Web “Scan Device”).
Directory Manager	Yes	Yes	
Display Manager	Yes	No	
Distribution Packages	Yes	Yes	
Host Intrusion Prevention	Yes	No	
LaunchPad Link Manager	Yes	Minimal	Scheduled LaunchPad Link Deployments are visible and controllable by Web Console users with rights to Software Distribution.
Logs	Yes	No	
Manage Scripts	Yes	Partial	From Scripts, existing scripts can be scheduled and grouped.
OS Deployment	Yes	Minimal	Existing OS Deployment scripts that have already been scheduled can be viewed and controlled by Web Console users with rights to OSD via Scripts > OSD Scripts.
Power Management	Yes	Minimal	Scheduled power policy tasks are potentially visible and controllable by Web Console users.
Provisioning	Yes	No	
PXE Boot Menu	Yes	No	
QueCapability	Yes	Partial	The Web Console allows use of a Count feature which is not in the Console. Queries cannot be viewed as reports in the Web Console.
Remote Control	Yes	Yes	
Reports	Yes	Yes	The reporting console launches in a separate browser window.
Scheduled Tasks	Yes	Yes	
Scopes	Yes	Partial	Existing Scopes can be added to a User, but new Scopes cannot be created.
Security and Patch Manager	Yes	Minimal	Scheduled scans and repair tasks are visible and controllable by Web Console users with Patch Manager rights.
Software License Monitoring	Yes	Partial	In the Web Console product usage data is not visible, individual product and group compliance reports are not available and you cannot ignore or group products.
Thin Client Configuration	Yes	No	

Capability	Console	Web Console	Notes
Unmanaged Device Discovery	Yes	Minimal	Scheduled Unmanaged Device Discovery Scans are visible and controllable by Web Console users with rights to UDD.
Users	Yes	No	
Windows CE Agent Configuration	Yes	No	
Windows CE CAB Creator	Yes	No	

Running CoreDbUtil to reset, rebuild, or update a database

The CoreDbUtil.exe utility, in the core server's \Program Files\LANDesk\ManagementSuite folder, creates all the tables, indexes, and constraints needed to use the core database. Before running CoreDbUtil.exe, you must install your database correctly or the table creation may fail. CoreDbUtil.exe looks for registry keys on the core server to determine the core database connection information. CoreDbUtil doesn't work on core rollup databases.

Use CoreDbUtil to:

- **Reset database:** Drops all tables, and rebuilds the database from scratch using DATAMART.XML. Rebuilds Vulnerability scanning database tables. **Warning:** all existing data will be lost.
- **Build components:** Updates the schema (specifically to include column additions) in an existing core database from metadata.xml. This isn't destructive to existing data.
- **Publish app list:** Publishes the software configuration list using defaults.xml and ldappl3.template to generate ldappl3.ini, ldappl3.bak, ldappl3.ldz, ldappl3.pat, ldappl3.paz, and ldappl3.reset.
- **Update Display Names:** Updates the Display Name field in an existing core database for all devices in that database. This isn't destructive to other existing data.

To run CoreDbUtil

1. On the core server, run CoreDbUtil.exe
2. After CoreDbUtil connects to the database, select the option you want.
3. Wait until the **Status** is finished. Depending on the database size and the task you chose, this could take a few minutes or several hours.

If you reset the database, some patch management and LANDesk NAC features won't work correctly until you do the following.

To update patch management database components after resetting a database

1. Launch CoreDbUtil as follows:

   ```
   CoreDbUtil.exe /xml=datamartpm.xml
   ```

2. Click **Build components**.

Choosing the core server and database hardware

When setting up a LANDesk Management Suite core server, decisions must be made on the speed, memory, and storage of the servers involved. The administrator must also decide when to move to multiple core servers. This section will cover these decisions. The four main hardware choices are the CPU, memory, storage, and network card selection. The lists that follow are recommendations on hardware for various numbers of managed nodes.

The biggest factor in making these decisions will be the number of managed nodes in the network. The number of nodes should have already been estimated during while gathering network information. However, other factors such as which components will be the most used, the number of people needing to access the LANDesk console or the Web console, network management model, and compliance with business practices and standards should be considered.

Hardware recommendations are different for each environment and the following are general guidelines to help determine what the desired hardware would be for a given environment.

When choosing the database software there are four choices:

- Microsoft SQL 2005
- Microsoft SQL 2008
- Oracle 10g
- Oracle 11g

All Management Suite services hosted on one server (up to 750 devices)

For Management Suite management domains with 1,000 devices or fewer, you can install the core server, console, Web console server, and the core database on one server. For these networks, you may want to consider using the default Microsoft MSDE database, which is generally easier to maintain. Your server should at least meet these system requirements before you install Management Suite in a 1,000 or less device configuration.

- Intel Xeon Dual Core 32-bit or 64-bit processor
- 4 GB of RAM
- 100/1000 Megabit network adapter
- 72 GB of free disk space on 10K RPM or faster drives or arrays

Important: Microsoft SQL Express 2005 has a 4 gigabyte limitation. If this limitation is reached, the core server will stop functioning properly and the database will no longer be able to write more data. It is possible that each agent could use as much as 2-4 megabyte or more so be careful to monitor the disk usage and upgrade to a full version of SQL prior to reaching the 4 gigabyte limit.

All Management Suite Services Hosted on One Server (750-1,500 Devices)

If your Management Suite management domain consists of 1,001-3,000 devices, you can still use one server. Your servers should at least meet the following system requirements before you install Management Suite.

- Intel Xeon Dual Core 32 bit or 64 bit processor
- 4 GB or more of RAM
- One gigabit network adapter
- 3 drives or arrays with 72 GB of free disk space per array on 15K RPM or faster drives

Note: A core server that is at 750 to 1,500 nodes and is running all LANDesk features may see some read/write slowness on drives if the operating system, the LANDesk management suite application, the database application, the database, and the database logs are all on the same drive or array. Tuning may be needed. The server hosting such a full-featured configuration is recommended to have three drive arrays on separate spindles (physical disks) to prevent resource issues. The following drive configuration should be implemented.

- One drive or array for the Operating System
- One drive or array for the LANDesk Management Suite application and the database application
- One drive or array for the database and database logs

Important: The server hosting this configuration requires three drive arrays on separate spindles (physical disks).

Single server configuration (1,500-3,000 devices)

If your Management Suite management domain consists of 1,500 – 3,000 devices, LANDesk recommends that you divide your Management Suite components between two servers for improved database performance. Your servers should at least meet the following system requirements before you install Management Suite.

Management Suite core server and Web console software on one server

- Dual (two physical processors) Intel Xeon Quad Core 64-bit processors
- 6-10 GB or more of RAM (4 GB for the OS and LANDesk services, plus 1 to 2 MB per node for the database. For RAM to spare, get 10 GB.)
- Important: The Management Suite core server in this configuration requires two drive arrays on separate spindles.
- One gigabit network adapter
- 3 drives or arrays with 72 GB of free disk space per array on 15K RPM or faster drives

Note: A core server that is at 1,500 to 3,000 nodes and is running all LANDesk features may see some read/write slowness on drives if the operating system, the LANDesk management suite application, the database application, the database, and the database logs are all on the same drive or array. Tuning may be needed. The server hosting such a full-featured configuration is recommended to have three drive arrays on separate spindles (physical disks) to prevent resource issues. The following drive configuration should be implemented.

- One array for the Operating System, Raid 0, 1, 5 or equivalent/faster technology
- Management Suite software should be installed to an array in RAID 0, 5, 10 or an equivalent/faster technology
- One array for the database and database logs, RAID 0, RAID 5, or RAID 10 or an equivalent/faster technology

Important: The server hosting this configuration requires three drive arrays on separate spindles (physical disks).

Multi-server configuration (3,000 – 5,000 devices)

If your Management Suite management domain consists of 3,000 – 5,000 devices, LANDesk recommends that you divide your Management Suite components between two servers for improved database performance. Your servers should at least meet the following system requirements before you install Management Suite.

Management Suite core server and Web console software on one server

- Dual (two physical processors) Intel Xeon Quad Core 32 bit or 64-bit processors
- 4 GB or more of RAM
- One gigabit network adapter (the core and database should have a gigabit connection to each other)
- Two arrays of 72 GB of free disk space per array on 15K RPM or faster drives
- The Operating System array should be RAID 0 or 1 or an equivalent / faster technology
- Management Suite software should be installed to an array in RAID 0, 5, or 10 or an equivalent / faster technology

Core database on a second server

- 64-bit Operating System is recommended for the database server for the memory management

Important: If using a 32-bit Windows Server Operating System with SQL 2000 Enterprise or SQL 2005, AWE (Addressing Windowing Extensions) must be enabled.

- Dual (two physical processors) Intel Xeon Quad Core 64-bit processors
- 4 GB to 10 GB or RAM (1 GB for the OS, plus 1 – 2 MB per node.)

Important: RAM requirement vary. Multiply the total devices this core server will be managing by 2 MB to get a better estimate. For example, 5,000 devices require 6-10GB of RAM.

- SQL 2005 or 2008 Enterprise, or Oracle 10g or 11g
- Three arrays of 72 GB of free disk space per array on 15K RPM or faster drives
- The Operating System array should be RAID 1 or an equivalent / faster technology
- One array for the database, RAID 0, RAID 5, RAID 10 or an equivalent / faster technology
- One array for the database logs, RAID 0,1, 5 or an equivalent / faster technology

Important: The database server in this configuration requires three drive arrays on separate spindles.

- One gigabit network adapter (the core and database should have a gigabit connection to each other)

Multi-server configuration (5,000-8,000 devices)

If your Management Suite management domain consists of 5,000-8,000 devices, LANDesk recommends that you divide your Management Suite components between two servers for improved database performance. Your servers should at least meet the following system requirements before you install Management Suite.

Management Suite core server and Web console software on one server

- Quad (four physical processors) Intel Xeon Quad Core 64-bit processors

Important: If using a 32-bit Windows Server Operating System with SQL 2000 Enterprise or SQL 2005, AWE (Addressing Windowing Extensions) must be enabled.

- 4 GB or more of RAM

Important: The Management Suite core server in this configuration requires two drive arrays on separate spindles.

- Two arrays of 72 GB of free disk space per array on 15K RPM or faster drives
- The Operating System array should be RAID 1 or an equivalent / faster technology
- Management Suite software should be installed to an array in RAID 0, 1, 5, or 10 or an equivalent / faster technology

- One gigabit network adapter (the core and database should have a gigabit connection to each other)

Core database on a second server

- 64bit Operating System is recommended for the database server for the memory management
- Dual (two physical processors) Intel Xeon Quad Core 64-bit processors
- 6 GB to 12 GB or RAM (1 GB for the OS, plus 1 – 2 MB per node.)

Important: RAM requirement vary. Multiply the total devices this core server will be managing by 2 MB to get a better estimate. For example, 8,000 devices require 9-16GB of RAM.

- SQL 2005 or 2008 Enterprise, or Oracle 10g or 11g
- Three arrays of 72 GB of free disk space per array on 15K RPM or faster drives
- The Operating System array should be RAID 1 or an equivalent / faster technology
- One array for the database, RAID 0, RAID 5, RAID 10 or an equivalent / faster technology
- One array for the database logs, RAID 0,1, 5 or an equivalent / faster technology

Important: The database server in this configuration requires three drive arrays on separate spindles.

- One gigabit network adapter (the core and database should have a gigabit connection to each other)

Multi-server configuration (8,000-12,000 devices)

If your Management Suite management domain consists of 8,000 or more devices, LANDesk recommends that you divide your Management Suite components between multiple servers for improved performance in all areas. Your servers should at least meet the following system requirements before you install Management Suite.

Management Suite core server and Web console software on one server

- Four physical processors, each dual-core or better
- 4 - 8 GB of RAM
- Two arrays of 72 GB of free disk space per array on 15K RPM or faster drives
- The Operating System array should be RAID 1 or an equivalent / faster technology
- Management Suite software should be installed to an array in RAID 0, 1, 5, or 10 or an equivalent / faster technology

Important: LANDesk performs a lot of write operations on the following folders under LDLogon: LDScan, VulscanResults, sdstatus, AlertQueue, etc. Mounting a drive as a folder such as LDlogon instead of a drive letter can improve disk I/O.

Important: The Management Suite core server in this configuration requires two drive arrays on separate spindles.

- The Operating System array should be RAID 1 or an equivalent / faster technology
- The application array should be on a second separate RAID array
- One gigabit network adapter (the core and database should have a gigabit connection to each other)

Core database on a second server

- 64bit Operating System is recommended for the database server for the memory management

Important: If using a 32-bit Windows Server Operating System with SQL 2000 Enterprise or SQL 2005, AWE (Addressing Windowing Extensions) must be enabled.

- Quad (four physical processors) Intel Xeon Quad Core 64 bit processors
- 12 to 24 GB or more of RAM minimum

Important: RAM requirement varies. Multiply the number of devices this core server will be managing by 1 to 2 MB to get a better estimate. For example, 16,000 devices require 17 to 24 GB of RAM.

- SQL 2005 or 2008 Enterprise, or Oracle 10g or 11g
- Three arrays of 72 GB of free disk space per array on 15K RPM or an equivalent / faster technology
- The Operating System array should be RAID 1 or an equivalent / faster technology
- One array for the database, RAID 0, RAID 5, or RAID 10 or an equivalent / faster technology
- One array for the database logs, RAID 0,1, or 5 or an equivalent / faster technology
- One gigabit network adapter (the core and database should have a gigabit connection to each other)

Off-core Web console server (optional)

In some organizations a large number of support individuals may be accessing the Web console. If the core server is already under a heavy load, the use of the Web console may be slowed significantly. This can be alleviated by installing an additional Web Console server.

- Intel Xeon processor or better (preferably a dual-core processor)
- 2-3 GB of RAM
- Gigabit Network adapter

Off-core inventory server (optional)

In some organizations a large number of inventory scans may be coming in and the core server may be under a heavy load with other LANDesk® features. In this instance it may be desired to off-load inventory scanning to an additional Inventory server. This feature is used less often now that the core server supports multiple inventory threads but still may be needed if the core server's processor is reaching maximum capability.

- Intel Xeon processor or better (preferably a dual-core processor)
- 2-3 GB of RAM
- Gigabit Network adapter

Multi-server configuration (16,000 or more devices)

Yes, with our new Enterprise core features LANDesk supports single core servers that exceed 16,000 nodes. For LANDesk Management Suite installations of this size and larger we recommend obtaining further tuning assistance from LANDesk Professional Services or a valued Expert Solutions Provider (ESP).

Installing LANDesk Management Suite

Before installing Management Suite, make sure the server you've chosen meets the system requirements described earlier in this section. The following steps install Management Suite with the default Microsoft SQL Express 2005 database. If you'll be using one of the other supported databases, you need to install and configure that database before running Management Suite setup. For detailed instructions on doing this and installing Management Suite, refer to the LANDesk User Community at http://support.landesk.com.

The Indexing Service and Windows Search Service must both be disabled prior to installation of LANDesk Management Suite 9.0; failure to disable these services could cause the installation to fail. See the following article for more information: http://community.landesk.com/support/docs/DOC-7245.

Because each environment has different needs, we recommended that you contact your reseller or Expert Solution Provider (ESP) about the Certified LANDesk® Deployment. If you are unsure who your reseller is, go to this site to find a LANDesk inside sales manager who can direct you to your reseller:

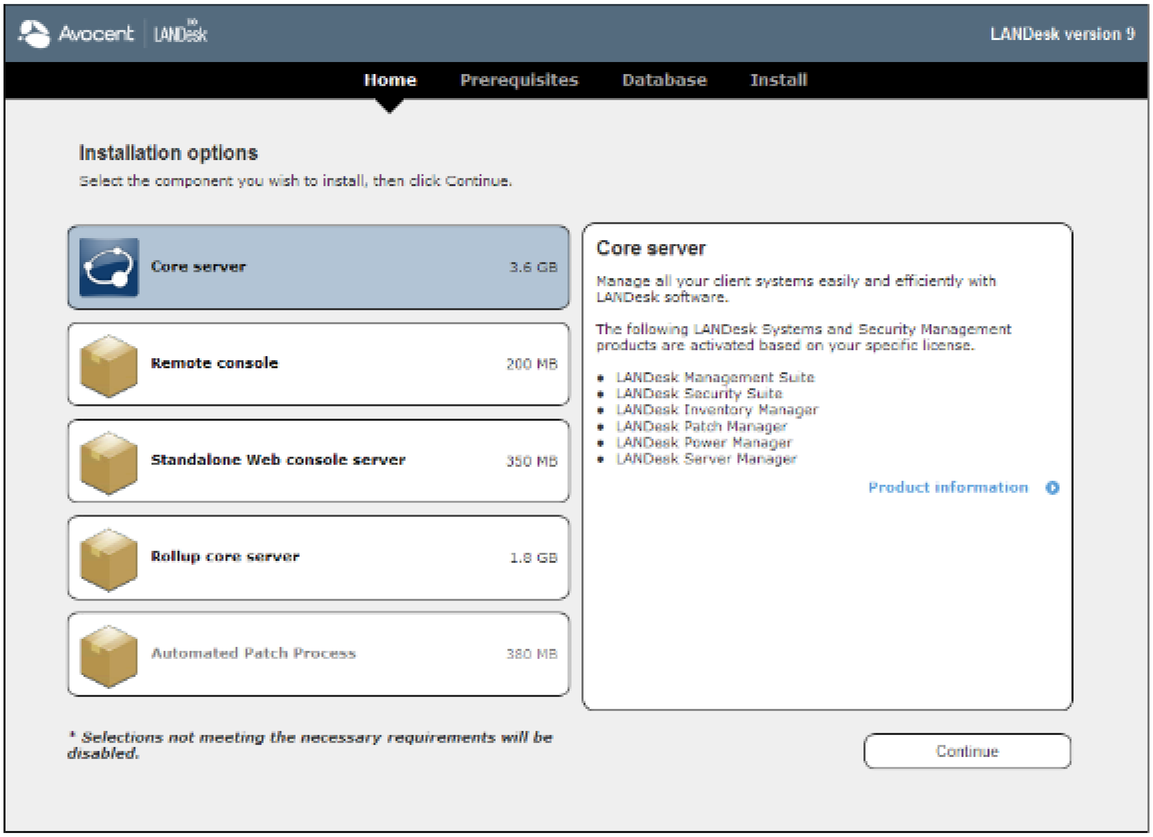
- http://www.landesk.com/wheretobuy/default.aspx

For more information visit the following web site:

- http://www.landesk.com/SupportDownload/Support.aspx?id=3215

To install LANDesk Management Suite

1. From your installation media, launch Autorun.exe.



Installation options

Select the component you wish to install, then click Continue.

Core server	3.6 GB
Remote console	200 MB
Standalone Web console server	350 MB
Rollup core server	1.8 GB
Automated Patch Process	380 MB

Core server

Manage all your client systems easily and efficiently with LANDesk software.

The following LANDesk Systems and Security Management products are activated based on your specific license.

- LANDesk Management Suite
- LANDesk Security Suite
- LANDesk Inventory Manager
- LANDesk Patch Manager
- LANDesk Power Manager
- LANDesk Server Manager

** Selections not meeting the necessary requirements will be disabled.*

2. In the LANDesk autorun, click **Core server** and then click **Continue**.
3. On the **Prerequisites** page, make sure your server passes the prerequisites check. If it doesn't, install the missing prerequisites and click **Continue**.
4. On the **Database** page, click **Create new 9.0 database** and then click **Continue**.
5. On the **Enter database information** page, enter and confirm the password that you want to use for SQL Express.
6. On the same page, enter a **User name** for the Avocent Management Platform, which installs with Management Suite and handles licensing, reporting, and role-based administration. The credentials you provide will let you log directly into the Avocent Management Platform.

7. Click **Continue**. SQL Express will install and setup configures the database.
8. After the database installation finishes, click **Run setup** on the **Install** page.
9. On the **Welcome** page, click **Next**.
10. On the **License agreement** page, review the license and click **Next**.
11. On the **Destination folder** page, click **Next** to accept the default installation path (C:\Program Files\LANDesk\Management Suite\).
12. On the **Security certificate** page, enter your **Organization name** and a **Certificate name**, then click **Next**.
13. On the **Ready to install** page, click **Install**.
14. When setup finishes click **Reboot now**.
15. After you reboot, wait five minutes for all of the services to start.
16. Activate your core as described in "Core activation" on page 41.
17. Launch the console and log in with the Windows credentials of the user logged in during Management Suite setup. (During setup, this user is automatically given full administrator rights in the console.)

When you launch the console, a getting started wizard opens to help you configure Management Suite. It's important that you complete these steps. After you've done this, see "Configuring device agents" on page 75 and the LANDesk User Community at http://community.landesk.com for more information about agent deployment.

Core activation

This chapter provides information about activating your core server with a valid LANDesk software licensee.

Activating the core server

LANDesk Software, Ltd. uses a central licensing server at LANDesk to help you manage your core server's product and node licenses. To use the LANDesk products, you must obtain from LANDesk a user name and password that will activate the core server with an authorized certificate. Activation is required on each core server before you can use LANDesk products on that server. You can activate each core server either automatically by the Internet or manually by e-mail. You may need to reactivate a core server in the event that you significantly modify its hardware configuration.

On a periodic basis, the activation component on each core server will generate data regarding:

- The precise number of nodes you're using
- The non-personal encrypted hardware configuration
- The specific LANDesk Software programs you're using (collectively, the "node count data")

No other data is collected or generated by the activation. The hardware key code is generated on the core server using non-personal hardware configuration factors, such as the size of the hard drive, the processing speed of the computer, and so on. The hardware key code is sent to LANDesk in an encrypted format, and the private key for the encryption resides only on the core server. The hardware key code is then used by LANDesk to create a portion of the authorized certificate.

After installing a core server, use the Core Server Activation utility (**Start > All Programs > LANDesk > Core Server Activation**) to either activate it with a LANDesk account associated with the licenses you've purchased or with a 45-day evaluation license. The 45-day evaluation license is for 100 nodes. The 45-day evaluation period begins when you first activate a product on the core server. If you install other LANDesk products for evaluation on the core server later in the 45-day period, that doesn't extend the initial 45-day evaluation period. All LANDesk products on a single core server share the same evaluation license and the same 45-day evaluation period.

You can install additional LANDesk products under your 45-day evaluation license by using the installation CD's autorun program. From the autorun install the product you want, and during setup choose the **Modify** option. You will then be able to add or remove LANDesk products on your core server.

You can switch from a 45-day evaluation to a paid license at any time by running the Core Server Activation utility and entering your LANDesk username and password.

There are two types of licenses, client and server. Any time you install Management Suite agents on a server operating system, such as Windows 2000 Server or Windows 2003 Server, that installation consumes a Management Suite license for a server. Rollup core servers don't need to be activated.

Each time the node count data is generated by the activation software on a core server, you need to send the node count data to LANDesk, either automatically by the Internet or manually by e-mail. If you fail to provide node count data within a 30-day grace period after the initial node count verification attempt, the core server may become inoperative until you provide LANDesk with the node count data. Once you send the node count data, LANDesk will provide you with an authorized certificate that will allow the core server to work normally once again.

Once you've activated a core server, use the Management Suite console's **Configure > Product Licensing** dialog to view the products and the number of authorized nodes purchased for the account the core server authenticates with. You can also see the date the core server will verify node count data with the central licensing server. The core server doesn't limit you to the number of authorized nodes you purchased.

About the Core Server Activation utility

Use the Core Server Activation utility to:

- Activate a new server for the first time
- Update an existing core server or switch from a trial-use license to a full-use license
- Activate a new server with a 45-day trial-use license

Start the utility by clicking **Start > All Programs > LANDesk > Core Server Activation**. If your core server doesn't have an Internet connection, see "Manually activating a core or verifying the node count data" on page 43.

Each core server must have a unique authorized certificate. Multiple core servers can't share the same authorization certificate, though they can verify node counts to the same LANDesk account.

Periodically, the core server generates node count verification information in the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the LANDesk licensing server. This file is in XML format and is digitally signed and encrypted. Any changes manually made to this file will invalidate the contents and the next usage report to the LANDesk licensing server.

The core communicates with the LANDesk licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require any intervention by you.

Note that the Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.

If your core server doesn't have an Internet connection, you can verify and send the node count manually, as described later in this section.

Activating a server with a LANDesk account

Before you can activate a new server with a full-use license, you must have an account set up with LANDesk that licenses you for the LANDesk products and number of nodes you purchased. You will need the account information (contact name and password) to activate your server. If you don't have this information, contact your LANDesk sales representative.

To activate a server

1. Click **Start > All Programs > LANDesk > Core Server Activation**.
2. Click **Activate this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use.

4. Click **Activate**.

Activating a server with a trial-use license

The 45-day trial-use license activates your server with the LANDesk licensing server. Once the 45-day evaluation period expires, you won't be able to log in to the core server, and it will stop accepting inventory scans, but you won't lose any existing data in the software or database. During or after the 45-day trial use license, you can rerun the Core Server Activation utility and switch to a full activation that uses a LANDesk account. If the trial-use license has expired, switching to a full-use license will reactivate the core.

To activate a 45-day evaluation

1. Click **Start > All Programs > LANDesk > Core Server Activation**.
2. Click **Activate this core for a 45-day evaluation**.
3. Click **Activate**.

Updating an existing account

The update option sends usage information to the LANDesk licensing server. Usage data is sent automatically if you have an Internet connection, so you normally shouldn't need to use this option to send node count verification. You can also use this option to change the LANDesk account the core server belongs to. This option can also change a core server from a trial-use license to a full-use license.

To update an existing account

1. Click **Start > All Programs > LANDesk > Core Server Activation**.
2. Click **Update this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use. If you enter a name and password that's different than the one used to originally activate the core, this switches the core to the new account.
4. Click **Activate**.

Manually activating a core or verifying the node count data

If the core server doesn't have an Internet connection, the Core Server Activation utility won't be able to send node count data. You'll then see a message prompting you to send activation and node count verification data manually through e-mail. E-mail activation is a simple and quick process. When you see the manual activation message on the core, or if you use the Core Server Activation utility and see the manual activation message, follow these steps.

To manually activate a core or verify the node count data

1. When the core prompts you to manually verify the node count data, it creates a data file called {languagecode}-activate.{ datestring}.txt in the "\Program Files\LANDesk\Authorization Files" folder. Attach this file to an e-mail message and send it to licensing@landesk.com. The message subject and body don't matter.
2. LANDesk will process the message attachment and reply to the mail address you sent the message from. The LANDesk message provides instructions and a new attached authorization file.
3. Save the attached authorization file to the "\Program Files\LANDesk\Authorization Files" folder. The core server immediately processes the file and updates its activation status.

If the manual activation fails or the core can't process the attached activation file, the authorization file you copied is renamed with a .rejected extension and the utility logs an event with more details in the Windows Event Viewer's Application Log.

Role-based administration

LANDesk Management Suite lets you manage console users with an extensive set of role-based administration features, you can:

- Assign granular feature-based group permissions
- Easily assign permissions to multiple users through local or LDAP user groups
- Synchronize console user configurations across multiple core servers

You can create roles based on user responsibilities, the management tasks you want them to be able to perform, and the devices you want them to be able to see, access, and manage. Access to devices can be restricted to a geographic location like a country, region, state, city or even a single office or department. Or, access can be restricted to a particular device platform, processor type, or some other device hardware or software attribute. With role-based administration, it's completely up to you how many different roles you want to create, which users can act in those roles, and how large or small their device access scope should be. For example, you can have one or more users whose role is software distribution manager, another user who is responsible for remote control operations, a user who runs reports, and so on.

If you don't have many console users or you don't want to limit the console users that you do have, you can bypass role-based administration entirely and just add users to the core server's local LANDesk Administrators group. Members of this group have full access to the console and can manage all devices. By default, the account used to install Management Suite is placed into the LANDesk Administrators group.

The table below lists some of the possible Management Suite administrative roles you might want to implement, the common tasks that user would perform, and the permissions that user would need in order to function effectively in that role.

Role	Tasks	Required rights
Administrator	Configure core servers, install additional consoles, perform database rollup, manage users, configure alerts, and so on. (Of course, administrators with full permissions can perform any management tasks.)	Management Suite administrator (all permissions implied). Member of core's LANDesk Administrators local group.
Device inventory manager	Discover devices, configure devices, run the inventory scanner, create and distribute custom data forms, enable inventory history tracking, and so on.	Device management. Member of core's LANDesk Management Suite local group.
Helpdesk	Remotely control devices, chat, transfer files, execute software, shutdown, reboot, view agent and health status, and so on.	Remote control tools. Member of core's LANDesk Management Suite local group.
Application	Distribute software packages, use Targeted	Software distribution.

Role	Tasks	Required rights
manager	Multicast and peer download, and so on.	Member of core's LANDesk Script Writers local group.
Migration manager	Create images, deploy OS images, migrate user profiles, create and distribute user-initiated profile migration packages, deploy PXE representatives, assign PXE holding queues, configure the PXE boot menu, create boot floppy disks, and so on.	OS deployment - provisioning. Member of core's LANDesk Script Writers local group.
Reporting manager	Run predefined reports, create custom reports, print reports, publish reports, import and export reports, test user reports, and so on.	Reporting designer or Reporting viewer roles. Member of core's LANDesk Management Suite local group.
Software license monitoring manager	Configure applications to monitor, add licenses, downgrade licenses, verify reports, and so on.	Software license monitoring. Member of core's LANDesk Management Suite local group.
Security manager	Download security content updates and patches, configure devices for security and antivirus scanning, create vulnerability scans and configure security scanner settings, create antivirus scans and configure antivirus settings, edit custom variables and configure custom variable override settings, and many more security-related tasks.	Endpoint security. Member of LANDesk Script Writers local group.

Note: Some of the example administrative roles would require the "Basic Web console" permission in order to use the features in the Web console.

These are just example administrative roles. Role-based administration is flexible enough to let you create as many custom roles as you need. You can assign the same few permissions to different users but restrict their access to a limited set of devices with a narrow scope. Even an administrator can be restricted by scope, essentially making them an administrator over a specific geographic region or type of managed device. How you take advantage of role-based administration depends on your network and staffing resources, as well as your particular needs.

The following is the basic process for using role-based administration:

1. Create roles for console users.
2. Add console users to the Windows LANDesk Management Suite group.
3. Create authentications for each active directory you will be using to designate console users.
4. Optionally use scopes to limit the list of devices that console users can manage.
5. Create a group permission by assigning the roles you created to the active directory groups containing your console users.

6. Optionally use teams to further categorize console users.

Note: If you've upgraded from Management Suite 8, setup creates a log file called ..\LANDesk\Management Suite\RBAUpgradeReport.txt. This file has information to help you map 8.x roles to 9.x.

For more information on using roles, see the following sections:

- "Adding Management Suite console users" on page 46
- "Managing authentications" on page 47
- "Managing roles" on page 48
- "Understanding console rights" on page 51
- "Managing group permissions" on page 57
- "Creating scopes" on page 59
- "Using teams" on page 61
- "Managing report access with role-based administration" on page 61

Adding Management Suite console users

Management Suite users can log in to the console and perform specific tasks for specific devices on the network. The user that is logged in to the server during Management Suite installation is automatically placed into the Windows NT **LANDesk Administrators group**, which gives them full administrator permissions. This individual is responsible for adding additional groups of users to the console and assigning permissions and scopes. Once other administrators have been created, they can perform the same administrative tasks.

Management Suite setup creates several local Windows groups on the core server. These groups control file system permissions to the Management Suite program folders on the core server. You must manually add console users to one of these local Windows groups:

- **LANDesk Management Suite:** This group allows basic core access. The Management Suite folders are read-only. Users in this group can't write to the scripts directory, so they won't be able to manage scripts. Patching vulnerabilities and OS deployment won't work correctly for users in this group because both those features use scripts.
- **LANDesk Script Writers:** This group includes the rights of the LANDesk Management Suite group and it also allows users to write to the scripts folder. Patching vulnerabilities and OS deployment require membership in this group.
- **LANDesk Administrators:** This is the failsafe group for console access. Anyone in this group has full rights in the console, including script writing. By default, the user account that installed Management Suite is added to this group. If you don't have many console users or you don't want to limit the console users that you do have, you can bypass role-based administration entirely and just add users to this group.

When adding full administrators to the console, you can either add them to the core server's local LANDesk Administrators group or you can add them to a different group that has the LANDesk "Administrator" right. The only difference is that users in the Windows LANDesk Administrators group can't be deleted from the console until they are removed from the LANDesk Administrators group.

IMPORTANT: Don't put user accounts in multiple local or Active Directory groups that have group permissions. If an account is a member of more than one group with a group permission, the console won't be able to define which group permission to apply and the resulting rights may not be consistent. The best way to have rights for more than one group is to make a group with all the roles that the user will need, and then make the user part of that group.

IMPORTANT: Additional consoles and the core server must be members of the same domain or workgroup. Console users won't be able to authenticate with a core server that is in a different domain or workgroup.

To add users to a LANDesk group from the Windows Computer Management dialog

1. Navigate to the server's **Administrative Tools > Computer Management > Local Users and Groups > Groups** utility.
2. Right-click the LANDesk group you want, and then click **Add to group**.
3. In the group's **Properties** dialog, click **Add**.
4. In the **Select the users and groups** dialog, select the desired users (and groups) from the list and click **Add**.
5. Click **OK**.

Viewing the user log and deleting users

The Users tool's **All users** group is a log that gets populated as console users log in. You can see the last time they logged in, their group, role, and team. For example, you can monitor users that haven't logged in a long time and consider whether they need the rights that they have. When you add a console user, they won't appear in this list until they log into the console.

You can also delete a user from this list. When you delete a user, you'll be prompted to decide how you want to handle console items they are the owners of, such as queries, scheduled tasks, and so on. You can either have the console automatically delete any items they own or you can have the console reassign items they own to another user that you select. Note that deleting a user only deletes that user from the Management Suite user database. You'll need to also manually remove the user from any Active Directory groups that give them console access. If you don't do this, the deleted user will still be able to log into the console.

To view the user log

1. Click **Tools > Administration > Users**.
2. In the **Users, roles, and scopes** tree click **All users**.

To delete a console user

1. Click **Tools > Administration > Users**.
2. In the **Users, roles, and scopes** tree click **All users**.
3. Select the user you want to delete and press the Delete key.
4. If you want to delete objects associated with the user, click **OK**.
5. If you want to reassign objects associated with the console user, select **Assign Objects to the following user** and click the user or team you want to receive the objects and click **OK**.
6. Remove the user from the local or Active Directory group that gives them console access.

Managing authentications

Use the authentications tree to define credentials for Active Directory groups that will have console access. These credentials only need to let Management Suite enumerate the directory. You'll need to provide credentials for each active directory containing users you want to have console access. The authentications you provide determine which user groups you can select from to assign console group permissions.

Console authentication is based on Windows local or Active Directory group membership. When a LANDesk administrator assigns group permissions to a local or Active Directory group, users who are members of that group can log into the Windows or Web consoles and share the permissions assigned to that group.

You should be aware of the following issues when managing Active Directories for use with Management Suite:

- Active Directory is fully integrated with DNS and TCP/IP (DNS) is required, and to be fully functional, the DNS server must support SRV resource records or service records.
- Using Active Directory to add a user to a group being used in the console will not enable the user to log in to the console even though the user has Management Suite permissions assigned. In order to log in to the console, a user must belong to the core server's local LANDesk groups. For more information, see "Adding Management Suite console users" on page 46.
- In order for Active Directories to work properly with role-based administration, you need to configure the COM+ server credentials on the core server. This enables the core server to use an account in one of the core server's local LANDesk groups that has the necessary permissions to enumerate Windows domain members, such as the administrator account. For instructions on how to perform the configuration, see "Multi-core support" on page 62.

If the account password for an authentication changes, you will have to log into the console and change the password in the authentication dialog to the new password. You can do this by logging in as a local group. Users are authenticated when they log in, so any existing session will continue to work. Users in the domain that has had the password changed won't be allowed to log in until the password change as been corrected in the Users tool.

To add an authentication

1. In the **Users** tool, right-click **Authentications** and click **New authentication**.
2. In the **Authentication details** dialog, enter credentials that give access to the Active Directory.
3. Click **OK**.

Setting rights with Active Directory

The following rules apply to when using Active Directory with RBA:

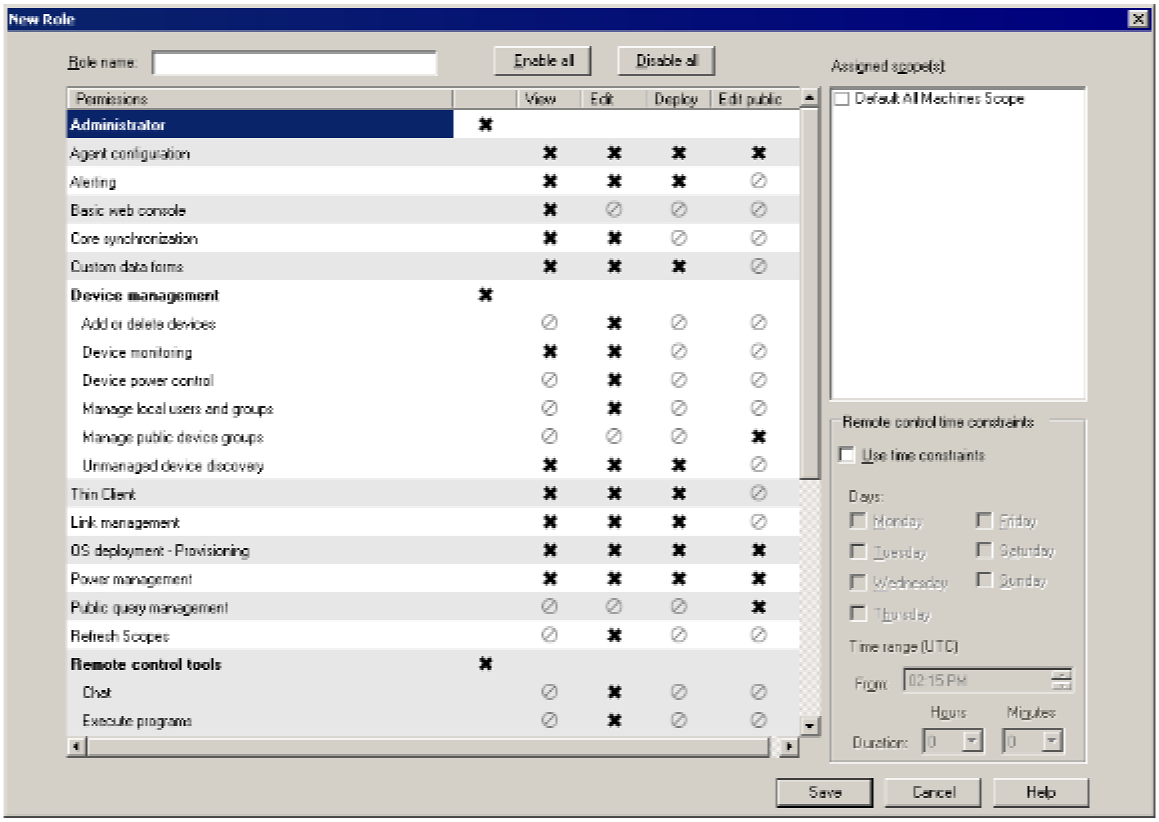
- If a user is a member of an Active Directory group on OU, the user inherits the RBA rights for that group or OU.
- If a user is a member of an Active Directory group or OU, which is a member of a higher level group or OU, the user inherits the RBA rights of the upper level group or OU.
- Groups can be nested and inherit the appropriate rights according to the usual Active Directory rules.

Managing roles

Use the Roles tree to define and maintain administrative roles and their associated console rights. Console rights are based on Management Suite features. For example, you can create a help desk role and give it the remote control right.

You can add as many additional roles as you need. New roles aren't automatically assigned to any user groups. Once you create a role, you associate it with a user group in the Group Permissions tree.

Since you can assign multiple roles to a group of users, decide how you want to assign rights. You can either assign rights based on a job description, such as "help desk," or you can assign rights based on console feature, like "remote control." Depending on the number and variety of console users your organization may have, one way may work better than the other.



Role name:

Permissions		View	Edit	Deploy	Edit public
Administrator	✖				
Agent configuration		✖	✖	✖	✖
Alerting		✖	✖	✖	⊘
Basic web console		✖	⊘	⊘	⊘
Core synchronization		✖	✖	⊘	⊘
Custom data forms		✖	✖	✖	⊘
Device management	✖				
Add or delete devices		⊘	✖	⊘	⊘
Device monitoring		✖	✖	⊘	⊘
Device power control		⊘	✖	⊘	⊘
Manage local users and groups		⊘	✖	⊘	⊘
Manage public device groups		⊘	⊘	⊘	✖
Unmanaged device discovery		✖	✖	✖	⊘
Thin Client		✖	✖	✖	⊘
Link management		✖	✖	✖	⊘
OS deployment - Provisioning		✖	✖	✖	✖
Power management		✖	✖	✖	✖
Public query management		⊘	⊘	⊘	✖
Refresh Scopes		⊘	✖	⊘	⊘
Remote control tools	✖				
Chat		⊘	✖	⊘	⊘
Execute programs		⊘	✖	⊘	⊘

Assigned scope(s)

☐ Default All Machines Scope

Remote control time constraints

☐ Use time constraints

Days:

☐ Monday ☐ Friday
☐ Tuesday ☐ Saturday
☐ Wednesday ☐ Sunday
☐ Thursday

Time range (UTC)

From: 02:15 PM

Duration: Hours 0 Minutes 0

To create a role

1. In the **Users** tool, right-click **Roles** and click **New role**.
2. In the **New role** dialog, enter a **Role name**.
3. Enable or disable the rights you want by clicking on the symbol in the appropriate column. Each click toggles the right's state.
4. Check the device scope you want associated with the role.
5. Set any remote control time constraints that you want.
6. Click Save.

Understanding rights and states

There are four types of rights a user can have:

- **View:** Allows users to access a console tool.
- **Edit:** Allows users to make changes in the associated console tool. Includes the view right.
- **Deploy:** Allows users to create, modify, or delete any scheduled tasks associated with the associated console tool.
- **Edit public:** Allows users to create, modify, or delete items in a console tool's **Public** folder.

Not all rights support all types. For example, the "Public query management" right can only have the "Edit public" type. It wouldn't make sense to also have the "View," "Edit," or "Deploy" types.

There are three states a right can have:

- A checkmark: ✔
- An X: ✖
- A not applicable symbol: ⊘

Clicking on a checkmark or an X will toggle its state.

If users have no rights for a tool, they won't see the tool when they log into the console. The tool won't appear in the Toolbox or in the **Tools** menu.

The **Scheduled tasks** tool is only visible to users who have a "Deploy" right, and in that case, they can only work with tasks associated with the tool they have deploy rights for. All other tasks are read-only.

Understanding the default roles

There are three default roles under the Roles tree. You can't edit or delete these default roles:

- **LANDesk Administrator:** This role has all console rights, including adding and deleting console users.
- **ReportingDesigner:** This role gives users the ability to create, edit, and run reports.
- **ReportingViewer:** This role gives users the ability to run reports.

LANDesk Administrators have full rights to all scopes and rights. They also have full access to the Users tool and can make any changes they want. Only users with the Administrator right can configure LANDesk services running on the core.

For more information on the reporting roles, see the reports chapter.

Understanding the "Edit public" right

A tool's Public group is visible to all users. Items in the public group are read-only, unless you have the "Edit public" right. Users that have "Edit public" rights on a feature can only edit public items for that feature. Other public items will be read-only. Read-only items are still useful, since users can copy those items to the "My ..." tree group and edit them there.

The **Scheduled tasks** tool's Public group works slightly differently. All tasks in the Public group are visible to users with a "deploy" right, including tasks for features users may not have access to. However, only tasks that users have a "Deploy" right for are editable. The rest are read-only.

If you have "Edit Public" and "Deploy" right types, you can create new tasks in the Public group as well as add/remove tasks from it.

Using remote control and time constraints

When creating a role, you have the opportunity to also define remote control time constraints. These time constraints limit the hours and days console users can initiate remote control sessions. When enabled, specify the days of the week, the starting time (in UTC format) and duration for the period of time that you want to allow remote control.

Note that the starting time is in UTC (Coordinated Universal Time or Greenwich Mean Time) format. The core server determines the starting time by checking the UTC time reported by the core server's operating system. The core server doesn't adjust for the console users' local time zone. When entering the starting time value, you need to compensate for the difference between UTC time and the console operators' local time zone and use the resulting adjusted time.

Note: Remote control integrated security only works with scope assigned to the same role.

Understanding console rights

Console rights provide access to specific Management Suite tools and features. Users must have the necessary rights to perform corresponding tasks. For example, in order to remote control devices in their scope, a user must be part of a group that has the remote control right.

Role-based administration includes the following permissions:

- Management Suite Administrator
- Agent configuration
- Alerting
- Basic Web console
- Core synchronization
- Custom data forms
- Device management
- Add or delete devices
    - Device monitoring
    - Device power control
    - Manage local users and groups
    - Manage public device groups
    - Unmanaged device discovery
- Thin client
- Link management
- OS deployment-Provisioning
- Power management
- Public query management
- Refresh scopes
- Remote control tools
    - Chat
    - Execute programs
    - Reboot
    - Remote control
    - Transfer files
- Endpoint security
    - Network access control
    - Patch and compliance
    - Security configurations
- Software distribution
    - Delivery methods
    - Directory management
    - Distribution packages
    - Manage scripts
- Software licensing
- User administration

See the descriptions below to learn more about each permission and how permissions can be used to create administrative roles.

Scope controls access to devices
Keep in mind that when using the features allowed by these permissions, users will always be limited by their scope (the devices they can see and manipulate).

Management Suite Administrator

The Management Suite Administrator permission provides full access to all of the application tools (however, use of these tools is still limited to the devices included in the administrator's scope).

The Management Suite Administrator permission provides users the ability to:

- Manage users with the Users tool.
- See and configure product licensing in the **Configure** menu.
- Configure LANDesk services.
- **Important:** Perform ALL of the Management Suite tasks allowed by the other permissions.

Agent configuration

- No rights: Can’t see the tool.
- View: Can see this tool and can view anything. Can’t change anything.
- Edit: Can see and change anything. Can’t deploy an agent configuration job.
- Deploy: Can see everything. Can’t change anything. Can schedule any agent configuration task that they can see (including public).
- Edit public: Can assign configurations to public. Can edit public configurations.

Alerting

- No rights: Can’t see the tool.
- View: Can see this tool and can view anything. Can’t change anything.
- Edit: Can see and change anything. Can’t deploy.
- Deploy: Can see everything. Can’t change anything. Can deploy.

Basic Web console

- No rights: Can’t log into Web console.
- View: Not applicable.
- Edit: Can log into Web console and see the most basic things.
- Deploy: Not applicable.

Core synchronization

- No rights: No core synchronization tool. No right-click options to **Autosync** or **Copy to core**. Still show import and export options. (These are tied into the "Edit" right for the tool that has these options.)
- View: Can see the tool, but can't make any changes. Still no synchronization options in context menus as above.
- Edit: Can do everything. Add/remove target cores, turn components on and off, enable auto sync on instances, and manual sync.
- Deploy: Not applicable.

Custom data forms

- No rights: Can’t see the tool.

- View: Can see this tool and can view anything. Can't change anything.
- Edit: Can see and change anything. Can't deploy.
- Deploy: Can see everything. Can't change anything. Can deploy.

Device management

Add / Delete devices

- No rights:
  - Can't see the **Insert new computer** option in the context menu when viewing **All devices** in the **Network view**.
  - Can't see the **Delete** option in the context menu when selecting a device in the **Network view**.
  - Can't see the **Network view > Configuration > User added computers** tree node.
- View: Not applicable.
- Edit:
  - Can see and use the **Insert new computer** option in the context menu when viewing **All devices** in the **Network view**.
  - Can see and use the **Delete** option in the context menu when selecting a device in the **Network view**.
  - Can see the **Network view > Configuration > User added computers** tree node.
- Deploy: Not applicable.

Manage public device groups

- No rights: Can't change anything in **Public devices**.
- View: Not applicable.
- Edit: Not applicable.
- Deploy: Not applicable.
- Edit Public: Can create, delete and change device groups in **Public devices**. Can move a device group into **Public devices**.

Unmanaged device discovery

- No rights: Can't see the UDD tool.
- View: Can open the UDD tool and view any item. Can't create/delete/edit anything.
- Edit: Can open the UDD tool and view any item. Can create/delete/edit anything.
- Deploy: Can open the UDD tool and view any item. Can't create/delete/edit anything. Can schedule a UDD task.

Device monitoring

- No rights: Can't see **Device monitoring** from the **Configure** menu.
- View: Can see the Alerting tool and Logs tool. Can see information in the Device monitoring tool. Can't edit it.
- Edit: Can see the Alerting tool and Logs tool. Can see and edit information in the Device monitoring tool.
- Deploy: Not applicable.

Wake/Reboot/Shutdown

- Edit: Can see and use **Wake up**, **Reboot** and **Shutdown** options in the context menu when selecting a device.

Manage local users and groups

- Edit: Can see and use **Manage local users and groups** in the context menu when selecting a device.

Handheld

- No rights: Can’t see the handheld tools.
- View: Can see the handheld tools. Can’t change anything.
- Edit: Can create, edit and delete items. Can't schedule a job.
- Deploy: Can't create, edit and delete items. Can schedule a job. Can use the **Handheld task** button in the Scheduled tasks tool.

Launchpad

- No rights: Can’t see the Launchpad tool.
- View: Can see the tool. Can’t change anything.
- Edit: Can create, edit, and delete items. Can't schedule a task/policy.
- Deploy: Can't create, edit, and delete items. Can schedule a task/policy.

OS Deployment / Provisioning

- No rights: Can’t see the OS Deployment tool.
- View: Can see the tool. Can’t change anything.
- Edit: Can create, edit and delete items. Can't schedule tasks.
- Deploy: Can schedule tasks for items that they can see (including public). Can't create, edit and delete items.
- Edit Public: Can move items to the Public folder. Can create, edit or delete items in the Public folder.

Power management

- No rights: Can’t see the Power Management tool.
- View: Can see the tool. Can’t change anything.
- Edit: Can create, edit and delete items. Can't schedule tasks.
- Deploy: Can schedule tasks for items that they can see (including public). Can't create, edit and delete items.
- Edit Public: Can move items to the Public folder. Can create, edit or delete items in the Public folder.

Public query management

- No rights: Regular behavior.
- View: Not applicable.
- Edit: Not applicable.
- Deploy: Not applicable.
- Edit Public: Can move queries to the Public folder. Can create, edit or delete queries in the Public folder.

Refresh scopes

No rights: The **Network view**'s **Refresh scopes** toolbar button doesn't do anything.

Edit: The **Network view**'s **Refresh scopes** toolbar button updates all scopes. Use this when you've added devices to a scope or changed a user's scope and you want that user to see the new scope. Otherwise the scope refresh can wait up to an hour before it occurs automatically.

Remote control tools

Remote control

- No rights: Can’t see the **Remote control > Remote control** option in the context menu.
- View: Can see the **Remote control > Remote control** option and can remote control a device. Can’t take control of the device (view only).
- Edit: Can see the **Remote control > Remote control** option and can remote control and take control of a device.
- Deploy: Not applicable.

Execute programs

- Edit: Can see the **Remote control > Execute program** option and can use it. The **Execute program** option is enabled in the Remote control window.

Transfer files

- Edit: Can see the **Remote control > Transfer files** option and can use it. The **Transfer files** option is enabled in the Remote control window.

Chat

- Edit: Can see the **Remote control > Chat** option and can use it. The **Chat** option is enabled in the Remote control window.

Reboot

- Edit: Can see the **Remote control > Reboot** option and can use it. The **Reboot** option is enabled in the Remote control window.

Security

Patch and compliance

- No rights: Can’t see the tool. Can’t see any scheduled tasks or policies in software distribution that are created from the tool.
- View: Can see the tool. Can see everything inside. Can't download content, create/edit/delete configurations, or change anything. It is read-only.
- Edit: Can see the tool. Can see everything inside. Can edit anything. Can’t schedule anything, including: content downloads, scan jobs, repair jobs, gather history, etc.
- Deploy: Can see the tool. Can see everything inside. Can't modify anything, but can create a task or policy using the information there for items that they can see (including public).
- Edit Public: Can move items to the Public folder. Can create, edit or delete items in the Public folder.

Security configurations

- No rights: Can’t see the tool. Can’t see any scheduled tasks or policies in the Scheduled tasks window that are created from this tool.
- View: Can see this tool and the Security Activities tool. Can look at but not change any configurations or create any tasks.
- Edit: Can see the tool and the Security Activities tool. Can see everything inside. Can edit anything. Can’t schedule anything.
- Deploy: Can see the tool and the Security Activities tool. Can see everything inside. Can't modify anything, but can create a task or policy to deploy this to a client or change its configuration for items that they can see (including public).
- Edit Public: Can move items to the Public folder. Can create, edit or delete items in the Public folder.

Network access control

- No rights: Can’t see the tool.
- View: Can see this tool and can view anything (such as the 802.1x configuration). Can’t change anything.
- Edit: Can see and change anything, including publishing NAC settings.
- Deploy: Not applicable.

Software distribution

Delivery methods

- View: Can see the tool and everything in it.
- Edit: Can create/edit/delete methods.
- Deploy: Not applicable
- Edit Public: Can move items to the Public folder. Can create, edit or delete items in the Public folder.

Distribution packages

- View: Can see the tool and everything in it.
- Edit: Can create/edit/delete packages.
- Deploy:
  - Can deploy a package in the distribution package tool.
  - Can use the **Create software distribution task** button in the Scheduled tasks tool.
  - Can use the **Create custom script task** button in the Scheduled tasks tool.
  - This applies to all items that they can see (including public).
- Edit Public: Can move items to the Public folder. Can create, edit or delete items in the Public folder.

Directory manager

- View: Can see the tool and everything in it (assuming someone has authenticated already).
- Edit: Can authenticate to a new directory and can see everything and can create/edit/delete queries.
- Deploy: Not applicable.

Manage scripts

- View: Can see this tool and can view anything. Can’t change anything.
- Edit: Can see and change anything. Can’t schedule a task.
- Deploy: Can schedule tasks for items that they can see (including Public). Can't create, edit and delete items.
- Edit Public: Can move items to the Public folder. Can create, edit or delete items in the Public folder.

Scheduled tasks

- If someone has "Deploy" rights for any of the tools listed below, they can see the scheduled task tool.
- If someone has "Deploy" rights they have rights to modify any part of the type of task that they have "Deploy" rights for (for example, agent configuration, software distribution, Patch, etc.).
- If someone has "Deploy" rights, they can change only the **Target** and the **Schedule** panes of a Public task.
- If someone has "Deploy" rights and "Edit Public" rights, they can make any changes to Public tasks and can move tasks to and from the Public folder.
- If someone has "Edit Public" rights but not "Deploy" rights, they can't edit any task of that type, including Public tasks.

Software license monitoring

- No rights: Can’t see the Software license monitoring tool.
- View: Can see everything. Can’t change anything.
- Edit: Can see and edit anything.
- Deploy: Not applicable.

User administration

- No rights: Can’t see the Users tool.
- View: Can see everything. Can’t change anything.
- Edit: Not applicable.
- Deploy: Not applicable.

Managing group permissions

Use the **Group permissions** tree to associate local or Active Directory groups with roles you've created. This combination of roles and groups is called a group permission. When you add or edit group permissions, only active directories that you've provided authentication credentials for are visible.

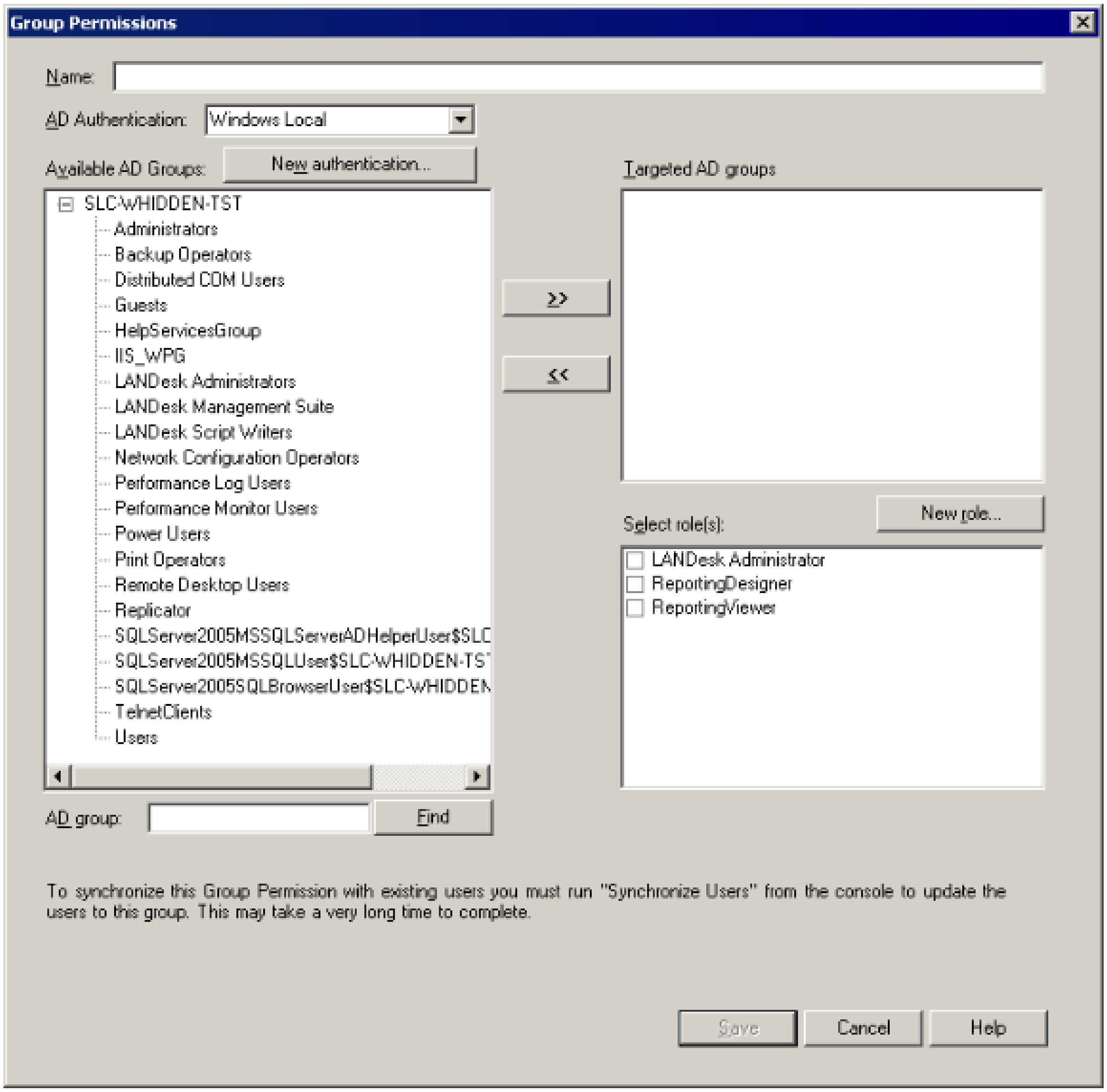
You can't assign permissions to an individual, only a group. If you want to assign rights to an individual, you must put them into a group first and then assign rights to that group.

You can assign multiple roles to a single Active Directory group. If there are conflicting rights among the selected roles, the group permission consists of the sum of the combined roles and scopes. For example, if one included role allows remote control and another included role denies it, the resulting group permission will allow remote control.

Generally, you should avoid assigning group permissions to the default local groups: LANDesk Management Suite, LANDesk Script Writers, and LANDesk Administrators. Assigning group permissions to a group affects everyone in the group. Since all console users must be a member of one of these three groups, you could unintentionally restrict everyone's access to console features.

Also, make sure users aren't in multiple groups that have different group permissions. In this scenario, users will only get one of their assigned group permissions and the group permission they get may vary from login to login.

Note: The LANDesk Administrators group permission associates the LANDesk Administrator role with the LANDesk Administrators local users group. This group permission can't be edited or deleted.



AD Authentication: Windows Local

To synchronize this Group Permission with existing users you must run "Synchronize Users" from the console to update the users to this group. This may take a very long time to complete.

To create a group permission

1. In the **Users** tool, right-click **Group permissions** and click **New group permission**.
2. In the **Group permissions** dialog, enter a **Name** for your group permission.
3. Select an **AD authentication source**. This determines which groups appear in the **Available AD groups** box.

4. Use the **>>** and **<<** buttons to move groups from the **Available AD groups** box to the **Targeted AD groups** box.
5. Select the roles you want assigned to this group permission.
6. Click **Save**.

Creating scopes

A scope defines the devices that can be viewed and managed by a Management Suite user.

A scope can be as large or small as you want, encompassing all of the managed devices scanned into a core database, or possibly just a single device. This flexibility, combined with modularized tool access, is what makes role-based administration such a versatile management feature.

Default scopes

Management Suite's role-based administration includes one default scope: the "default all machines scope." This scope includes all managed devices in the database. You can't edit or remove the default scope.

Custom scopes

There are three types of custom scopes you can create and assign to users:

- **LDMS query:** Controls access to only those devices that match a custom query search. You can select an existing query or create new queries from the Scope properties dialog to define a scope. Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group. For more information on creating queries, see "Creating database queries" on page 105.
- **LDAP:** Controls access to only those devices gathered by the inventory scanner that are located in an LDAP-compliant directory structure. Select directory locations from the **Select visible devices** dialog to define a scope. This directory-based scope type also supports custom directory locations (if you've entered custom directory paths as part of an agent configuration). Available custom directory paths appear in the **Select visible devices** dialog. Use custom directories to define a scope if you don't have an LDAP-compliant structure, or if you want to be able to restrict access to devices by a specific organizational detail such as geographic location or department.
- **Device group:** Controls access to only those devices that belong to a specific device group in the network view.

A Management Suite user can be assigned one or more scopes at a time. Additionally, a scope can be associated with multiple users.

How multiple scopes work

More than one scope can be assigned to any of the Management Suite users. When multiple scopes are assigned to a user, the user has rights to all computers in all assigned scopes. The cumulative list of computers in all assigned scopes is the user's effective scope.

A user’s effective scope can be customized by adding and removing scopes at any time. Multiple scopes and scope types can be used together.

A user’s rights and scopes can be modified at any time. If you modify a user’s rights or scopes, those changes take affect the next time that user logs into the console or when a console administrator clicks the **Refresh scope** toolbar button on the Console (top of window).

Creating a scope

To create a scope

1. Click **Tools > Administration > Users**.
2. Right-click **Scopes** and click **New Scope**.
3. In the **Scope Properties** dialog, enter a name for the new scope.
4. Specify the type of scope you want to create (LDMS query, LDAP or custom directory, or device group) by clicking a scope type from the drop-down list, and then clicking **New**.
5. If you're creating an LDMS query-based scope, define the query in the **New scope query** dialog, and then click **OK**.
6. If you're creating a directory-based scope, select locations (LDAP directory and/or custom directory) from the **Select visible devices** list, and then click **OK**.

Click on the plus (+) and minus (-) signs to expand and collapse nodes in the directory tree. You can multi-select locations by using Ctrl-click. All nodes under a selected parent node will be included in the scope.

LDAP directory locations are determined by a device's directory service location. Custom directory locations are determined by a device's computer location attribute in the inventory database. This attribute is defined during device agent configuration.

7. If you're creating a device group-based scope, select a group from the available device group list, and then click **OK**.
8. Click **OK** again to save the scope and close the dialog.

About the Scope Properties dialog

Use this dialog to create or edit a scope. You can access this dialog by selecting a scope and clicking the **Edit scope** toolbar button or by right-clicking the scope and then clicking **Properties**.

- **Scope name:** Identifies the scope.
- **Select a scope type:**
  - **LDMS query:** Creates a scope whose device range is determined by a custom query. Clicking **New** with this scope type selected opens the **New query** dialog where you can define and save a query. This is the same query dialog you use when creating a database query from the network view. (Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group.)
  - **LDAP:** Creates a scope whose device range is determined by the device location (LDAP directory and/or custom directory). Clicking **New** with this scope type selected opens the **Select visible devices** dialog where you can select locations. Click on the plus (+) and minus (-) signs to expand and collapse nodes in the directory tree. You can multi-select locations by using Ctrl-click. All nodes under a selected parent node will be included in the scope.
  - **Device group:** Creates a scope whose device range is determined by an existing group of devices contained under the Devices object in the network view. Clicking **New** with this scope type selected opens the **Query filter** dialog where you can select a device group.
- **Current scope definition:** Displays the query statements for a query-based scope, the location paths for a directory-based scope, or the group name for a device group-based scope.
- **Edit:** Opens the scope's appropriate dialog where you can change query parameters and statements.

Using teams

A role-based administration team is a group of users that can view and share ownership of tasks and configurations that belong to the team. For example, if you have multiple departments that want to share queries or tasks, you can group the departments into a team. A team's tasks and configurations appear in a special group named after the team in a tool's tree view. For example, if you have a team named "Salt Lake" that you are a member of, you would see a "'Salt Lake' devices" subgroup under the **Devices** group in the **Network view**. People can belong to multiple teams.

People who aren't in a particular team won't see that team's group anywhere in the console. People with the administrator right see all teams and team content. While you can use public folders to share console content, public folder content is visible to everyone with rights to a tool. The advantage with teams is that only team members see team content, potentially making content more organized and accessible to team members.

Teams consist of one or more group permissions. You can even create teams with as few as 1 or 2 people. For example, if a person is out sick, you can add that person's substitute to the same team. Or, if you have two people that share responsibilities, you can put them in the same team.

Administrators and team members can change the ownership of tree items by right-clicking them and clicking **Info**. Information dialog boxes have an **Owner** drop-down list where you can select the item's owner.

To create a team

1. In the **Users** tool, right-click **Teams** and click **New team**.
2. Enter a **Team name**.
3. Check the **Group permissions** you want for the members of this team.
4. Click **Save**.

Managing report access with role-based administration

Users who need to use Management Suite reports must have one of these roles assigned to them in the Users tool:

- **ReportingDesigner:** This role gives users the ability to create, edit, and run reports.
- **ReportingViewer:** This role gives users the ability to run reports.

These roles are defaults and aren't editable. Users without one of these roles won't see the console's Reports tool.

In the Reporting console (**Tools > Reporting / Monitoring > Reports**), reports and the folders that contain them are associated with role-based administration roles. By default, reports and folders have these roles and associated rights:

- **Avocent administrator:** Folder read, folder write, report read, report write
- **LANDesk administrator:** Folder read, folder write, report read, report write
- **ReportingDesigner:** Folder read, folder write, report read, report write
- **ReportingViewer:** Folder read, report read

Reporting rights do the following:

- Read rights on a folder let users open that folder and see the reports that are visible to them.
- Read rights on a report let users run that report.

- Write rights on a folder let users add reports to a folder or delete an empty folder.
- Write rights on a report let users modify or delete that report.

Reporting rights only apply to the selected object and they aren't recursive. For example, applying read rights to a folder doesn't automatically give read rights to all reports in that folder.

Limiting access to specific reports or folders

By default, anyone with the ReportingViewer role can see all reports and folders. If necessary, you can restrict access to specific reports and folders.

To restrict access to specific reports and folders

1. In the Users tool under **Roles**, right-click the **ReportingViewer** role and click **Clone**.
2. Rename the cloned ReportingViewer role to something more specific, like "Inventory report viewer"
3. Create a new group permission for the users you want to limit, and in the **Group permissions** dialog, target the Active Directory groups you want. In the roles box, clear the **ReportingViewer** right and check your new cloned role (Inventory report viewer, for example).
4. Click **Tools > Reporting / Monitoring > Reports**.
5. In the Reports viewer, open the properties for the report or folder you want to limit by right-clicking it and clicking **Edit**. Go to the **Security** page and **Add** the cloned reporting role you made. You'll need to do this on the parent folder level too, otherwise users with the cloned right won't be able to open the folder to see the report they need access to.

Multi-core support

The following conditions must be met in order to use multiple cores:

- Both cores must be part of the same domain.
- The domain administrator account must be added to the LANDesk ManagementSuite local user group on both cores.
- The identity of the LANDesk COM+ application under component services must be set to the domain administrator. This is described in the next section.
- The core.asp file must be edited to include the second core. The core.asp file is in the \inetpub\wwwroot\LANDesk\LDMS\xml folder. Once this is done, when you initially access the Web console in a browser, you'll see a dropdown list containing the servers defined in core.asp. Click the server you want and click **Connect**.

Below is a sample core.asp that includes multiple servers.

```
<?xml version="1.0" ?>
<core>
<cores>
<item name="Core_Host_Name_1" rollup="0"/>
<item name="Core_Host_Name_2" rollup="0"/>
<item name="Rollup_Core_Host_Name_3" rollup="1"/>
</cores>
</core>
```

To log into a core in a multi-core environment

1. Launch the Management Suite Web console.
2. In the **Select a core** list, select the core that you want to log into and click **Connect**. Type the user name and password.

Notes

- To successfully complete client configuration, use the correct URL for the core. Otherwise, the configuration won't work.
- You may find it useful to add entries for each core server to your Favorites menu in Internet Explorer. This facilitates switching between cores.

Configuring COM+ server credentials

When using a Web console server that isn't on the core, or if you want to use domain groups inside the LANDesk Management Suite group on the core server, there is some additional server configuration you must do for Management Suite authentication to work correctly. Remote Web console servers must get database connection information and user information from the core server, but since remote Web console servers use impersonated Web credentials on IIS, they can't communicate with the core server directly.

To solve this issue, the Web console server and core server use a COM+ application to communicate via HTTPS, allowing the Web console server to get core server database and user information. You need to configure this COM+ application on the Web console server to use an account that has the necessary rights, such as the domain administrator account. The account that you provide needs to be in the LANDesk Management Suite group on the core server (this allows it to access core server database connection information), and it needs to have rights to enumerate Windows domain members.

If you're using domain groups inside the core server's LANDesk Management Suite group, Management Suite also needs to be able to enumerate Windows domain members. In this case, you also need to provide an account for the core server's LANDesk1 COM+ application.

To configure the LANDesk1 COM+ application on a core or remote Web console server

1. Go to the Web server or core server you want to configure.
2. From the Windows Control Panel's Administrative Tools, open **Component Services**.
3. Click **Component Services > Computers > My Computer > COM+ Applications**.
4. Right-click the **LANDesk1** COM+ application and select **Properties**.
5. On the **Identity** tab, enter the credentials you want to use.
6. Click **OK**.

Configuring services

Many of the most integral and fundamental functions provided by LANDesk components, such as the inventory server and the scheduler service, can and should be configured in order to optimize performance in your particular network environment. Do this by using the **Configure LANDesk Software Services** applet that you can launch from the **LANDesk** Start menu program group.

Configuring services is restricted to only LANDesk Administrators
Only a user with the LANDesk Administrator right can modify service settings. Also, the **Configure services** option is available only from the main console, not from any additional consoles you may have set up.

Read this chapter to learn about:

Selecting a core server and database

Before configuring a service, use the **General** tab to specify the core server and database you want to configure the service for.

Note: Any service configuration changes you make for a core server and database will not take effect until you restart the service on that core server.

About the Configure LANDesk Software Services dialog: General tab

Use this dialog to select the core server and database you want to configure a specific service for. Then, select the desired service tab and specify the settings for that service.

- **Server name:** Displays the name of the core server you're currently connected to.
- **Server:** Lets you enter the name of a different core server and its database directory.
- **Database:** Lets you enter the name of the core database.
- **User name:** Identifies a user with authentication credentials to the core database (specified during setup).
- **Password:** Identifies the user's password required to access the core database (specified during setup).
- **This is an Oracle database:** Indicates that the core database specified above is an Oracle database.
- **Web console settings:** Displays the server name or IP address on which the Web console can be run. When you want to access the Web console from another device, you type this name or address, followed by /remote, in a Web browser.

- **Refresh settings:** Restores the settings that were present when you opened the dialog.

When specifying usernames and passwords to a database, the username and the password may not contain an apostrophe ('), a semicolon (;) or an equals sign (=).

Configuring the Inventory service

Use the **Inventory** tab to configure the Inventory service for the core server and database you selected using the General tab.

If you need to restart the Inventory service on a clustered core, you'll need to do it through the Windows Service Control Manager. The **Restart** services button in the LANDesk Software Services dialog's **Inventory** tab can't restart the Inventory service on a clustered core.

About the Configure LANDesk Software Services dialog: Inventory tab

Use this tab to specify the following inventory options:

- **Server name:** Displays the name of the core server you're currently connected to.
- **Log statistics:** Keeps a log of core database actions and statistics. You can view the log data in the Windows Event Viewer's Application log.
- **Encrypted data transport:** Enables the inventory scanner to send device inventory data from the scanned device back to the core server as encrypted data through SSL.
- **Scan server at:** Specifies the time to scan the core server.
- **Perform maintenance at:** Specifies the time to perform standard core database maintenance.
- **Days to keep inventory scans:** Sets the number of days before the inventory scan record is deleted.
- **Primary owner logins:** Sets the number of times the inventory scanner tracks logins to determine the primary owner of a device. The primary owner is the user who has logged in the most times within this specified number of logins. The default value is 5 and the minimum and maximum values are 1 and 16, respectively. If all of the logins are unique, the last user to log in is considered the primary owner. A device can have only one primary owner associated with it at a time. Primary user login data includes the user's fully qualified name in either ADS, NDS, domain name, or local name format (in that order), as well as the date of the last login.
- **Advanced settings:** Displays the **Advanced settings** dialog. You can change inventory-related advanced settings here. As you click each item, help text appears at the bottom of the dialog explaining each option. The default values should be fine for most installations. To change a setting, click it, change the **Value**, then click **Set**. Restart the inventory service when you're done.
- **Unknown items:** Opens the **Unknown inventory items** dialog box, which lists any objects that have been found in scans that are not already found in the database. This gives you control over what new items are added to the database so you can eliminate potential problems with data. You can choose to allow the data to be added to the database, simply delete the data from this list, or ignore the item in all future scans.
- **Software:** Displays the **Software scan settings** dialog. Configure when the software scans run and how long to save the inventory history.
- **Manage duplicates: Devices**: Opens the **Duplicate devices** dialog, where you can configure how duplicate devices are handled.
- **Manage duplicates: Device IDs:** Opens the **Duplicate device ID** dialog, where you can select attributes that uniquely identify devices. You can use this option to avoid having duplicate device IDs scanned into the core database (see "Resolving duplicate device records in the database" on page 67).

- **Status of inventory service:** Indicates whether the service is started or stopped on the core server.
    - **Start:** Starts the service on the core server.
    - **Stop:** Stops the service on the core server.
    - **Restart:** Restarts the service on the core server.

About the Unknown inventory items dialog

The **Unknown inventory items** dialog box lets you control what new items are added to the inventory database. When the inventory scan runs, it can find objects that are not identified in the database. Because there can be corrupt data or other issues on a managed device, you may not want the new data to be added to the database. This dialog box lists all items that have been found and gives you the option to add the new items to the database, delete them, or block them from ever being added to the database.

- **Block unknown inventory items:** When this check box is selected, all unknown items are listed here until you choose how to disposition them.
- **Blocked items:** Lists all inventory objects that are not currently in the database. Click one or more items to select them and apply an action.
- **Allow:** Select items and click **Allow** to add the data to the database. The items will be added to the database and allow it to be processed in future inventory scans.
- **Delete:** Select items and click **Delete** to remove them from this list only. If the item if found again, it will be listed again. Typically you would delete items that are the result of data corruption and will likely never be found again in a scan.
- **Ignore:** Select items and click **Ignore** to permanently block them from being added to the database. For performance reasons, the Ignore list should be kept as short as possible. Note that items in this list are permanently ignored; the only way to remove them from the list is to remove them manually from the META_IGNORE table in the inventory database and restart the inventory service.
- **OK/Cancel:** In this dialog box, the **OK** and **Cancel** buttons apply only to the **Block unknown inventory items** check box, not to any actions on blocked items.

About the Software scan settings dialog

Use this dialog (**Configure > Services > Inventory** tab **> Software** button) to configure the frequency of software scans. A device's hardware is scanned each time the inventory scanner is run on the device, but the device's software is scanned only at the interval you specify here.

- **Every login:** Scans all of the software installed on the device every time the user logs on.
- **Once every (days) :** Scans the device's software only on the specified daily interval, as an automatic scan.
- **Save history (days) :** Specifies how long the device's inventory history is saved. Clear the check box to not save the inventory history.

Configuring what inventory scan attributes get stored in the database

The inventory scanner looks for hundreds of inventory items. If you don't need all of this scan information in your database, you can speed up scan insertion time and reduce your database size by limiting the number of scan attributes that get stored in the database. When you do this, managed devices still submit complete inventory scans, but the core server's inventory service only stores the attributes you specify in the database.

By default, the inventory service inserts all scan attributes into the database. Any attribute filtering changes you make won't affect data that is already in the database. To limit what data gets stored, follow the steps below.

To set up inventory scan data filtering

1. Click **Configure > Services > Inventory** tab **> Attributes** button.
2. Attributes in the **Selected attributes** column on the right get inserted into the database. Move the attributes you don't want in the database to the **Available attributes** column on the left. When you have finished, click **OK**.
3. Restart the inventory service by clicking **Restart** on the Inventory tab.
4. Click **OK**.

Resolving duplicate device records in the database

In some environments OS imaging is used regularly and frequently to set up devices. Because of this, the possibility of duplicate device IDs among devices is increased. You can avoid this problem by specifying other device attributes that, combined with the device ID, create a unique identifier for your devices. Examples of these other attributes include device name, domain name, BIOS, bus, coprocessor, and so on.

The duplicate ID feature lets you select device attributes that can be used to uniquely identify the device. You specify what these attributes are and how many of them must be missed before the device is designated as a duplicate of another device. If the inventory scanner detects a duplicate device, it writes an event in the applications event log to indicate the device ID of the duplicate device.

In addition to duplicate device IDs, you may also have duplicate device names or MAC addresses that have accumulated in the database. If you're experiencing persistent duplicate device problems (and you want to prevent future duplicate device records being scanned into your database), you can also specify that any duplicate device names currently residing in the database are removed. This supplementary duplicate device handling feature is included as part of the procedure below.

To set up duplicate device handling

1. Click **Configure > Services > Inventory > Device IDs**.
2. Select attributes from the **Attributes list** that you want to use to uniquely identify a device, and then click the right-arrow button to add the attribute to the **Identity Attributes** list. You can add as many attributes as you like.
3. Select the number of identity attributes (and hardware attributes) that a device must fail to match before it's designated as a duplicate of another device.
4. If you want the inventory scanner to reject duplicate device IDs, select the **Reject duplicate identities** check box.
5. Click **OK** to save your settings and return to the **Configure Inventory** dialog.
6. (Optional) If you also want to resolve duplicate devices by name and/or address, click **Devices** to open the **Duplicate Devices** dialog box, where you can specify the conditions when duplicate devices are removed, such as when device names match, MAC addresses match, or both match.

About the Duplicate Device ID dialog

Use this dialog (click **Configure > Services >| Inventory** tab **> Device IDs** button) to set up duplicate device ID handling.

- **Attributes list:** Lists all of the attributes you can choose from to uniquely identify a device.
- **Identity attributes:** Displays the attributes you've selected to uniquely identify a device.
- **Log as a duplicate device ID when:** Identifies the number of attributes that a device must fail to match before it's designated as a duplicate of another device.

- **Reject duplicate identities:** Causes the inventory scanner to record the device ID of the duplicate device and reject any subsequent attempts to scan that device ID. Then, the inventory scanner generates a new device ID.

About the Duplicate Devices dialog

Use this dialog (click **Configure > Services > Inventory** tab **> Devices** button) to specify the name and/or address conditions when duplicate devices are removed from the database. When you have one of the remove duplicate options checked, duplicates are allowed in the database, but they are removed the next time database maintenance happens.

- **Remove duplicate when:**
  - **Device names match:** Removes the older record when two or more device names in the database match.
  - **MAC addresses match:** Removes the older record when two or more MAC addresses in the database match.
  - **Both device names and MAC addresses match:** Removes the older record ONLY when two or more device names and MAC addresses (for the same record) match.
- **Restore old device IDs:** Restores the original device ID from the older record of a scanned device, *if* two records for that device exist in the database and at least one of the remove options above is selected and its criteria met. The original device ID is restored when the next inventory maintenance scan runs. This option has no effect unless one of the remove options above is selected.

Configuring the scheduler service

Use the **Scheduler** tab to configure the scheduler service (**Tools > Distribution > Scheduled tasks**) for the core server and database you selected using the **General** tab.

You must have the appropriate rights to perform these tasks, including full administrator privileges to the Windows NT/XP/2000/2003 devices on the network, allowing them to receive package distributions from the core server. You can specify multiple login credentials to use on devices by clicking **Change login**.

One additional setting you can configure manually is the **Scheduled task** window's refresh rate. By default, every two minutes the **Scheduled tasks** window checks the core database to determine if any of the visible items have been updated. If you want to change the refresh rate, navigate to this key in the registry:

- HKEY_CURRENT_USER\Software\LANDesk\ManagementSuite\WinConsole

Set "TaskRefreshIntervalSeconds" to the number of seconds between refreshes for an active task. Set "TaskAutoRefreshIntervalSeconds" to the refresh interval for the whole **Scheduled task** window.

About the Configure LANDesk Software Services dialog: Scheduler tab

Use this tab to see the name of the core server and the database that you selected earlier, and to specify the following scheduled task options:

- **User name:** The user name under which the scheduled tasks service will be run. This can be changed by clicking the **Change login** button.
- **Number of seconds between retries:** When a scheduled task is configured with multiple retries, this setting controls the number of seconds the scheduler will wait before retrying the task.
- **Number of seconds to attempt wake up:** When a scheduled task is configured to use Wake On LAN, this setting controls the number of seconds that the scheduled tasks service will wait for a device to wake up.

- **Interval between query evaluations:** A number that indicates the amount of time between query evaluations, and a unit of measure for the number (minutes, hours, days, or weeks).
- **Wake on LAN settings:** The IP port that will be used by the Wake On LAN packet set by the scheduled tasks to wake up devices.
- **Status of scheduler service:** Indicates whether the scheduler service is started or stopped on the core server.
  - **Start:** Starts the service on the core server.
  - **Stop:** Stops the service on the core server.
  - **Restart:** Restarts the service on the core server.
- **Advanced:** Displays the **Advanced scheduler settings** dialog. You can change scheduler-related advanced settings here. As you click each item, help text appears at the bottom of the dialog explaining each option. The default values should be fine for most installations. To change a setting, click it, click **Edit**, enter a new value, then click **OK**. Restart the scheduler service when you're done.

About the Configure LANDesk Software Services dialog: Change login dialog

Use the **Change login** dialog (click **Change login** on the **Scheduler** tab) to change the default scheduler login. You can also specify alternate credentials the scheduler service should try when it needs to execute a task on unmanaged devices.

To install LANDesk agents on unmanaged devices, the scheduler service needs to be able to connect to devices with an administrative account. The default account the scheduler service uses is LocalSystem. The LocalSystem credentials generally work for devices that aren't in a domain. If devices are in a domain, you must specify a domain administrator account.

If you want to change the scheduler service login credentials, you can specify a different domain-level administrative account to use on devices. If you're managing devices across multiple domains, you can add additional credentials the scheduler service can try. If you want to use an account other than LocalSystem for the scheduler service, or if you want to provide alternate credentials, you must specify a primary scheduler service login that has core server administrative rights. Alternate credentials don't require core server administrative rights, but they must have administrative rights on devices.

The scheduler service will try the default credentials and then use each credential you've specified in the **Alternate credentials** list until it's successful or runs out of credentials to try. Credentials you specify are securely encrypted and stored in the core server's registry.

Note: Rollup core servers use the scheduler service credentials to authenticate for synchronization. On rollup cores, these scheduler service credentials must be a member of a group with console administrator privileges on the source core servers. If the credentials don't have these privileges, the rollup will fail and you'll see task handler errors in the source core server's synchronization log.

You can set these options for the default scheduler credentials:

- **User name:** Enter the default domain\username or username you want the scheduler to use.
- **Password:** Enter the password for the user name you specified.
- **Confirm password:** Retype the password to confirm it.

You can set these options for additional scheduler credentials:

- **Add:** Click to add a new user name and password to the **Alternate credentials** list.
- **Remove:** Click to remove the selected credentials from the list.
- **Modify:** Click to change the selected credentials.

When adding alternate credentials, specify the following:

- **User name:** Enter the username you want the scheduler to use.

- **Domain:** Enter the domain for the username you specified.
- **Password:** Enter the password for the credentials you specified.
- **Confirm password:** Retype the password to confirm it.

Configuring preferred server credentials

There is a **Credentials** button at the bottom of the **Configure LANDesk Software services** dialog box. This button launches the **Preferred servers** dialog, where you can specify the preferred servers that devices will check for software distribution packages. These preferred servers offload demand on the core server and help you distribute network traffic in low-speed WAN environments where you don't want devices downloading packages from off-site servers. Preferred servers work for every delivery method except multicast. UNC package shares work with all packages. HTTP package shares only work with MSI and SWD packages.

Importing and exporting preferred server lists

You can share lists of preferred servers by exporting a list and then importing it on another core server. Lists are saved as LANDesk exported items files, with a .ldms extension.

- **File > Import server list:** Select this option to import an exported items file, with a .ldms extension. Browse in the Select file to import dialog box to select the list, and then click **Open**.
- **File > Export server list:** Select this option to create an exported items file that contains the services currently listed in the Preferred servers list. Specify a file name and browse to the location where you want to save the file, and then click **Save**.
- **File > Copy to other cores:** Select this option to copy custom content (such as configurations, scheduled tasks, software packages, and patch content) directly to other core servers. Select other core servers from the list and click **Copy content**.

Adding servers to the preferred servers list

You can add servers, remove them, and modify server information for the **Preferred servers** list.

- **Edit > Add server:** Opens the **User name and password** dialog, where you specify the following options:
    - **Description:** A description for this preferred server. The description appears in the **Server credentials** dialog.
    - **Server name:** The name of the server that will host packages.
    - **User name:** The user name devices will use to log into the server. This user name should allow only read access for security reasons.
    - **Password/Confirm password:** The password for the user name you specified.
    - **Limit preferred server usage by these IP address ranges:** If you only want devices within a specified IP range to use this preferred server, you can specify the **Starting IP address** and **Ending IP address**, and click **Add**. Select an IP address range and click **Delete** to remove it from this list.
    - **Test credentials:** Click this button to make sure the server name and credentials you entered work correctly.

Note: When controlling preferred server access through IP address ranges, note that devices within the same multicast domain share their configuration files and may use the same servers, even if some of those devices aren't in a particular preferred server's IP address range.

When you have completed the information in this dialog box, click **OK** to save the server information to the **Preferred servers** list.

To modify a server or remove it from the list, select it and click **Edit > Edit selected server** or **Remove selected server**.

Configuring the Custom jobs service

Use the **Custom jobs** tab to configure the custom jobs service for the core server and database you selected using the General tab. Examples of custom jobs include inventory scans, device deployments, or software distributions.

Jobs can be executed with either of two remote execution protocols, TCP or the standard LANDesk agent protocol, CBA. When you disable TCP remote execute as the remote execute protocol, custom jobs uses the standard LANDesk agent protocol by default, whether it's marked disabled or not. Also, if both TCP remote execute and standard LANDesk agent are enabled, the custom jobs service tries to use TCP remote execute first, and if it's not present, uses standard LANDesk agent remote execute.

The **Custom jobs** tab also enables you to choose options for device discovery. Before the custom jobs service can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

About the Configure LANDesk Software Services dialog: Custom jobs tab

Use this tab to set the following custom jobs options:

Remote execute options

- **Disable TCP execute:** Disables TCP as the remote execute protocol, and thereby uses the standard LANDesk agent protocol by default.
- **Disable CBA execute / file transfer:** Disables the standard LANDesk agent as the remote execute protocol. If the standard LANDesk agent is disabled and TCP remote execute protocol is not found on the device, the remote execution will fail.
- **Enable remote execute timeout:** Enables a remote execute timeout and specifies the number of seconds after which the timeout will occur. Remote execute timeouts trigger when the device is sending heartbeats, but the job on the device is hung or in a loop. This setting applies to both protocols (TCP or standard LANDesk agent). This value can be between 300 seconds (5 minutes) and 86400 seconds (1 day).
- **Enable client timeout:** Enables a device timeout and specifies the number of seconds after which the timeout will occur. By default, TCP remote execute sends a heartbeat from device to server in intervals of 45 seconds until the remote execute completes or times out. Device timeouts trigger when the device doesn't send a heartbeat to the server.
- **Remote execute port:** Specifies the port over which the TCP remote execute occurs. The default is 12174. If this port is changed, it must also be changed in the device configuration.

Distribution options

- **Distribute to <nn> computers simultaneously:** Specifies the maximum number of devices to which the custom job will be distributed simultaneously.

Discovery options

- **UDP:** Select UDP to use a LANDesk agent ping via UDP. Most LANDesk device components depend on standard LANDesk agent, so your managed devices should have standard LANDesk agent on them. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping number of **Retries** and a **Timeout** value.

- **TCP:** Select TCP to use an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Select Both to have the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast.
- **Disable DNS/WINS lookup:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

Configuring the Multicast service

Use the **Multicast** tab to configure the multicast domain representative discovery options for the core server and database you selected using the General tab.

About the Configure LANDesk Software Services dialog: Multicast tab

Use this tab to set the following multicast options:

- **Use multicast domain representative:** Uses the list of multicast domain representatives stored in the network view's **Configuration > Multicast domain representatives** group.
- **Use cached file:** Queries each multicast domain to find out who might already have the file, therefore not needing to download the file to a representative.
- **Use cached file before preferred domain representative:** Changes the order of discovery to make **Use cached file** the first option attempted.
- **Use broadcast:** Sends a subnet-directed broadcast to find any device in that subnet that could be a multicast domain representative.
- **Log discard period:** Specifies the number of days that entries in the log will be retained before being deleted.

Configuring the OS deployment service

Use the **OS deployment** tab to designate PXE representatives as PXE holding queues, and to configure basic PXE boot options for the core server and database you selected using the General tab.

PXE holding queues are one method of deploying OS images to PXE-enabled devices. You designate existing PXE representatives (located in the **Configuration** group in the network view) as PXE holding queues. For more information, see "PXE-based deployment" on page 211.

Select and move PXE representatives from the **Available proxies** list to the **Holding queue proxies** list.

About the Configure LANDesk Software Services dialog: OS Deployment tab

Use this tab to assign PXE holding queue proxies (representatives), and to specify the PXE boot options.

- **Available proxies:** Lists all available PXE proxies on your network, identified by device name. This list is generated when the inventory scanner detects PXE software (PXE and MTFTP protocols) running on the device.
- **Holding queue proxies:** Lists the PXE proxies that have been moved from the **Available proxies** list, thereby designating the proxy as a PXE holding queue. PXE-enabled devices on the same subnet as the PXE holding queue proxy will be

automatically added to the **PXE holding queue** group in the console's network view when they PXE boot. The devices can then be scheduled for an image deployment job.

- **Reset:** Forces all of the PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the **PXE holding queue** group in the console's network view. The devices can then be scheduled for an imaging job. (The Reset button is enabled when you select a PXE proxy in the Holding queue proxies list).

Note: Changes you make here to the PXE boot options will not take effect on any of your PXE representatives until you run the PXE Representative Deployment script on that representative.

- **Timeout:** Indicates how long the boot prompt displays before timing out and resuming the default boot process. The maximum number of seconds you can enter is 60 seconds.
- **Message:** Specifies the PXE boot prompt message that appears on the device. You can type any message you like in the text box, up to 75 characters in length.

Validating your OS deployment preboot environment

There is an **OSD Validation** button at the bottom of the **Configure LANDesk Software services** dialog box. Click this to open the **OSD imaging environment** dialog box, with which you can validate your license to use a DOS or Windows preboot environment for OS deployment.

About the OSD imaging environment dialog

Use the **OSD imaging environment** dialog to validate your license to use a DOS or Windows preboot environment. (No validation is required for using a Linux preboot environment.) License validation requirements are as follows:

- **DOS:** License verification requires a Windows NT 4 server CD and a Windows 98 CD. This 7 MB image is the smallest one, reducing the network bandwidth used. It potentially is the slowest at creating and restoring images, and has lower hardware compatibility than the other imaging solutions.
- **Windows PE:** License verification requires that you install the Windows Automated Installation Kit (WAIK) available from Microsoft. The OSD imaging environment dialog box includes a link to download the WAIK in a .iso image, which you then need to burn to a DVD or mounted as a disk image with a drive emulator. The Windows PE is the largest environment. It has the best hardware compatibility and is potentially the fastest at creating and restoring images.

To validate a DOS PE environment

1. Click the **OSD Validation** button at the bottom of the **Configure LANDesk Software services** dialog box. (If you are using the OS deployment tool, click the **Validate licenses** button on the toolbar.)
2. In the **DOS imaging environment** section, click **Validate now**.
3. Insert a Windows NT4 server install CD in a drive. Click **Browse** and select the \CLIENTS\MSCLIENT\DISKS folder on the CD.
4. Click **OK**. The validation process accesses files on that CD. When finished, it prompts for the next CD.
5. When prompted, insert a Windows 98 install CD into a drive. Click **Browse** and select the \WIN98 folder on the CD.
6. Click **OK**. The validation process will continue, and when complete, click **OK**.

To validate a Windows PE environment

1. Click the **OSD Validation** button at the bottom of the **Configure LANDesk Software services** dialog box. (If you are using the OS deployment tool, click the **Validate licenses** button on the toolbar.)
2. In the **Windows PE imaging environment** section, click **Validate now**.
3. Click the link to download the WAIK. At the download dialog box, save the .iso image to a location on your core server.
4. Burn the .iso image to a DVD, or make it accessible from your hard disk drive by using a drive emulator.
5. Run the WAIK install from the DVD or image, using the default settings.
6. When it is installed, return to the **Windows PE imaging environment validation** dialog box and click **Next**.
7. Click **Browse** and select the location where you installed WAIK. Click **OK**.
8. Click **Next**. The validation process will continue, and when you see the success message, click **Finish**.

Information about downloading and installing the WAIK is available in a LANDesk Support Community document at http://community.landesk.com/support/docs/DOC-6794.pdf.

To select a default preboot environment

1. After you have validated the preboot environments you want to use, return to the OSD imaging environment dialog box.
2. From the **Default preboot environment** list, select **DOS**, **Linux**, or **Windows** as your default preboot environment.
3. Click **OK**.

Configuring the BMC password

Use the **BMC password** tab to create a password for the IPMI Baseboard Management Controller (BMC) on IPMI-enabled devices.

- **Password:** Type the password to be used for the BMC password on IPMI devices.
- **Confirm password:** Retype the password in this text box, then click **Apply** or **OK** to set the password.

The password can be no longer than 15 characters and can contain only numbers 0-9 or upper/lowercase letters a-z.

Configuring OS virtualization credentials

Use the **OS virtualization** tab to enter default credentials for managing VMware ESX servers that are configured as virtual OS hosts. Virtual OS hosts that have been discovered are displayed in the network view in a separate **Virtual OS hosts** folder.

- **User name:** Type the default user name
- **Password/Confirm password:** Type and confirm the password to be used, then click **Apply** or **OK** to set the credentials.

Configuring device agents

Devices need the Management Suite agents on them to be fully manageable. Read this chapter to learn about:

The **Agent configuration** window lets you create new agent configurations for Windows, Linux, and Macintosh devices. The agent configurations you create can then be pushed to clients using the console's **Scheduled tasks** window.

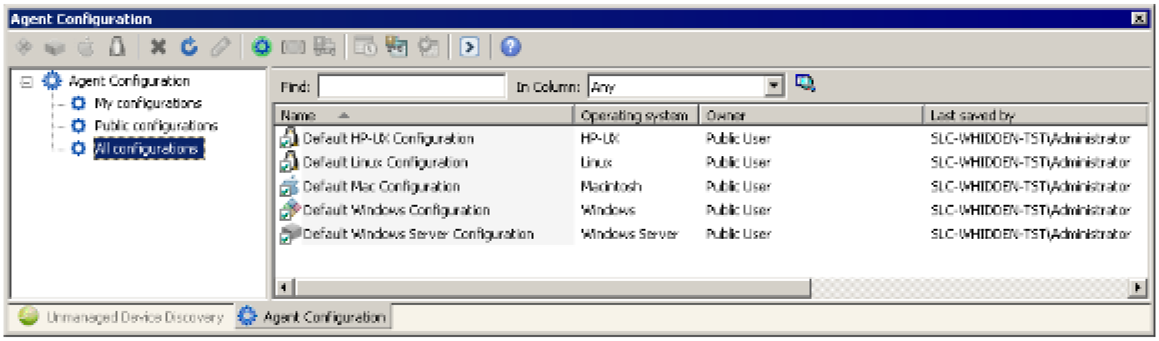
Deploying agents to Windows 95 / 98 / NT devices
Management Suite no longer ships with agents that support Windows 95, Windows 98, or Windows NT devices. You can contact LANDesk Customer Care if you need the legacy agent that works with these devices.

Creating device configurations for Windows devices not enabled for management
If you have Windows devices that are part of a Windows domain, you can push a configuration to those devices even if the standard LANDesk agent and the remote control agents aren't present. For more information, see the deployment documentation on the LANDesk community at http://community.landesk.com.

Working with agent configurations

Management Suite uses agent configurations that you create to deploy agents and agent preferences to managed devices. Once devices have the Management Suite agents on them, you can easily update agent configurations.

The Agent Configuration tool is used to create and update device and server agent configurations (such as what agents are installed on devices and what network protocols the agents use). Different configurations can be created for department or group specific needs. For example, configurations can be created for the devices in the accounting department or for devices using a particular Operating System. For each type of configuration there can only be one default configuration. The default configuration cannot be deleted, but it can be edited. It is a good idea not to have too many different configurations, as this makes support and troubleshooting more complex and time-consuming.



Name	Operating system	Owner	Last saved by
Default HP-UX Configuration	HP-UX	Public User	SLC-WHIDDEN-TST\Administrator
Default Linux Configuration	Linux	Public User	SLC-WHIDDEN-TST\Administrator
Default Mac Configuration	Macintosh	Public User	SLC-WHIDDEN-TST\Administrator
Default Windows Configuration	Windows	Public User	SLC-WHIDDEN-TST\Administrator
Default Windows Server Configuration	Windows Server	Public User	SLC-WHIDDEN-TST\Administrator

Prior to installing any Agent software it is necessary to create an Agent Configuration (or use the default). This involves considerable planning and testing. It is best to deploy the correct configuration the first time - although the agent can be reconfigured and redeployed again if necessary.

An organization may need to have multiple Agent configurations. A laptop system might need a different configuration than a desktop system. In order to avoid deploying the wrong agent to the wrong system, it is important to adopt a sensible naming convention for each Agent configuration.

The security and patch scanner agent is installed by default with the standard LANDesk agent. You can configure security scans to determine how and when the security scanner runs on managed devices and whether to show progress and interactive options to the end user. (The security scanner allows you to check for LANDesk software updates on devices and core servers even if you don't have a LANDesk Security Suite content subscription. With a Security Suite subscription you can take full advantage of the security scanner's capability to scan for and remediate known vulnerabilities, spyware, unauthorized applications, viruses, and other potential security risks.)

Before deploying agents, be sure to see the best known methods for agent deployment on the LANDesk user community Web site at http://community.landesk.com/support/community/systems/agent.

IMPORTANT: When creating agent configurations in mixed-language environments, make sure the agent configuration name is ASCII (English character set). An English core server is compatible with clients using all supported languages.

However, if the agent configuration name uses a non-ASCII characters, such as Japanese, Chinese, or Russian, the agent configuration must be created on a core/console of that same language and will only work on devices using the same language. For example, an agent configuration that includes Japanese characters must be created on a Japanese core, and must be deployed to a Japanese client.

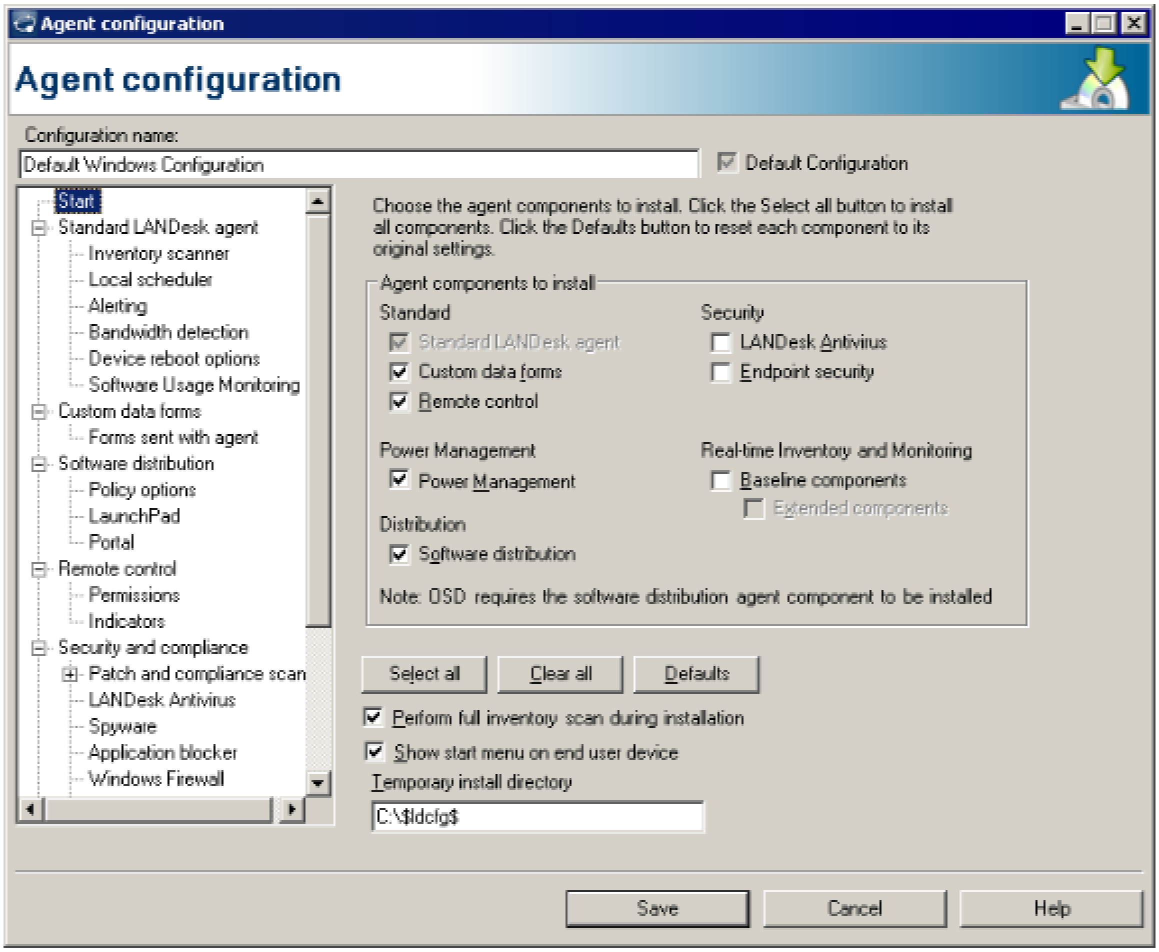
Read the following sections for more information on:

- Creating an agent configuration
- Updating agent preferences on devices
- Creating standalone agent configuration packages

Creating an agent configuration

Use the **Agent configuration** window to create and update device and server agent configurations (such as what agents are installed on devices and what network protocols the agents use).

You can create different configurations for groups' specific needs. For example, you could create configurations for the devices in your accounting department or for devices using a particular operating system.



Agent configuration

Configuration name: Default Windows Configuration

☑ Default Configuration

Choose the agent components to install. Click the Select all button to install all components. Click the Defaults button to reset each component to its original settings.

Agent components to install

Standard
☑ Standard LANDesk agent
☑ Custom data forms
☑ Remote control

Security
☐ LANDesk Antivirus
☐ Endpoint security

Power Management
☑ Power Management

Real-time Inventory and Monitoring
☐ Baseline components
☐ Extended components

Distribution
☑ Software distribution

Note: OSD requires the software distribution agent component to be installed

☑ Perform full inventory scan during installation

☑ Show start menu on end user device

Temporary install directory: C:\$ldcfg$

To push a configuration to devices, you need to:

- **Create the agent configuration:** Set up specific configurations for your devices. An "advance agent configuration" is usually the best choice. For more information, see the next section, "Using the advance agent" on page 78.
- **Schedule the agent configuration:** Push the configuration to devices that have the standard LANDesk agent installed. For more information, see "Scripts and tasks" on page 120. Users with administrative rights can also install the default agent configuration by running WSCFG32.EXE or IPSETUP.BAT from the core server's LDLogon share.

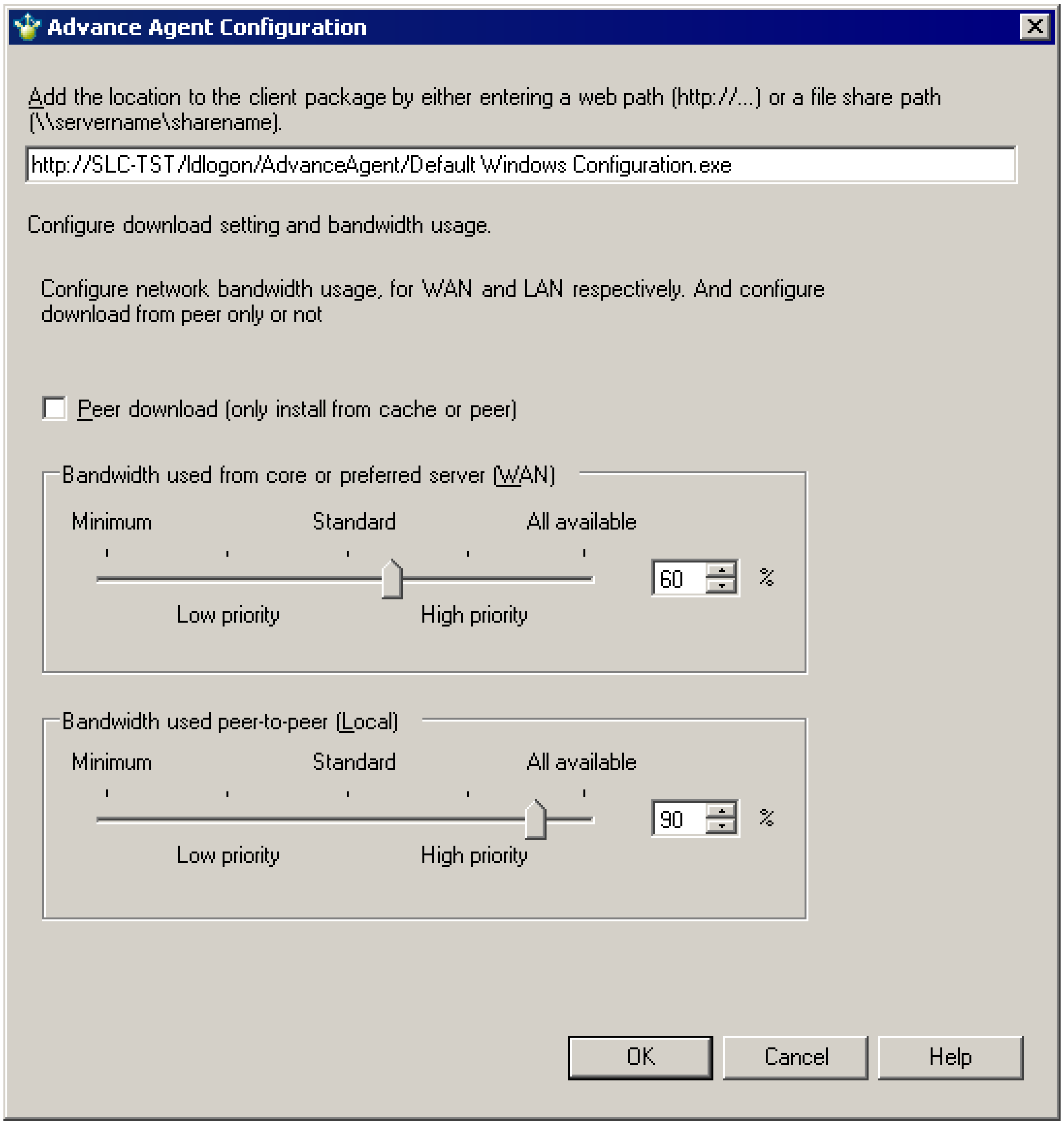
To create an agent configuration

1. In the console, click **Tools > Configuration > Agent configuration**.
2. In the **Agent configuration** tree, click the configurations category you want.
3. Click the **New Windows, New Windows Server, New Macintosh,** or **New Linux** toolbar button.
4. Enter a **Configuration name**.
5. In the **Agent configuration** window's **Start** page, select the agents you want to deploy.
6. Use the tree to navigate the dialogs relating to the options you selected. Customize the options you selected as necessary. Click **Help** for more information if you have questions about a page.
7. Click **Save**.

8. If you want the configuration to be the default (the configuration LDLOGON\WSCFG32.EXE or LDLOGON\IPSETUP.BAT will install), from the configuration's shortcut menu, click **Default configuration**.

Using the advance agent

The Advance agent is the preferred method for deploying the agent in most environments. Advance agent has been created to leverage LANDesk bandwidth-friendly technology during the agent deployment. The Advance agent can reduce the amount of network bandwidth used for Windows-based agent configuration. The Advance agent is a two stage deployment method. The Advance agent is an MSI file that is deployed in advance of the full agent. The MSI installs and then initiates the download and install of the full agent exe package.



Advance Agent Configuration

Add the location to the client package by either entering a web path (http://...) or a file share path (\\servername\sharename).

http://SLC-TST/ldlogon/AdvanceAgent/Default Windows Configuration.exe

Configure download setting and bandwidth usage.

Configure network bandwidth usage, for WAN and LAN respectively. And configure download from peer only or not

□ Peer download (only install from cache or peer)

Bandwidth used from core or preferred server (WAN)

60 %

Bandwidth used peer-to-peer (Local)

90 %

The advance agent works well most devices, including laptops with intermittent or slow network connections. The advance agent doesn't support PDAs and other handheld devices.

The advance agent is a small 500 KB .MSI package. When this package runs on a managed device, it downloads an associated full agent configuration package, which may be up to 15 MB in size, depending on the agents you select. In the **Advance agent configuration** dialog, you can configure what bandwidth-friendly distribution options the .MSI will use for the full agent configuration download.

The advance agent works independently from the core server once it starts downloading the full agent configuration. If a device disconnects from the network before the agent configuration finishes downloading, the advance agent will automatically resume the download once the device is back on the network.

When you create an advance agent configuration, it takes a few seconds for the console to create the full agent configuration package. The console places the advance agent package (<configuration name>.msi) and the newly-created full agent configuration package (<configuration name>.exe) in the core server's LDLogon\AdvanceAgent folder. The file names are based on the agent configuration name.

Once you've created an agent configuration package, you need to run the .MSI portion on devices by using one of the following methods:

- Schedule the small .MSI portion for push distribution.
- Run the .MSI manually on each device.
- Manually configure the .MSI to run via a login script.

Once you deploy the advance agent to devices, the advance agent starts downloading the associated agent configuration. The agent runs silently on the managed device, without showing any dialogs or status updates. The advance agent uses the bandwidth preferences you specified in the **Advance agent configuration** dialog, such as Peer Download and dynamic bandwidth throttling.

Once the .MSI installs and successfully configures agents on a device, it removes the full agent configuration package. The .MSI portion stays on the device and if the same .MSI runs again it won't reinstall the agents.

To create an advance agent configuration

1. Create a Windows-based agent configuration (**Tools > Configuration > Agent configuration**).
2. From that configuration's shortcut menu, click **Advance agent**.
3. Select the options you want.
4. If you select **Peer download**, you must make sure that the advance agent .msi file and the full agent configuration .EXE package are in the software distribution cache of a device in the broadcast domain. If you select **Peer download** and don't do this before deploying the advance agent configuration, the deployment will fail because no cache or peer in the broadcast domain has the necessary files.
5. If you'll be relocating the associated agent configuration package (the .EXE file), change the path for the agent configuration package to match the new location.
6. Click **OK**.
7. If necessary, copy the associated .EXE file from the LDLogon\AdvanceAgent folder to your distribution server. Make sure the path to the agent configuration executable matches the path you specified in the **Advance agent configuration** dialog. You should leave the MSI package on the core server in the default location. Otherwise, the package won't be visible for the advance agent push distribution task below.

To set up an advance agent push distribution

1. In the Agent configuration window (**Tools > Configuration > Agent configuration**), click the **Schedule a push of an advance agent configuration** button.

2. The **Advance agent configurations** dialog lists the agent configurations in the LDLogon\AdvanceAgent folder. Click the configuration you want to distribute and click **OK**.
3. The **Scheduled tasks** window opens with the advance agent task you created selected. The task name is "Advance agent <your configuration name>".
4. Add target devices to the task by dragging them from the **Network view** and dropping then on the task in the **Scheduled tasks** window.
5. From the task's shortcut menu, click **Properties** and schedule the task. You can see the .MSI portion distribution progress in the **Scheduled tasks** window. There are no status updates on the full agent configuration once the .MSI distribution completes.

Updating agent preferences on devices

If you want to update agent preferences on devices, such as requiring permission for remote control, you don't have to redeploy the entire agent configuration. You can make the changes you want in the **Agent configuration** window, and from that configuration's shortcut menu click **Schedule update**. This opens the **Scheduled tasks** window and creates an update task and package for the configuration you scheduled the update from. This package is only a few hundred kilobytes in size.

Updating preferences won't install or remove agents on a device. If the update contains preferences for agents that aren't on a device, the preferences that don't apply will be ignored.

IMPORTANT: Agent Watcher doesn't support preference changes through scheduled updates. If you want to change Agent Watcher preferences, right-click the device you want in the **Network view** and click **Update Agent Watcher settings**.

To update agent preferences on devices

1. Click **Tools > Configuration > Agent configuration**.
2. Customize the configuration you want to use.
3. When you're done, from the configuration's shortcut menu, click **Schedule update to agent settings**. This opens the **Scheduled tasks** window.
4. Target the devices you want to update and schedule the task.

Creating standalone agent configuration packages

Normally the client configuration utility, WSCFG32.EXE, configures clients. If you want, you can have the **Agent configuration** window create a self-extracting single-file executable that installs an agent configuration on the device it's run on. This is helpful if you want to install agents from a CD or portable USB drive, or if you want to multicast an agent configuration.

To create a standalone agent configuration package

1. Click **Tools > Configuration > Agent configuration**.
2. Customize the configuration you want to use.
3. When you're done, from the configuration's shortcut menu, click **Create self-contained client installation package**.
4. Select the path where you want the package stored. Make sure the file name contains only ASCII characters (a-z, A-Z, 0-9).
5. Wait for Management Suite to create the package. It may take a few minutes.

Agent security and trusted certificates

With Management Suite 8, the certificate-based authentication model has been simplified. Device agents still authenticate to authorized core servers, preventing unauthorized cores from accessing clients. However, Management Suite 8 doesn't require a separate certificate authority to manage certificates for the core, console, and each client. Instead, each core server has a unique certificate and private key that Management Suite Setup creates when you first install the core or rollup core server.

These are the private key and certificate files:

- **<keyname>.key:** The .KEY file is the private key for the core server, and it only resides on the core server. If this key is compromised, the core server and device communications won't be secure. Keep this key secure. For example, don't use e-mail to move it around.
- **<keyname>.crt:** The .CRT file contains the public key for the core server. The .CRT file is a viewer-friendly version of the public key that you can view to see more information about the key.
- **<hash>.0:** The .0 file is a trusted certificate file and has content identical to the .CRT file. However, it's named in a manner that lets the computer quickly find the certificate file in a directory that contains many different certificates. The name is a hash (checksum) of the certificates subject information. To determine the hash filename for a particular certificate, view the <keyname>.CRT file. There is a .INI file section [LDMS] in the file. The hash=value pair indicates the <hash> value.

An alternate method for getting the hash is to use the openssl application, which is stored in the \Program Files\LANDesk\Shared Files\Keys directory. It will display the hash associated with a certificate using the following command line:

```
openssl.exe x509 -in <keyname>.crt -hash -noout
```

All keys are stored on the core server in \Program Files\LANDesk\Shared Files\Keys. The <hash>.0 public key is also in the LDLOGON directory and needs to be there by default. <keyname> is the certificate name you provided during Management Suite Setup. During Setup, it's helpful to provide a descriptive key name, such as the core server's name (or even its fully qualified name) as the key name (example: ldcore or ldcore.org.com). This will make it easier to identify the certificate/private key files in a multi-core environment.

You should back up the contents of your core server's Keys directory in a safe, secure place. If for some reason you need to reinstall or replace your core server, you won't be able to manage that core server's devices until you add the original core's certificates to the new core, as described below.

Sharing keys among core servers

Devices will only communicate with core and rollup core servers for which they have a matching trusted certificate file. For example, let's say you have three core servers, managing 5,000 devices each. You also have a rollup core managing all 15,000 devices. Each core server will have its own certificate and private keys, and by default, the device agents you deploy from each core server will only talk to the core server from which the device software is deployed.

There are two main ways of sharing keys among core and rollup core servers:

1. Distributing each core server trusted certificate (the <hash>.0 file) to devices and their respective core servers. This is the most secure way.
2. Copying the private key and certificates to each core server. This doesn't require you to do anything to devices, but since you have to copy the private key, it exposes more risk.

In our example, if you want the rollup core and Web console to be able to manage devices from all three cores, you need to distribute the rollup core's trusted certificate (the <hash>.0) file to all devices, in addition to copying the same file to each core server's LDLOGON directory. For more information, see the next section. Alternatively, you can copy the certificate/private key files from each of the three core servers to the rollup core. This way, each device can find the matching private key for its core server on the rollup core server. For more information, see "Copying certificate/private key files among core servers" on page 82.

If you want one core to be able to manage devices from another core, you can follow the same process, either distributing the trusted certificate to devices or copying the certificate/public key files among cores.

If you are copying certificates between standalone cores (not to a rollup core), there is an additional issue. A core won't be able to manage another core's devices unless it first has an inventory scan from those devices. One way of getting inventory scans to another core is to schedule an inventory scan job with a custom command line that forwards the scan to the new core. In a multiple core scenario, using a rollup core and the Web console is a simpler way to manage devices across cores. Rollup cores automatically get inventory scan data from all devices on the cores that get rolled up to it.

Distributing trusted certificates to devices

There are two ways you can deploy trusted certificates to devices:

1. Deploy a device setup configuration that includes the core server trusted certificates you want.
2. Use a software distribution job to directly copy the trusted certificate files you want to each device.

Each additional core server trusted certificate (<hash>.0) that you want devices to use must be copied to the core server's LDLOGON directory. Once the trusted certificate is in this directory, you can select it within the device setup dialog's **Common base agent** page. Device setup copies keys to this directory on devices:

- Windows devices: \Program Files\LANDesk\Shared Files\cbaroot\certs
- Mac OS X devices: /usr/LANDesk/common/cbaroot/certs

If you want to add a core server's certificate to a device, and you don't want to redeploy device agents through device setup, create a software distribution job that copies < hash>.0 to the directory specified above on the device. You can then use the **Scheduled tasks** window to deploy the certificate distribution script you created.

The following is an example of a custom script that can be used to copy a trusted certificate from the LDLOGON directory of the core server to a device. To use this, replace d960e680 with the hash value for the trusted certificate you want to deploy.

```
; Copy a trusted certificate from the ldlogon directory of the core server
; into the trusted certificate directory of the client
[MACHINES]
REMCOPY0=%DTMDIR%\ldlogon\d960e680.0, %TRUSTED_CERT_PATH%\d960e680.0
```

Copying certificate/private key files among core servers

An alternative to deploying certificates (<hash>.0) to devices is to copy certificate/private key sets among cores. Cores can contain multiple certificate/private key files. As long as a device can authenticate with one of the keys on a core, it can communicate with that core.

When using certificate-based remote control, target devices must be in the core database
If you're using certificate-based remote control security with devices, you can only remote control devices that have an inventory record in the core database that you're connected to. Before contacting a node to launch remote control, the core looks in the database to ensure the requesting party has the right to view the device. If the device isn't in the database, the core denied the request.

To copy a certificate/private key set from once core server to another

1. At the source core server, go to the \Program Files\LANDesk\Shared Files\Keys folder.
2. Copy the source server's <keyname>.key, <keyname>.crt, and <hash>.0 files to a floppy disk or other secure place.
3. At the destination core server, copy the files from the source core server to the same folder (\Program Files\LANDesk\Shared Files\Keys). The keys take effect immediately.

Care should be taken to make sure that the private key <keyname>.key is not compromised. The core server uses this file to authenticate devices, and any computer with the <keyname>.key file can perform remote executions and file transfer to a Management Suite device.

Agent configuration in mixed-language environments

When creating agent configurations in mixed-language environments, make sure the agent configuration name is ASCII (English character set). An English core server is compatible with all supported languages. However, if the agent configuration name uses a non-ASCII characters, such as Japanese, Chinese, or Russian, the agent configuration must be created on a core/console of that same language and will only work on devices using the same language. For example an agent configuration that includes Japanese characters must be created on a Japanese core, and must be deployed to a Japanese client.

Uninstalling device agents

Prior to Management Suite 8.5, anyone could uninstall Management Suite agents by running WSCFG32 with the /u parameter. Since WSCFG32 was in the LDLogon share, which managed devices could access, it was relatively easy for users to uninstall Management Suite agents.

With Management Suite 8.5 and later, the /u parameter has been removed from WSCFG32. There's a new utility called UninstallWinClient.exe in the LDMain share, which is the main ManagementSuite program folder. Only administrators have access to this share. This program uninstalls Management Suite or Server Manager agents on any device it runs on. You can move it to any folder you want or add it to a login script. It's a Windows application that runs silently without displaying an interface.

Running this program won't remove a device from the core database. If you redeploy agents to a device that ran this program, it will be stored in the database as a new device.

Using LANDesk® System Manager with LANDesk® Management Suite

System Manager helps you manage devices on your network and troubleshoot common computer problems before they become serious. If you have devices on your network that you're already managing with System Manager, you can use Management Suite and System Manager integration to manage these computers from the Management Suite console.

Configuring Linux and UNIX device agents

You can use LANDesk Management Suite to manage supported Linux/UNIX distributions.

Read this chapter to learn about:

- Supported Linux/UNIX distributions
- Installing Linux agents
- Installing UNIX agents

- Using the inventory scanner with Linux/UNIX

Supported Linux/UNIX distributions

Supported Linux and UNIX distributions:

- Red Hat Enterprise Linux 3, 4, and 5
- SuSE Linux Professional 9 and 10
- SuSE Linux Enterprise Server 9 and 10
- Ubuntu 8 and 9
- UNIX Hewlett Packard (HP-UX 11/11i)

SUSE Linux and Red Hat Enterprise Linux support these Management Suite features:

- Agent deployment
- Standard LANDesk agent
- Inventory scanning for hardware and software
- Software distribution, including policy support
- Vulnerability scanning and remediation

Ubuntu Linux supports these Management Suite features:

- Agent deployment
- Standard LANDesk agent
- Inventory scanning for hardware and software

Linux runs on a variety of architectures, but the Linux inventory scanner will only run on Intel architecture.

Installing Linux agents

You can remotely deploy and install Linux agents on Linux servers. Your Linux server must be configured correctly for this to work. To install an agent on a Linux server, you must have root privileges.

The default Red Hat Enterprise Linux AS and ES install includes the RPMs that the Linux standard agent requires. For the complete list of RPMs that the product requires, see the list later in this chapter.

For an initial Linux agent configuration, the core server uses an SSH connection to target Linux servers. You must have a working SSH connection with username/password authentication. This product doesn't support public key/private key authentication. Any firewalls between the core and Linux servers need to allow the SSH port. Consider testing your SSH connection from the core server with a 3rd-party SSH application.

The Linux agent installation package consists of a shell script, agent tarballs, .INI agent configuration, and agent authentication certificates. These files are stored in the core server's LDLogon share. The shell script extracts files from the tarballs, installs the RPMs, and configures the server to load the agents and run the inventory scanner periodically at the interval you specified in the agent configuration. Files are placed under /usr/LANDesk.

Use the Configure Services (**Tools > Configure Services**) dialog to enter the SSH credentials you want the scheduler service to use as alternate credentials. The scheduler service uses these credentials to install the agents on your servers. You should be prompted to restart the scheduler service. If you aren't, click **Stop** and then **Start** on the **Scheduler** tab to restart the service. This activates your changes.

Deploying the Linux agents

After you've configured your Linux servers and added Linux credentials to the core server, you must create a Linux agent configuration, and then use unmanaged device discovery to discover your Linux servers. You can then add the discovered servers to the **My devices** list so you can deploy the Linux agents. Before you can deploy to a server, you must add it to the **My devices** list. Do this by discovering your Linux server with unmanaged device discovery.

To create a Linux agent configuration

1. In **Tools > Configuration > Agent configuration**, click the **New Linux** button.
2. Enter a **Configuration name**.
3. On the **Start** page, the Standard LANDesk agent, remote control, and software distribution agents are installed by default. If you want to install the **LANDesk vulnerability scanner**, check that box.
4. On the **Standard LANDesk agent** page, select the **Trusted certificates for agent authentication** that you want installed. For more information, see Agent security and trusted certificates.
5. Click **Save**.

To discover your Linux servers and deploy a configuration to them

1. In **Tools > Configuration > Unmanaged Device discovery**, create a discovery job for each Linux server. Use a standard network scan and enter the Linux server's IP address for the starting and ending IP ranges. If you have many Linux servers, enter a range of IP addresses. Click **Scan now** once you've added your discovery IP ranges.
2. When the task finishes, verify that unmanaged device discovery found the Linux servers you want to manage.
3. In the **Unmanaged device discovery** window, drag the Linux servers onto the Linux configuration that you want in the **Agent configuration** window.
4. Finish scheduling the task in the **Scheduled tasks** window.

To manually pull a Linux agent configuration

1. Create a new Linux configuration using the console or you can use the Default Linux configuration.
2. Create a directory on your Linux device (for example, /mnt/core) .
3. Mount to LDLOGON. You can use the following command to do this:

   ```
   mount –t smbfs –o username=administrator,workgroup=<yourworkgroup>
   //<corename>/ldlogon /mnt/core
   ```

4. Change the directory to /mnt/core.
5. Enter ./linuxpull.sh <configuration name.ini> (where this is the name of the configuration you created).

To uninstall a Linux agent configuration

1. On the Linux device you want to uninstall the agent from, mount <corename>\LDMAIN.
2. From the LDMAIN share, copy linuxuninstall.tar.gz to the Linux device.
3. Extract linuxuninstall.tar.gz.
4. In the extracted folder, run the following command: ./linuxuninstall.sh -f ALL

Required RPMs for Red Hat and SUSE (version # or later)

It is recommended that you store all RPMs in the ...\ManagementSuite\ldlogon\RPMS directory. You can browse to this folder through http://*core name*/RPMS.

Red Hat Enterprise

python

RPM Version:2.2.3-5 (RH3), 2.3.4-14 (RH4)
Binary Version:2.2.3

pygtk2

RPM Version:1.99.16-8 (RH3), 2.4.0-1 (RH4)
Binary Version:

sudo

RPM Version:1.6.7p5-1, Binary Version:1.6.7.p5

bash

RPM Version:2.05b-29 (RH3), 3.0-19.2 (RH4)
Binary Version:2.05b.0(1)-release

xinetd

RPM Version:2.3.12-2.3E, (RH3) 2.3.13-4 (RH4)
Binary Version:2.3.12

mozilla

RPM Version: 1.7.3-18.EL4 (RH4)
Binary Version:1.5

openssl

RPM Version:0.9.7a-22.1 (RH3), 0.9.7a-43.1 (RH4)
Binary Version:0.9.7a

sysstat

RPM Version:4.0.7-4, Binary Version:4.0.7

lm_sensors

RPM Version: 2.6 (this version may not be sufficient to display sensors on newer ASIC machines. Please see the lm_sensors documentation or the web site (http://www2.lm-sensors.nu/~lm78) for more detailed information.

SUSE Linux (SUSE 64)

bash

RPM Version: 2.05b-305.6

mozilla

RPM Version: 1.6-74.14

net-snmp

RPM Version: 5.1-80.9

openssl

RPM Version: 0.9.7d-15.13

python-gtk

RPM Version: 2.0.0-215.1 [note: package name change]

python

RPM Version: 2.3.3-88.1

sudo

RPM Version: 1.6.7p5-117.1

sysstat

RPM Version: 5.0.1-35.1

xinetd

RPM Version: 2.3.13-39.3

lm_sensors

RPM Version: NA (note: this has been incorporated into the kernel for the 2.6 version)

Installing UNIX agents

You have to manually install the UNIX agents. Follow the steps below for your UNIX distribution.

To install the agents on HPUX

You must be logged in as root on the HP-UX machine to perform the installation.

1. From the LDLogon share on the core server machine (c:\Program Files\LANDesk\ManagementSuite\ldlogon), copy the following files to a temporary directory on the HP-UX machine:
   - Default HP-UX Server Configuration.sh — rename file to install.sh
   - Default HP-UX Server Configuration.ini — rename file to install.ini
   - certificate file — this file will have the extension ‘.0’. You can search the ldlogon directory for files matching ‘*.0’ to find the certificate file.
   - unix/hpux/baseclient.tar.gz
   - unix/hpux/vulscan.tar.gz
2. Change the file access permissions by running the following command:
   ```
   chmod +x install.sh
   ```
3. Open install.ini and look for the ServerFQDN line. Take note of the name and exit. Ping the ServerFQDN from the command line to make sure the core server is visible to the client machine with the following command:
   ```
   ping ServerFQDN
   ```
   If you can’t ping the machine, an entry for the core server may have to be added to the /etc/hosts file.
4. Run the install using the following command:
   ```
   ./install.sh install.ini
   ```
5. Modify the PlatformID line in the /etc/vulscan.conf file to match your OS and machine type. This will be necessary for vulnerability scans to properly identify the machine type when scanning. For example:
   ```
   platformid=HP-UX11.31:S800
   ```
6. If the machine is a NIS server, a new NIS services map needs to be generated. This can be done by running the following command:
   ```
   ypmake services.byname
   ```

If the machine is a NIS client machine, the master server and slave servers will need to be updated to include pds and cba service entries inserted into the /etc/services file on the client machine.

To install the agents on Solaris (Intel architecture)

1. From LDLogon\unix\common, copy ldiscnux.conf and ldappl.conf to /etc. Copy ldiscnux.8 to /usr/man/man8. Give ldiscnux.conf read/write access for users. Give ldappl.conf read access for users. Use the UNIX chmod command to assign rights to the files.
2. Edit ldappl.conf to customize the software scanning if desired. See the sample entries in ldappl.conf for more information.
3. From LDLogon\unix\common\solia, copy ldiscnux to a directory that is accessible by the individuals who will be running the application. Usually this is /usr/sbin.
4. If needed, make ldiscnux executable using the chmod command.

To install the agents on Solaris 8 and 9 (SPARC architecture)

- From LDLogon\solsparc, follow the directions in installation.txt.

Required HPUX libraries

Depot packages required beyond the standard OS installation include:

- openssl 0.9.8j: cryptography toolkit implementing SSL
- expat 1.95.8: a C library for parsing XML

Required software dependencies for cba:

- OS-Core.CORE-SHLIBS: /usr/lib/libdld.2
- OS-Core.CORE-SHLIBS: /usr/lib/libc.2
- OS-Core.CORE-SHLIBS: /usr/lib/libcl.2
- OS-Core.CORE-SHLIBS: /usr/lib/libCsup_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libstd_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libpam.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libisamstub.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libm.2
- openssl.OPENSSL-LIB: /usr/lib/libcrypto.sl.0
- openssl.OPENSSL-LIB: /usr/lib/libssl.sl.0

Required software dependencies for pds2d:

- OS-Core.CORE-SHLIBS: /usr/lib/libdld.2
- OS-Core.CORE-SHLIBS: /usr/lib/libc.2
- OS-Core.CORE-SHLIBS: /usr/lib/libcl.2
- OS-Core.CORE-SHLIBS: /usr/lib/libCsup_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libstd_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libpam.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libisamstub.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libm.2

Required software dependencies for ldiscan:

- OS-Core.CORE-SHLIBS: /usr/lib/libdld.2
- OS-Core.CORE-SHLIBS: /usr/lib/libc.2

- OS-Core.CORE-SHLIBS: /usr/lib/libcl.2
- OS-Core.CORE-SHLIBS: /usr/lib/libCsup_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libstd_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libpam.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libisamstub.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libm.2

Required software dependencies for vulscan:

- OS-Core.CORE-SHLIBS: /usr/lib/libdld.2
- OS-Core.CORE-SHLIBS: /usr/lib/libc.2
- OS-Core.CORE-SHLIBS: /usr/lib/libcl.2
- OS-Core.CORE-SHLIBS: /usr/lib/libCsup_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libstd_v2.2
- OS-Core.CORE-SHLIBS: /usr/lib/libpam.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libisamstub.1
- COMPLIBS.LIBISAM-PS32: /usr/lib/libm.2
- expat.expat-RUN: /usr/local/lib/libexpat.sl

Required Solaris libraries

Solaris 8 libraries:

- libstdc++.so.5.0.4 (ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/libgcc-3.3-sol8-sparc-local.gz)
- libexpat.so (ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/expat-1.95.5-sol8-sparc-local.gz)

Solaris 9 libraries:

- libstdc++.so.5.0.5 (ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/libgcc-3.3-sol9-sparc-local.gz)
- libexpat.so (ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/expat-1.95.5-sol9-sparc-local.gz)

Using the inventory scanner with Linux/UNIX

Inventory scanner command-line parameters

The inventory scanner, ldiscan for Linux or ldiscnux for UNIX, has several command-line parameters that specify how it should run. See "ldiscnux -h" or "man ldiscnux" for a detailed description of each. Each option can be preceded by either '-' or '/'.

Parameter	Description
-d=Dir	Starts the software scan in the Dir directory instead of the root. By default, the scan starts in the root directory.
-f	Forces a software scan. If you don't specify -f, the scanner does software scans on the day interval (every day by default) specified in the console under **Configure > Services > Inventory > Scanner Settings**.
-f-	Disables the software scan.

Parameter	Description
-i=ConfName	Specifies the configuration filename. Default is /etc/ldappl.conf.
-ntt=address:port	Host name or IP address of core server. Port is optional.
-o=File	Writes inventory information to the specified output file.
-s=Server	Specifies the core server. This command is optional, and only exists for backward compatibility.
-stdout	Writes inventory information to the standard output.
-v	Enables verbose status messages during the scan.
-h or -?	Displays the help screen.

Examples

To output data to a text file, type:

```
ldiscnux -o=data.out -v
```

To send data to the core server, type:

```
ldiscnux -ntt=ServerIPName -v
```

UNIX inventory scanner files

File	Description
ldiscnux	The executable that is run with command-line parameters to indicate the action to take. All users that will run the scanner need sufficient rights to execute the file. There is a different version of this file for each platform supported above.
/etc/ldiscnux.conf	This file always resides in /etc and contains the following information: • Inventory assigned unique ID • Last hardware scan • Last software scan All users who run the scanner need read and write attributes for this file. The unique ID in /etc/ldiscnux.conf is a unique number assigned to a computer the first time the inventory scanner runs. This number is used to identify the computer. If it ever changes, the core server will treat it as a different computer, which could result in a duplicate entry in the database. **Warning:** Do not change the unique ID number or remove the ldiscnux.conf file after it has been created.

File	Description
/etc/ldappl.conf	This file is where you customize the list of executables that the inventory scanner will report when running a software scan. The file includes some examples, and you'll need to add entries for software packages that you use. The search criteria are based on filename and file size. Though this file will typically reside in /etc, the scanner can use an alternative file by using the -i= command-line parameter.
ldiscnux.8	Man page for ldiscnux.

Console integration

Once a Linux/UNIX computer is scanned into the core database, you can:

- Query on any of the attributes returned by the Linux inventory scanner to the core database.
- Use the reporting features to generate reports that include information that the Linux scanner gathers. For example, Linux will appear as an OS type in the Operating Systems Summary Report.
- View inventory information for Linux computers.
- Distribute software on distributions that support this.

Queries on "System Uptime" sort alphabetically, returning unexpected results
If you want to do a query to find out how many computers have been running longer than a certain number of days (for example, 10 days), query on "System Start" rather than "System Uptime." Queries on System Uptime may return unexpected results, because the system uptime is simply a string formatted as "x days, y hours, z minutes, and j seconds." Sorting is done alphabetically and not on time intervals.

Path to config files referenced in ldappl.conf doesn't appear in the console
ConfFile entries in ldappl.conf file need to include a path.

Supported platforms and functionality

The following table shows which operating system products and versions are supported by Management Suite. Major functionality support is also shown for the various operating systems.

	Microsoft Windows9x and ME	Microsoft Windows NT*, XP, and 2000	Apple Macintosh*	Linux*	Unix
Protocols	TCP/IP	TCP/IP	TCP/IP	TCP/IP	TCP/IP
Console support	No	Yes (MDAC 2.8)	No	No	No
Remote control	Yes	Yes	Yes	Yes	No
Inventory	Yes	Yes	Yes	Yes	Yes
Software distribution	Yes	Yes	Yes	Yes	Yes (RPM only)
LANDesk standard agent	Yes	Yes	Yes	Yes	No

	Microsoft Windows9x and ME	Microsoft Windows NT*, XP, and 2000	Apple Macintosh*	Linux*	Unix
Real-time inventory and monitoring	Yes	Yes	No	Yes	Yes
Software license monitoring	Yes	Yes	Yes	No	No
Vulnerability scanner	Yes	Yes	Yes	Yes	Yes
Operating system deployment	Microsoft Windows 9x and ME are NOT supported.	Yes	Yes	No	No
All other agents	Yes	Yes	Yes	No	No

Managed devices

Management Suite supports the following managed device operating systems (not all operating systems are supported equally):

Microsoft Windows

Supported client platforms:

- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Vista Business/Ultimate/Enterprise SP1 (32-bit and 64-bit)
- Microsoft Windows XP Professional SP1 or SP2 or SP3
- Microsoft Windows XP Professional, x64 Edition
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows NT 4.0 Workstation SP6a
- Microsoft Windows 98 SE
- Microsoft Windows 95 B with Winsock 2

Supported client/server platforms:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2003 SP1 or greater Standard Edition
- Microsoft Windows Server 2003 R2, Standard Edition
- Microsoft Windows Server 2003 SP1 or greater Enterprise Edition
- Microsoft Windows Server 2003 R2 Enterprise Edition
- Microsoft Windows Server 2000 Server SP4
- Microsoft Windows Server 2000 Advanced Server SP4

Linux and UNIX

Supported client platforms:

- Red Hat Enterprise Linux 3, 4, 5 WS
- SUSE Linux Professional 9.1, 10
- Ubuntu

Supported client/server platforms:

- HP-UX 11/11i
- Red Hat Enterprise Linux 3, 4, 5, ES and AS (with or without EM64T)
- SLES 9 SP2, 10 (with or without EM64T)

Mac OS

- Mac OS 10.5, 10.4, 10.3

Client languages supported

The following is a list of supported languages:

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French
- German
- Italian (client only)
- Japanese
- Korean
- Portuguese (Brazilian)
- Russian
- Spanish

Managing inventory

LANDesk Management Suite uses an inventory scanning utility to add devices to the core database and to collect device hardware and software data. You can view, print, and export inventory data. You can also use it to define queries, group devices together, and generate specialized reports.

Read this chapter to learn about:

Inventory

Note: For more information about running the inventory scanner, and inventory scanner troubleshooting tips, see "Appendix: Additional inventory operations and troubleshooting" on page 557.

Inventory scanning overview

The inventory scanner collects hardware and software data and enters it into the core database. When you configure a device with the Agent configuration tool, the inventory scanner is one of the components of the standard Management Suite agent that gets installed on the device. The inventory scanner runs automatically when the device is initially configured. A device is considered managed once it sends an inventory scan to the core database. The scanner executable is named LDISCN32.EXE and supports Macintosh, Linux, and Windows 95/98/NT/2000/2003/XP devices.

There are two types of inventory scans:

- **Hardware scan**: Hardware scans inventory hardware on managed devices. Hardware scans run quickly. You can configure the hardware scan interval in an agent configuration (**Tools > Configuration > Agent Configuration**) that you can deploy to managed devices. By default, hardware scans run each time the device boots.
- **Software scan**: Software scans inventory software on managed devices. These scans take longer to run than hardware scans. Software scans can take a few minutes to complete, depending on the number of files on the managed device. By default, the software scan runs once a day, regardless of how often the inventory scanner runs on the device. You can configure the software scan interval in the **Configure > Services > Inventory** tab.

You can scan a device on demand by finding it in the network view, and from its shortcut menu, and clicking **Inventory scan**.

Note: A device added to the core database using the discovery feature has not yet scanned its inventory data into the core database. You must run an inventory scan on each device for full inventory data to appear for that device.

You can view inventory data and use it to:

- Customize the network view columns to display specific inventory attributes

- Query the core database for devices with specific inventory attributes
- Group devices together to expedite management tasks, such as software distribution
- Generate specialized reports based on inventory attributes

You can also use inventory scans to keep track of hardware and software changes on devices, and generate alerts or log file entries when such changes occur. For more information, see "Tracking inventory changes" on page 97.

Read the sections below to learn more about how the inventory scanner works.

Delta scanning

After the initial full scan is run on a device, the inventory scanner only captures delta changes and sends them to the core database. By sending only changed data, network traffic and data processing times are minimized.

Forcing a full scan

If you want to force a full scan of the device's hardware and software data, you can delete the existing delta scan file and change a setting in the **Configure LANDesk Software Services** applet.

1. Delete the **invdelta.dat** file from the server. A copy of the latest inventory scan in stored locally as a hidden file named invdelta.dat. The LDMS_LOCAL_DIR environment variable sets the location for this file. By default it is in C:\Program Files\LANDesk\LDClient\Data.
2. Add the **/sync** option to the inventory scanner utility's command line. To edit the command line, click **Start > All Programs > LANDesk Management**, right-click the **Inventory Scan** shortcut icon, select **Properties > Shortcut**, then edit the **Target** path.
3. At the core server, click **Start > All Programs > LANDesk > LANDesk Configure Services**.
4. Click the **Inventory** tab, then click **Advanced settings**.
5. Click the **Do Delta** setting. In the **Value** box type **0**.
6. Click **OK** twice, then click **Yes** at the prompt to restart the service.

Scan compression

Inventory scans performed by the Windows inventory scanner (LDISCAN32.EXE) are compressed by default. The scanner compresses full scans and delta scans with approximately an 8:1 compression ratio. Scans are first built completely in memory, then compressed and sent to the core server using a larger packet size. Scan compression requires fewer packets and reduces bandwidth usage.

Scan encryption

Inventory scans are encrypted (TCP/IP scans only). You can disable inventory scan encryption by changing a setting in the LANDesk Configure Services applet.

1. At the core server, click **Start > All Programs > LANDesk > LANDesk Configure Services**.
2. Click the **Inventory** tab, then click **Advanced settings**.
3. Click the **Disable Encryption** setting. In the **Value** box type **1**.
4. Click **Set**, then click **OK**.
5. Click **OK**, then click **Yes** at the prompt to restart the service.

Encrypted data transport

In **Configure > Services > Inventory** tab, there is an **Encrypted data transport** option. This option causes device scans to be sent to the core using SSL. Since the files are sent through the Web service and not the inventory service front end, a NAT address won't be appended to the scan file, even if that option is enabled in the registry.

Viewing inventory data

Once a device has been scanned by the inventory scanner, you can view its system information in the console.

Device inventories are stored in the core database, and include hardware, device driver, software, memory, and environment information. You can use the inventory to help manage and configure devices, and to quickly identify system problems.

You can view inventory data in the following ways:

- "Viewing a summary inventory" on page 96
- "Viewing a full inventory" on page 96

You can also view inventory data in reports that you generate. For more information, see "Reports" on page 113.

Viewing a summary inventory

Summary inventory is found on the device's properties page and provides a quick look at the device's basic OS configuration and system information. The summary also shows the date and time of the last inventory scan so you know how current the data is.

Note: If you added a device to the core database using the discovery tool, its inventory data isn't yet scanned into the core database. You must run an inventory scan on the device for the summary inventory feature to complete successfully.

To view summary inventory

1. In the console's network view, right-click a device.
2. Click **Properties** > **Inventory** tab.

Viewing a full inventory

A full inventory provides a complete listing of a device's detailed hardware and software components. The listing contains objects and object attributes.

To view a full inventory

1. In the console's network view, right-click a **device**.
2. Click **Inventory**.

For detailed information, see "Inventory help" on page 610.

Viewing attribute properties

You can view attribute properties for a device's inventory objects from the inventory listing. Attribute properties tell you the characteristics and values for an inventory object. You can also create new custom attributes and edit user-defined attributes.

To view an attribute's properties, double-click the attribute.

For more information, see "About the Inventory attribute properties dialog" on page 612.

Tracking inventory changes

LANDesk can detect and record changes about the device hardware and software. Tracking inventory changes can help you control your network assets. Inventory change settings let you select which types of changes you want to save and with what severity level. The selected changes can be saved in an inventory history log, the core server's Windows event log, or sent as an AMS alert.

You can view and print a device's history of inventory changes. Additionally, you can export the inventory changes to a .CSV formatted file for analysis using your own reporting tools.

To track and use inventory changes, you must first configure the inventory change settings. You will be able to perform the other inventory changes history tasks:

- "Configuring inventory change settings" on page 97
- "Viewing, printing, or exporting inventory changes" on page 97

Configuring inventory change settings

Note: You must first configure these settings if you want to view, print, or export inventory changes for any devices on your network.

To configure inventory change settings

1. Click **Configure** > **Inventory history**.
2. In the **Inventory change settings** dialog, expand the **Computer** object in the **Current inventory** list, and select the system component you want to track.
3. In the **Log event in** list, select the component's attribute you want to track.
4. Check the appropriate box to specify where to record a change in that attribute. Inventory changes can be recorded in the inventory changes history log, Windows NT event viewer log, or as an AMS alert.
5. Select a severity level from the **Log/Alert severity** drop-down list. Severity levels include: None, Information, Warning, and Critical.
6. Click **OK.**

For more information, see "About the Inventory change settings dialog" on page 612.

Viewing, printing, or exporting inventory changes

To view, print, or export inventory changes

1. In the console's network view, right-click a device.
2. Click **Inventory history**.
3. Click **Print** to print the inventory changes history.
4. Click **Export** to save the inventory changes history as a .CSV file.

For more information, see "About the Inventory changes history dialog" on page 612.

Using custom data forms

LANDesk includes a custom data forms tool (**Tools** > **Configuration > Custom data forms**) that you can use to create and manage forms. Custom data forms provide a way for you to collect information from users and add it to the core database.

Custom data forms are not supported in LANDesk Security Suite
Custom data forms is not available with a LANDesk Security Suite only license. You must have a full LANDesk Management Suite in order to use the custom data forms feature.

The inventory scanner can't gather certain types of personalized user-specific information, such as:

- Where is a user's desk?
- What is a user's asset number?
- What is the user's phone number?

The best way to get this information is directly from your users with custom data forms.

Custom data forms have two main components: the form designer which is used by you to create forms for users to fill out, and the form viewer which is used by users to fill out forms.

Forms can be stored centrally or locally. If they're stored centrally, all users automatically have access to the latest forms because everyone views the same form from the same place. If forms are stored locally, you must ensure that users receive the latest forms.

After a user completes a form, the form viewer stores the results locally in C:\Program Files\LANDesk\LDClient\LDCSTM.DAT. This file contains the results from all of the forms the user has responded to. If the user ever needs to fill out the same form again (for example, if the original form was revised), the form viewer fills in the form with the previously entered data.

The inventory scanner takes the information from each device's LDCSTM.DAT file and adds it to the core database.

Oracle databases are case-sensitive
When creating custom fields with custom data forms (or using any other feature) on an Oracle database, make sure you consistently capitalize field names. For example, data associated with "Cube location" is stored in a different place in the database than data associated with "Cube Location."

Also, make sure custom fields have names that are unique regardless of capitalization. The correct inventory data may not be retrieved if two custom fields have the same name but different capitalization.

For more information about custom data forms, see the following procedures:

- "Creating custom data forms" on page 98
- "Creating a group of forms" on page 99
- "Configuring devices to receive custom data forms" on page 99
- "Filling out forms on the device" on page 100

Creating custom data forms

Follow these steps to create a custom data form.

To create a custom data form

1. Click **Tools > Configuration > Custom data forms**.
2. In the Custom Data Forms window, double-click **Add new form**.
3. Enter a name for the **form**.
4. Enter a description for the form.
5. Click **Add** to open the **Add question** dialog.
6. In the Add Question dialog, type in the **Question text**, **Inventory name**, and **Description.**
7. **S**elect the **Control type.**
8. **S**elect whether you want the field to be required.
9. If you selected the **Edit** control type, click **Finish** to close the **Add question** dialog. The Edit control type lets users type in their own answers to questions in an editable text box. You can add more questions or proceed to step 12.

10. If you selected either of the **Combo box** control types, click **Next** to open the **Add items** dialog. The Combo box control type lets users select their answers from a drop-down list of pre-defined items.
11. In the Add Items dialog, enter an item name and click **Insert** to place the item in the Items list. These items appear in a drop-down list for that question on the form. You can add as many items as you like, then click **Finish**.
12. When you're done adding questions, click **Close** to save the form.

You can right-click on a form to schedule it for distribution to devices.

Creating a group of forms

If you have more than one form that you want to send to devices, you can organize them into a group. Then you can simply schedule the group of forms for distribution. Of course, this is not a required procedure.

When you schedule a group of forms for distribution, the local scheduler reads the contents of the group when it's time to distribute it. In other words, you can still change the contents of the group even after it has been scheduled (as long as the scheduled job hasn't yet occurred).

Note: If a form that is part of a group is later modified or deleted, the group automatically reflects those changes.

To create a group of forms

1. In the **Custom data forms** window, click the **Multiple forms toolbar button.**
2. Enter a name for the new group.
3. Select the forms you want to add to the group from the list of available forms.
4. Click **OK**.

You can right-click on a group of forms to schedule it for distribution to devices.

Configuring devices to receive custom data forms

When you set up devices, you can configure them to receive custom data forms. You must select to install the custom data forms component, and specify custom data form options on the agent configuration dialog. For more information, see "Deploying custom data forms" on page 621.

In the agent configuration dialog, you need to specify how you want to update forms on the device:

- **Automatic update:** If all of the forms are stored centrally (automatic updates), users check a single location for new forms. That way, when a new form is available, all devices looking there have immediate access to it. The disadvantage is that users may see forms that aren't relevant to them.
- **Manual update:** If forms are stored locally (manual updates), you'll need to distribute the forms to the users that need to fill them out. There is less network overhead because each device has its own copy of the form. The benefit of local forms is that you can limit the forms users see to only those that are relevant to them. You copy forms to devices during device setup or with the Scheduled Tasks tool.

You also need to specify when forms will be shown on the device:

- **On startup:** The device's form viewer checks for any new or modified forms each time the device boots. The form viewer launches after the operating system loads. The next time the inventory scanner runs, it sends completed forms to the core database.
- **When the inventory scanner runs:** The inventory scanner starts the form viewer, which checks for any new or modified forms. As soon as users finish filling out the form

and close the form viewer, the scan finishes and the data is entered in the core database.

- **When launched from the LANDesk program folder:** The form viewer can be launched manually from the Management Suite program group. The next time the inventory scanner runs, it sends completed forms to the core database.

You can also use the **Scheduled tasks** window to launch the form viewer on devices at a predefined time. In this scenario, use the **Scheduled tasks** window to first distribute the forms to devices. Make sure to allow enough time to distribute the forms before you use the scheduled task scriptable jobs feature to run the form viewer.

Filling out forms on the device

When the form viewer launches on the device, a list of forms and each form's status displays:

- **New:** Indicates the form has never been filled out by this user.
- **Completed:** Indicates the user has opened this form and filled out, at a minimum, the required fields.
- **Do again:** Indicates the user has completed this form before, but the form has since changed. The user needs to look at the form again and make any necessary changes. Once this is done, the form's status changes to completed.

Once users select a form to fill out and click Open, a simple Form wizard appears. It contains a list of questions and fields for answers. If there are more questions than fit on a page, there are Back/Next buttons. Users can click Help (or press F1) while the cursor is in a field to display a help message generated by the **Description** field in the form designer.

Users must answer any required questions before continuing to the next page or exiting a form. Required questions have a red dot beside them.

The last page of the form wizard has a **Finish** button that users click when they're done. Clicking this button returns users to the **Form selection** dialog where the status message beside the form name is updated.

Using custom data forms on devices running the LANDesk legacy agent
The form designer saves forms in a Unicode format. The form viewer used by the legacy agent on Windows NT and Windows 98 devices can't open a Unicode form and so the viewer displays an error. You can work around this issue by opening the .FRM file on the core where it was created in the Windows Notepad application and saving the file as ANSI. Then the custom data form can be pushed to the legacy device and it will work.

Using an off-core inventory server

Normally, the core server processes inventory scans from managed devices. If you're concerned about the demand this scan processing is placing on your core server, you can install an off-core inventory server. This off-core inventory server contains a special version of the LANDesk Inventory Server service that will accept inventory scans and insert scan data into the database. Once you've configured an off-core inventory server, when the inventory scanner on a Windows-based device pings the core server, the core server replies telling the scanner to send its scan file to the off-core server.

The off-core inventory server only processes scans from Windows-based devices. The core server still processes scans from these devices:

- Macintosh
- Linux
- Unix
- Devices behind a Management Gateway
- Devices running pre-8.7 versions of the inventory scanner

The off-core inventory server has these system requirements:

- Microsoft Windows 2000 Server SP4, Microsoft Windows 2000 Advanced Server SP4, Microsoft Windows 2003 Standard Server, Microsoft Windows 2003 Enterprise Server, Windows Server 2008, Windows XP Professional SP1
- .NET Framework 2.0 or 3.0
- ASP.NET 2.0 or 3.0
- MDAC 2.8 or higher
- Administrator privileges
- Can't install on a core server or rollup core server, but you must already have a core server running elsewhere
- If the device is firewalled, you need to open port 5007

Don't use the inventory Encrypted Data Transport option with off-core inventory servers
The **Configure LANDesk Software Services** dialog's **Inventory** tab has **an Encrypted Data Transport** option. Encrypted transport isn't compatible with off-core inventory servers. If you're using an off-core inventory server, make sure this option is disabled.

To install an off-core inventory server

1. From the device you want to make an off-core inventory server, map a drive to the core server's LDMAIN share and run \Install\Off-Core Inventory Server\Setup. This installs the off-core inventory server. When setup finishes, it will prompt you to reboot. Reboot to finish the installation.
2. From the core server, click **Start > Programs > LANDesk > LANDesk Configure Services**.
3. On the **Inventory** tab, click **Advanced settings**.
4. Click the **Off-core inventory server** option.
5. In the **Value** box, enter the off-core inventory server's computer name and click **Set**.
6. Click **OK**, and on the **Inventory** tab click **Restart** to restart the inventory service.
7. Go to the off-core inventory server, and from the **Services** Control Panel applet, restart the **LANDesk Inventory Server** service.
8. Windows-based device scans will now go to the off-core inventory server.

Note: Any time you make changes on the **Configure LANDesk Software Services** dialog's **Inventory** tab, you need to restart the **LANDesk Inventory Server** service on both the core server and the off-core server. Restarting the off-core service allows it to load the configuration changes you made.

Manage software list

Use the **Manage software list** to configure the files you want scanned or ignored by the inventory scanner. The inventory scanner uses this configuration data to identify your devices' software inventory. The scanner recognizes software applications in three ways:

- Filename
- Filename and size
- Information included in an application's executable file

Note: By default, the inventory scanner only scans for files listed in the Manage software list. If you want to scan all files on devices, you can change the scanning mode to all files. A mode=all scan mode can generate inventory scan files from devices that may be several megabytes in size. After the initial scan, the inventory scanner sends only delta scans, which will be much smaller.

The Manage software tree contains two panes that show the following details.

- **Left pane:** This pane shows a Files tree.
  - **Files:** Displays the categories you can use to organize the files:

    - **To be scanned:** Files that the scanner can identify on devices. This list is prepopulated with descriptions of several thousand applications, providing a baseline of executables that your devices may have installed. You can add files to or exclude files from this list.
    - **To be dispositioned:** Files that have been discovered on devices but are unknown to the scanner. You must move these files into other categories before the scanner can identify them.
    - **To be excluded:** The scanner ignores all occurrences of a file that you move here. If you delete a file from **To be excluded**, it appears in the **To be dispositioned** category.
- **Right pane:** This pane displays the contents of the selected category as defined by the search criteria specified at the top of the pane.

Modifying the Manage software list

You can modify the Manage software list to determine which files are included in or excluded from scans. You can drag files from the right pane to the categories in the left pane. You can also change the properties for any file in the list by selecting it and clicking the **Properties.** toolbar button.

Important: After you have edited the core's Manage software list using any of the procedures below, you must click the **Make available to clients button** to update the product definition files used by the inventory scanner. The next time devices do an inventory scan, the scanner gets the updated product definition files from the core server and applies any changes.

About the File properties dialog

Use this dialog (click **Files >** and the **To be scanned** or **To be dispositioned** category, then click the **New File** toolbar button) to add files to Manage software list.

- **Browse button:** Use this button to directly select a file. Selecting a file this way fills in the Filename and Size fields for you.
- **Filename:** Browse for or enter a filename.
- **Size (in bytes):** Enter the file's size in bytes. Don't use commas or other separators between the digits. If you enter file size of 1, any file with that file name matches.
- **Product name:** Enter the product name the file belongs to.
- **Vendor:** Enter the vendor name for the product that uses the file.
- **Version:** Enter a version name for the file.
- **Action or state:** Select what you want done with the file:
    - **To be scanned:** Add the file to this category to have the inventory scanner look for it on devices.
    - **To be dispositioned:** Add the file to this category if you want to decide later what you want to do with the file.

Dispostioning files

You can disposition files by dragging them to either the **To be scanned** or **To be excluded category** in the Manage software tree.

Excluding files from the To be scanned list

To exclude a file

1. Select the **To be excluded** category under **Files** in the Manage software tree.
2. Click the **New file** toolbar button.
3. Enter the name of the file to be excluded.

4. Click **OK**.

Identifying application files that don't have .exe extensions

The default **To be scanned** list contains descriptions of executables (.exe files only). If you want the scanner to also identify other types of application files (.DLLs, .COMs, .SYSes, and so on), see "Editing the LDAPPL3.TEMPLATE file" on page 563.

Database queries

Queries are customized searches for managed devices. LANDesk Management Suite provides a method for you to query devices that have been scanned into your core database via database queries, as well as a method for you to query for devices located in other directories via LDAP queries. You view, create and organize database queries with the Queries groups in the console's network view. You create LDAP queries with the Directory Manager tool.

For more information on creating and using LDAP directory queries with Directory Manager, see "LDAP queries" on page 108.

Read this chapter to learn about:

- "Queries overview" on page 104
- "Query groups" on page 104
- "Creating database queries" on page 105
- "Running database queries" on page 106
- "Importing and exporting queries" on page 106

Queries overview

Queries help you manage your network by allowing you to search for and organize network devices that are in the core database, based on specific system or user criteria.

For example, you can create and run a query that captures only devices with a processor clock speed of less than 2 GHz, or with less than 1024 MB of RAM, or a hard drive of less than 20 GB. Create one or more query statements that represent those conditions and relate statements to each other using standard logical operators. When the queries are run, you can print the results of the query, and access and manage the matching devices.

Query groups

Queries can be organized into groups in the network view. Create new queries (and new query groups) by right-clicking either the **My queries** group and selecting **New query** or **New group**, respectively.

A Management Suite administrator (user with Management Suite Administrator rights) can view the contents of all of the query groups, including: **My queries**, **Public queries**, and **All queries**.

When other Management Suite users log in to the console, they can see queries in the **My queries**, **Public queries**, and **All queries** groups, based on their device scope.

When you move a query to a group (by right-clicking and selecting **Add to new group** or **Add to existing group**), or by dragging and dropping the query, you're actually creating a copy of the query. You can remove the copy in any query group and the master copy of the query (in the **All queries** group) isn't affected. If you want to delete the master copy, you can do it from the **All Queries** group.

For more information on how query groups and queries display in the network view, and what you can do with them, see "Understanding the network view" on page 15.

Creating database queries

Use the **New query** dialog to build a query by selecting from attributes, relational operators, and the attribute's values. Build a query statement by choosing an inventory attribute and relating it to an acceptable value. Logically relate the query statements to each other to ensure they're evaluated as a group before relating them to other statements or groups.

To create a database query

1. In the console's network view, right-click the **My queries** group (or **Public queries**), if you have the public query management right, and then click **New query**.
2. Enter a unique name for the query.
3. Select a **component** from the inventory attributes list.
4. **Select a relational operator**.
5. Select a **value** from the values list. You can edit a value.
6. Click **Insert** to add the statement to the query list.
7. If you want to query for more than one component, click a **logical operator (AND, OR)** and repeat steps 2-5.
8. (Optional) To group query statements so they're evaluated as a group, select two or more **query statements** and click **Group() .**
9. When you're finished adding statements, click **Save**.

About the New query dialog

Use this dialog to create a new query with the following functions:

- **Name:** Identifies the query in query groups.
- **Machine components:** Lists inventory components and attributes the query can scan for.
- **Relational operators:** Lists relational operators. These operators determine which description values for a certain component will satisfy the query.

The Like operator is a new relational operator. If a user doesn't specify any wild cards (*) in their query, the Like operator adds wildcards to both ends of the string. Here are three examples of using the Like operator:

```
Computer.Display Name LIKE "Bob's Machine" queries for: Computer.Display Name
LIKE "%Bob's Machine%"
Computer.Display Name LIKE "Bob's Machine*" queries for: Computer.Display Name
LIKE "Bob's Machine%"
Computer.Display Name LIKE "*Bob's Machine" queries for: Computer.Display Name
LIKE "%Bob's Machine"
```

- **Display scanned values:** Lists acceptable values for the chosen inventory attribute. You can also manually enter an appropriate value, or edit a selected value, with the Edit values field. If the selected relational operator is Exists or Does Not Exist, no description values are possible.
- **Logical operator:** Determines how query statements logically relate to each other:
  - **AND:** Both the previous query statement AND the statement to be inserted must be true to satisfy the query.
  - **OR:** Either the previous query statement OR the statement to be inserted must be true to satisfy the query.
- **Insert:** Inserts the new statement into the query list and logically relates it to the other statements according to the listed logical operator. You can't choose this button until you've built an acceptable query statement.
- **Edit:** Lets you edit the selected query statement. When you're finished making changes, click the **Update** button.

- **Delete:** Deletes the selected statement from the query list.
- **Clear all:** Deletes all statements from the query list.
- **Query list:** Lists each statement inserted into the query and its logical relationship to the other listed statements. Grouped statements are surrounded by parentheses.
- **Group ():** Groups the selected statements together so they're evaluated against each other before being evaluated against other statements.
- **Ungroup:** Ungroups the selected grouped statements.
- **Filters:** Opens the Query Filter dialog that displays device groups. By selecting device groups, you limit the query to only those devices contained in the selected groups. If you don't select any groups, the query ignores group membership.
- **Select columns:** Lets you add and remove columns that appear in the query results list for this query. Select a component, and then click the right-arrow button to add it to the column list. You can manually edit the Alias and Sort Order text, and your changes will appear in the query results list.
- **Qualifier: The** qualifier button is used to limit the results of one-to-many relationships in the database; without it, you will get the same machine listed numerous times in your result set. For example, if you want to see which version of Microsoft Word is installed on every machine in your organization, you would insert Computer.Software.Package.Name = 'Microsoft Word' in the query box and select Computer.Software.Package.Version in the Select Columns list. However, simply listing the software version will list every version of every piece of software installed on each machine; precisely what you don't want. To solution is to limit (or qualify) the version to only Microsoft Word. Click on the Qualify button and you will be able to insert Computer.Software.Package.Name = "Microsoft Word". This will return only the versions of Microsoft Word.
- **Save:** Saves the current query. When you save a query before running it, the query is stored in the core database and remains there until you explicitly delete it.

Query statements are executed in the order shown
If no groupings are made, the query statements listed in this dialog are executed in order from the bottom up. Be sure to group related query items so they're evaluated as a group; otherwise, the results of your query may be different than you expect.

Running database queries

To run a query

1. In the network view, expand the query groups to locate the query you want to run.
2. Double-click the query. Or, right-click and select **Run**.
3. The results (matching devices) display in the right-hand pane of the network view.

Importing and exporting queries

You can use import and export to transfer queries from one core database to another. You can import:

- Management Suite 8 exported queries
- Web console exported .XML queries

To import a query

1. Right-click the query group where you want to place the imported query.
2. Select **Import** from the shortcut menu.
3. Navigate to the query you want to import and select it.

4. Click **Open** to add the query to the selected query group in the network view.

To export a query

1. Right-click the query you want to export.
2. Select **Export** from the shortcut menu.
3. Navigate to the location where you want to save the query (as an .ldms file).
4. Type a name for the query.
5. Click **Save** to export the query.

LDAP queries

In addition to the ability to query the core database with database queries, Management Suite also provides the Directory Manager tool that lets you locate, access, and manage devices in other directories via LDAP (the Lightweight Directory Access Protocol).

You can query devices based on specific attributes such as processor type or OS. You can also query based on specific user attributes such as employee ID or department.

For information about creating and running database queries from the Queries groups in the network view, see "Database queries" on page 104.

Read this chapter to learn about:

- "Configure LDAP directories" on page 108
- "About the Directory manager window" on page 109
- "Creating LDAP directory queries" on page 109
- "More about the Lightweight Directory Access Protocol (LDAP) " on page 111

Configure LDAP directories

Use the Directory Manager configuration tool to manage the LDAP directories you use with LANDesk Management Suite. The LDAP server, username and password you enter are saved and used when you browse or execute queries to the directory. If you change the password of the configured user in the LDAP directory, you must also change the password in here.

Note: The account you configure here must be able to read the users, computers and groups that you use for management with LDMS.

To configure a new directory

1. Click **Configure > Manage Directories**.
2. Click **Add**.
3. Enter the DNS name of the directory server in the **LDAP://** field.
4. Enter the **User name** and **Password**.

Note: If you are using Active Directory, enter the name as <domain-name>\<nt-user-name>. If you are using another directory service, enter the distinguished name of the user.

5. Click **OK** to save the information. The information you enter is verified against the directory before the dialog closes.

To modify an existing directory configuration

1. Click **Configure > Manage Directories**.
2. Click the directory you want.
3. Click **Edit**.
4. Change the server, username, password as desired
5. Click **OK** to save the information. The information is verified against the directory before the dialog closes

To delete and existing directory configuration

1. Click **Configure > Manage Directories**.

2. Click the directory you want.
3. Click **Delete**.

Note: All LDAP queries using this directory will be deleted when the directory is removed.

About the Directory manager window

Use directory manager to accomplish the following tasks:

- **Manage directory:** Opens the **Directory properties** dialog where you identify and log in to an LDAP directory.
- **Remove directory:** Removes the selected directory from the preview pane and stops managing it.
- **Refresh view:** Reloads the list of managed directories and targeted users.
- **New query:** Opens the **LDAP query** dialog where you can create and save an LDAP query.
- **Delete query:** Deletes the selected query.
- **Run query:** Generates the results of the selected query.
- **Object properties:** See the properties for the selected object.

Using directory manager, you can drag LDAP groups and saved LDAP queries onto scheduled tasks, making them task targets.

The directory manager window consists of two panes: a directory pane on the left and a preview pane on the right.

Directory pane

The directory pane displays all registered directories and users. As an administrator, you can specify the name of a registered directory and see a list of queries that are associated with the directory. You can create and then save new queries for a registered directory with a right mouse click or by using drop-down menus. After creating a query, you can drag and drop it to the **Scheduled tasks** window so that the task is applied to users who match the query.

Preview pane

When you select a saved query in directory manager's directory pane on the left side of the dialog, the policies targeted to that query appear in the preview pane on the right side. Likewise, when an individual LDAP user is selected in the directory pane, the policies targeted to that user appear in the preview pane.

- **Registered directory:** Query groups item and Browse item.
- **Query groups:** Queries associated with the directory.
- **Query:** Provides details about the query.
- **Browse and directory items:** Sub-items in the directory.

Creating LDAP directory queries

To create and save a directory query

The task of creating a query for a directory and saving that query is divided into two procedures:

To select an object in the LDAP directory and initiate a new query

1. Click **Tools > Distribution > Directory Manager**.

2. Browse the **Directory Manager** directory pane, and select an object in the LDAP directory. You'll create an LDAP query that returns results from this point in the directory tree down.
3. From directory manager, click the **New query** toolbar button. Note that this icon only appears when you select the root organization (o) of the directory tree (o=my company) or an organizational unit (ou=engineering) within the root organization. Otherwise, it's dimmed.
4. The **Basic LDAP query** dialog appears.

To create, test, and save the query

1. From the **Basic LDAP query** dialog, click an attribute that will be a criterion for the query from the list of directory attributes (example = department).
2. Click a comparison operator for the query (=,<=, >=) .
3. Enter a value for the attribute (example department = engineering).
4. To create a complex query that combines multiple attributes, select a combination operator (AND or OR) and repeat steps 1 through 3 as many times as you want.
5. When you finish creating the query, click **Insert**.
6. To test the completed query, click **Test query**.
7. To save the query, click **Save**. The saved query will appear by name under **Saved queries** in the directory pane of directory manager.

About the Basic LDAP query dialog

- **LDAP query root:** Select a root object in the directory for this query (LDAP://ldap.xyzcompany.com/ou = America.o = xyzcompany). The query that you're creating will return results from this point in the tree down.
- **LDAP attributes:** Select attributes for user-type objects.
- **Operator:** Select the type of operation to perform relating to an LDAP object, its attributes, and attribute values including equal to (=), less than or equal to (<=), and greater than or equal to (>=).
- **Value:** Specify the value assigned to the attribute of an LDAP object.
- **AND/OR/NOT:** Boolean operators that you can select for your query conditions.
- **Test query:** Execute a test of the query you've created.
- **Save:** Save the created query by name.
- **Advanced:** Create a query using the elements of a basic LDAP query but in a freeform manner.
- **Insert:** Insert a line of query criteria.
- **Delete:** Delete a selected line of criteria.
- **Clear all:** Clear all lines of query criteria.

About the Save LDAP query dialog

From the **Basic LDAP query** dialog, click **Save** to open the **Save LDAP query** dialog, which displays the following:

- **Choose a name for this query:** Enables you to choose a name for the query you've created.
- **Query Details LDAP Root:** Enables you to create a query using the elements of a basic LDAP query but in a freeform manner.
- **Query Details LDAP Query:** Displays query examples you can use as a guide when creating your own query in freeform.

- **Save:** Enables you to save the created query by name. The query is saved under the **Saved queries** item under the LDAP directory entry in the directory manager directory pane.

About the Directory properties dialog

From the directory manager toolbar, click the **Manage directory** toolbar button to open the **Directory properties** dialog. This dialog enables you to start managing a new directory, or to view properties of a currently managed directory. This dialog also shows the URL to the LDAP server and the authentication information required to connect to the LDAP directory:

- **Directory URL:** Enables you to specify the LDAP directory to be managed. An example of an LDAP directory and the correct syntax is ldap.<companyname>.com. For example, you might type ldap.xyzcompany.com.
- **Authentication:** Enables you to log in as the following user (that is, you specify a user path and name and the user password).

About the Advanced LDAP query dialog

From the **Basic LDAP query** dialog, click **Advanced** to open the **Advanced LDAP query** dialog, which displays the following:

- **LDAP query root:** Enables you to select a root object in the directory for this query. The query that you're creating will return results from this point in the tree down.
- **LDAP query:** Enables you to create a query using the elements of a basic LDAP query but in a freeform manner.
- **Examples:** Displays query examples you can use as a guide when creating your own query in freeform.
- **Test query:** Enables you execute a test of the query you have created.

The **Advanced LDAP query** dialog appears when you select to edit a query that has already been created. Also, if you select an LDAP group in directory manager and then choose to create a query from that point, the **Advanced LDAP query** dialog appears with a default query that returns the users who are members of that group. You can't change the syntax of this default query, only save the query.

More about the Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for accessing and viewing information about users and devices. LDAP enables you to organize and store this information into a directory. An LDAP directory is dynamic in that it can be updated as necessary, and it is distributed, protecting it from a single point of failure. Common LDAP directories include Novell Directory Services* (NDS) and Microsoft Active Directory Services* (ADS).

The following examples show LDAP queries that can be used to search the directory:

- Get all entries: (objectClass=*)
- Get entries containing 'bob' somewhere in the common name: (cn=*bob*)
- Get entries with a common name greater than or equal to 'bob': (cn>='bob')
- Get all users with an e-mail attribute: (&(objectClass=user)(email=*))
- Get all user entries with an e-mail attribute and a surname equal to 'smith': (&(sn=smith)(objectClass=user)(email=*))
- Get all user entries with a common name that starts with 'andy', 'steve', or 'margaret': (&(objectClass=User)(| (cn=andy*)(cn=steve*)(cn=margaret*)))
- Get all entries without an e-mail attribute: (!(email=*))

The formal definition of the search filter is as follows (from RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> > <or> > <not> > <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> > <filter> <filterlist>
- <item> ::= <simple> > <present> > <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> > <approx> > <ge> > <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL > <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL > <value> '*' <starval>
- <final> ::= NULL > <value>

The token <attr> is a string representing an AttributeType. The token <value> is a string representing an AttributeValue whose format is defined by the underlying directory service.

If a <value> must contain one of the characters * or (or), precede the character with the slash (\) escape character.

Reports

Accurate and reliable information is essential to making any business decision. This is as true in IT as in finance. Reporting plays a role in almost every area of IT. Management Suite automates many aspects of reporting. By scheduling reports, information can be delivered to a central Web server, or directly to a user's inbox. Reports can be produced in a variety of formats, i.e., spreadsheet, Adobe PDF, HTML links, Rich Text files, .CSV, or XML format.

The reporting tool can be used to generate a wide variety of specialized reports that provide critical information about the devices on your network. The reporting tool takes advantage of Management Suite inventory scanning utility, which collects and organizes hardware and software data, in order to produce useful, informative, and up-to-date reports. The reporting console is also used independently of Management Suite as a reporting tool for third party programs that are connected to a database.

Several types of reports are available:

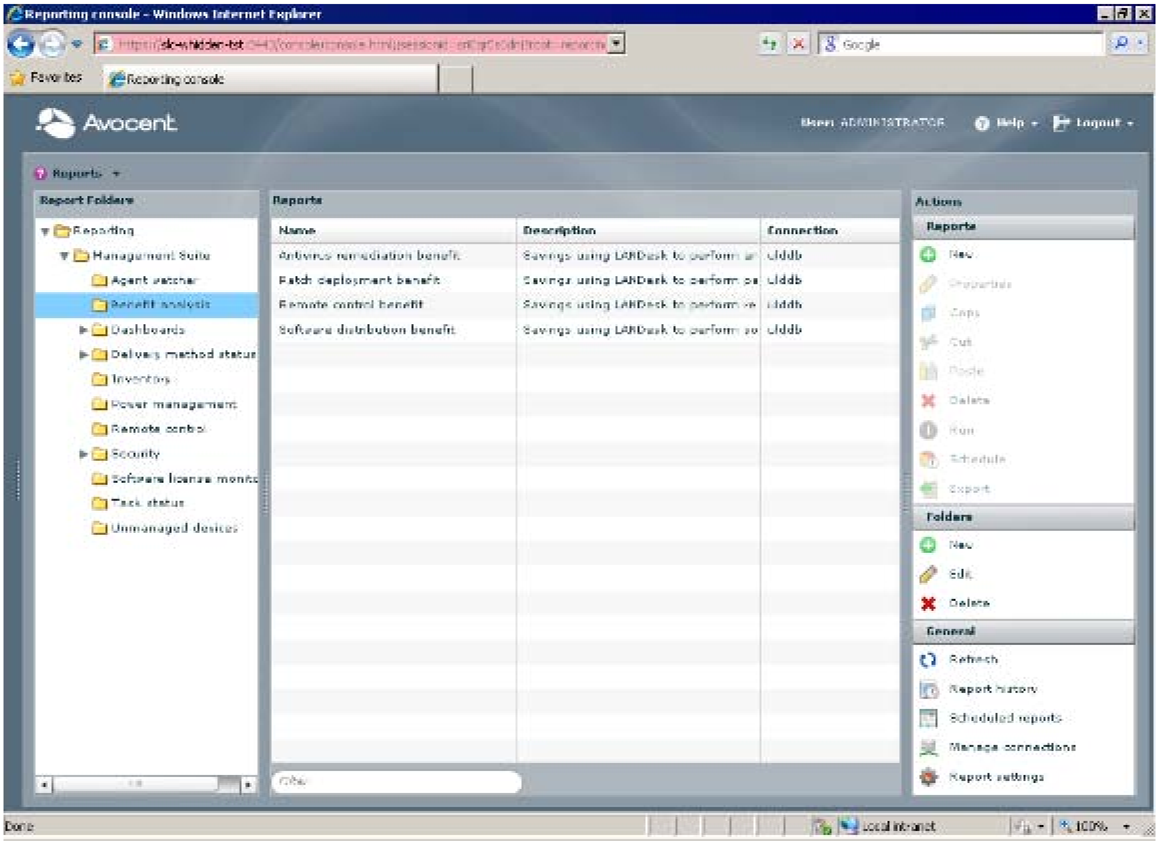
- **Standard (predefined) reports:** Default reports that ship with Management Suite.
- **Custom reports:** Custom reports created through Jaspersoft iReport that enable defining a unique set of information to generate a report. You can also customize any of the standard reports.
- **Ad-hoc reports:** One-click reports available from various areas of Management Suite.
- **Query-based reports:** One-click reports based on a query. Right-clicking a query and clicking **New report** creates a report under **Reporting > Auto generated** based on the query and named after it.

Additionally, you can schedule reports so they run at an interval you specify and you can also e-mail reports directly to users.

Read this chapter to learn about:

Using the reporting console

The reporting console is a Java-based application that works independently of Management Suite and can be used with third party programs. The reporting console runs off a centralized program called Avocent Management Platform (AMP) to accommodate reporting needs for any organization. In conjunction with iReport from Jaspersoft, full customization is possible with all reports inside the reporting console.



Name	Description	Connection
Antivirus remediation benefit	Savings using LANDesk to perform ar	Ulddb
Patch deployment benefit	Savings using LANDesk to perform pa	Ulddb
Remote control benefit	Savings using LANDesk to perform re	Ulddb
Software distribution benefit	Savings using LANDesk to perform so	Ulddb

To launch the reporting console from the Windows console

- Click **Tools > Reporting / Monitoring > Reports**.

To run the reporting console from a supported browser anywhere

- Use the following direct access URL. You'll need to replace <core name> with your core server name.

  https://<core name>:8443/console/console.html?root=reporting

The **Reports** section of the Reporting console is where the main body of reports is accessed. The **Reports** section is modeled after Windows Explorer on how the files are organized and accessed. It is organized into the following sections:

- **Report Folders:** (Left pane) Shows the reporting folder structure. Use this for navigation.
- **Reports:** (Middle pane) Shows reports in the selected folder.
- **Actions:** (Right pane) A toolbar that shows you what you can do with the current selection. Click an item that isn't dimmed to perform that action.

The standard reports that are included with Management Suite are filed under the **Reporting > Management Suite** folder. Auto-generated folders appear when you create a report from queries in Management Suite.

When running a report, you can choose from one of these formats:

- HTML: Standard HTML. You can often click on charting tools (such as pie charts) in HTML reports to get more detailed information about an item.

- PDF: Adobe PDF
- XLS: Microsoft Excel format
- CSV: Comma-separated value text file
- RTF: Rich-text format

Note: The PDF report format doesn't display double-byte characters correctly, such as Japanese. If you need a double-byte report in PDF format, choose an HTML format and generate a PDF from that using a third-party PDF generator.

If there's a default application associated with the selected file extension, the report opens in that application. If the file extension doesn't have a default association, you'll be prompted to save the file.

To run a report

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. In the **Reports** table, select a report to run.
3. Click the **Actions** panel > **Reports** heading > **Run**.
4. When the **Run report** dialog opens, enter or edit the information.
5. Click the **OK** button.

To run a query-based report

1. From the **Network view**, right-click the query you want a report for and click **New report**.
2. A dialog appears saying the report was created. Click **Yes** so the reporting console launches.
3. In the reporting console's **Report folders** panel, click **Reporting > Auto generated**. Your new report appears in this list. Double-click it to run it.

You can also run reports on most Windows console tree view items that are groups or containers. These "view as" reports contain information about the item you generated the report from. For example, running a report from a group in the **Network view** shows a list of devices in that group.

To run a "view as" report from the Windows console

1. Right-click a tree item, such as a group in the **Network view** or **My packages** in the Distribution packages tool.
2. If there's a **View as** menu item, click it and click the report format you want. If there's no **View as** menu item, what you right-clicked doesn't support "View as" reports.

Importing and exporting reports

You can import and export reports. This is helpful if you want to share report templates with others. If you've deleted some default reports and later decide you want them back, you can also re-import them.

Reports are stored in plain-text XML files with a .jrxml file extension. You can find them in this folder:

- C:\Program Files\Avocent\Management Platform\reporting\definition\managementsuite

The folder and file names generally match the way they appear in the reporting console.

To export a report

1. In the **Reports** content panel, select a folder from the **Report folders** column.

2. In the **Reports** table, select a report to export.
3. Click the **Actions** panel > **Reports** heading > **Export**.
4. When the window opens, go to the location where you want to export the report to and click **Save**.

To import a report in Internet Explorer

1. In the **Reports** content panel, select a folder. **Important:** The reports must be in a folder under the **Reporting** folder. If needed create a new folder for the report.
2. Click the **Actions** panel > **Reports** heading > **New**.
3. When the **Report properties** dialog opens, enter the information. **Important**: You must enter the path to the report file to add the new report.
4. Click the **OK** button.

Unlike Internet Explorer, Firefox doesn't support browsing for files with the standard file browser dialog. In Firefox, you'll instead need to open the .jrxml file you want in Notepad, copy the text to the clipboard, and paste it into the **Report properties** dialog's **Report definition** box.

To import a report in Firefox

1. In the **Reports** content panel, select a folder. **Important:** The reports must be in a folder under the **Reporting** folder. If needed create a new folder for the report.
2. Click the **Actions** panel > **Reports** heading > **New**.
3. When the **Report properties** dialog opens, enter the information. **Important**: For the **Report definition**, you must open the .jrxml file you want to import in a text editor, copy all of the text to the Windows clipboard, and paste the text into the **Report definition** box.
4. Click the **OK** button.

Scheduling reports

If there's a report you need regularly, you can schedule it to run ahead of time or during off-hours when the core database load may be lighter. You can view scheduled reports from the reporting console's **Report history** dialog or you can have the reporting console e-mail the report to e-mail addresses you specify. E-mailing reports requires an SMTP mail server.

Each time a scheduled report runs, the report uses the scope of the person who originally scheduled it.

To enter SMTP mail server information

1. In the **Reports** content panel, click the **Actions** panel > **General** heading > **Report settings**.
2. Enter the SMTP server information.
3. Click **OK**.

To schedule a report

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. In the **Reports** table, select a report to schedule.
3. Click the **Actions** panel > **Reports** heading > **Schedule**.
4. When the **Schedule report** dialog opens, enter or edit the information.
5. Click the **OK** button.

To view the scheduled reports

1. In the **Reports** content panel, click the **Actions** panel > **General** heading > **Scheduled reports**.
2. When the **Scheduled reports** dialog opens, view the information in the table.
3. Click the **OK** button.

Viewing the report history

The report history is a log of all reports that have been run. You can filter the history by date range or by text in the report name. If you double-click a report in the history it will display that report again. Every time a report runs it generates a temporary file on the core server and a history log entry. Periodically you should delete entries in the report history. When you delete an entry, the associated temporary file gets deleted too.

To view the report history

- In the reporting console's **Actions** panel, click **Report history**.

To delete report history entries

1. In the **Report history** dialog, select the entries you want to delete. You can hold down Ctrl while clicking to select multiple entries, or you can click the first item in a range and then hold down Shift while you click the last item. This will select the whole range.
2. Click **Delete**.
3. Click **Yes** to delete the selected entries and their associated temporary files.

Working with the reports tree

In the reporting console, you can copy, cut, paste, and delete reports. You can also add, edit, and delete folders.

Working with reports

To copy a report

Copying a report is useful when you have a report that is similar to the report you need. You can copy the report, paste the report, and then modify the pasted report.

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. In the **Reports** table, select a report to copy.
3. Click the **Actions** panel > **Reports** heading > **Copy**.

The report is copied to memory and is available to be pasted to another location. The **Paste** action is also enabled.

To cut a report

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. In the **Reports** table, select a report to cut.
3. Click the **Actions** panel > **Reports** heading > **Cut**.

The report is removed from the report list, copied to memory, and is available to be pasted to another location.

To paste a report

Pasting a report is useful when you have a report is similar to the report you need. You can copy the similar report, paste the report, and then modify the pasted report.

1. Cut or copy a report.
2. Move to the report folder where you want to paste the report.
3. Click the **Actions** panel > **Reports** heading > **Paste**.

The report is pasted to the report folder.

To delete report

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. In the **Reports** table, select a report to delete.
3. Click the **Actions** panel > **Reports** heading > **Delete**.
4. At the confirmation prompt, click **Yes**.

The report is deleted.

Working with report folders

To add a new folder

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. Click the **Actions** panel > **Folders** heading > **New**.
3. When the **Folder properties** dialog opens, enter the information.
4. Click the **OK** button.

The report folder is displayed in the **Report folders** content panel.

To edit a folder

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. Click the **Actions** panel > **Folders** heading > **Edit**.
3. When the **Folder properties** dialog opens, edit the information.
4. Click the **OK** button.

The report folder is updated in the **Report folders** content panel.

To delete a folder

1. In the **Reports** content panel, select a folder from the **Report folders** column.
2. Click the **Actions** panel > **Folders** heading > **Delete**.
3. At the warning prompt, click **Yes** to delete the folder, its sub folders and reports.

The folder is deleted from the **Report folders** content panel.

Managing reports for multiple cores

If you have multiple cores on your network, you don't have to manage reports separately on each core. You can pick a single core and configure the report to run against the core server you choose. The **Run report** dialog that appears when you double-click a report has a **Connection** list that you can use to choose which core server database the report runs against. You'll have to add a connection for each core server that you want to run reports on.

To add a connection to a core server that uses the default SQL database included with Management Suite

1. In the reporting console's **Actions** panel, click Manage connections.
2. Click **New**.
3. Enter a **Connection name** and **Description**.
4. For SQL databases, in **the JDBC drivers** list click **com.microsoft.sqlserver.jdbc.SQLServerDriver**.
5. In the **Server address** field, enter the remote core server address in the format of **<core name>\ldmsdata**.
6. In the **Database (service) name** field, enter **ulddb**.
7. In the **Username** field, enter **sa**.
8. In the **Password** field, enter the database password you provided during the core server installation.
9. Click **Test** to make sure the connection works.
10. Click **OK**. You can now select this connection when you run a report.

If the core server you're connecting to doesn't use the default database included with Management Suite, you'll need to change the field values to match your database installation.

To manage connections

Important: Changing a report's default connection does not change any scheduled report's default connections.

1. In the **Reports** content panel, click the **Actions** panel > **General** heading > **Manage connections**.
2. When the **Connections** dialog opens, view the information in the table.
3. Click **New**, **Edit**, or **Delete** and complete the dialog that appears. When **New** or **Edit** is clicked, the dialog opens. Enter or edit the applicable information.
4. Click the **OK** button.

The connection is updated in the **Connections** dialog.

Creating and editing custom reports

All reports in the reporting console are created by Jaspersoft's iReport program. You can customize the report appearance, underlying SQL query statements, and so on by using iReport. For more information on using iReport with Management Suite reports, go to the LANDesk User Community's reporting portal at http://community.landesk.com/ldmsreports. The reporting portal also has additional reports you can download.

Scripts and tasks

LANDesk Management Suite includes a powerful scheduled task system. Both the core server and managed devices have services/agents that support scheduled tasks. Management Suite consoles and Web consoles can add tasks to the scheduler.

A task consists of a distribution package, delivery method, targeted devices, and a scheduled time. Non-distribution tasks consist of a script, targeted devices, and scheduled time.

Here are some of the tasks you can schedule:

- Device configurations
- Various custom scripts
- Custom data form deployments
- Unmanaged device discoveries
- Vulnerability scans
- Software execution on managed devices

IMPORTANT: Console users who will be working with scripts must be in the core server's local LANDesk Script Writers group. This group gives console users write access to the ManagementSuite\Scripts folder.

Read this chapter to learn about:

- "Managing scripts" on page 120
- "Scheduling tasks" on page 121
- "Using the Scheduled tasks window" on page 121
- "Assigning targets to a task" on page 123
- "What you see when tasks run" on page 124
- "Monitoring task status" on page 124
- "Viewing task logs" on page 125
- "Using the default scripts" on page 125
- "Using the rollup core to globally schedule tasks" on page 126

Managing scripts

LANDesk Management Suite uses scripts to execute custom tasks on devices. You can create scripts from the **Manage scripts** window (**Tools > Distribution > Manage scripts**) for these tasks:

- "Creating file deployment scripts" on page 698
- Custom scripts that you create
- "Using the local scheduler" on page 127

The Manage scripts window divides scripts into three categories:

- **My scripts:** Scripts that you created.
- **Public scripts:** Scripts that have been marked public by a user with the Manage scripts "Edit public" right. These scripts are read-only to everyone else. Users can copy public scripts to their **My scripts** folder to edit them.
- **All scripts:** All scripts on the core server.

You can create groups under the **My scripts** item to further categorize your scripts. To create a new script, right-click the **My scripts** item or a group you've created and click the script type you want to create.

Once you've created a script, you can click Schedule on the script's shortcut menu. This launches the **Scheduled tasks** window (**Tools > Distribution > Scheduled tasks**) where you can specify devices the task should run on and when the task should run. See the next section for more information on scheduling tasks.

Due to specific capabilities supported by the Windows console, scripts created in the Windows console shouldn't be edited in the Web console.

Scheduling tasks

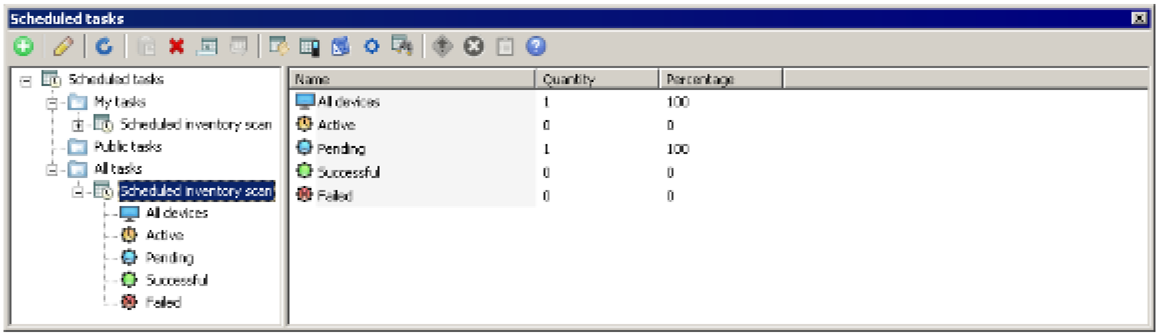
The **Scheduled tasks** window shows scheduled task status and whether tasks completed successfully or not. The scheduler service has two ways of communicating with devices:

- Through the standard LANDesk agent (must already be installed on devices).
- Through a domain-level system account. The account you choose must have the log in as a service privilege. For more information on configuring the scheduler account, see "Configuring the scheduler service" on page 68.

The console includes scripts that you can schedule to perform routine maintenance tasks such as running inventory scans on selected devices. You can schedule these scripts from **Tools > Distribution > Manage scripts > All scripts**.

Using the Scheduled tasks window

Use the **Scheduled tasks** window to configure and schedule scripts you've created. Schedule items for single delivery, or schedule a recurring task, such as a script task to regularly search for unmanaged devices.



Name	Quantity	Percentage
All devices	1	100
Active	0	0
Pending	1	100
Successful	0	0
Failed	0	0

The **Scheduled tasks** window is divided into two halves. The left half shows task tree and tasks, and the right half shows information specific to what you've selected in the tree.

Left pane

The left pane shows these task groups:

- **My tasks:** Tasks that you have scheduled. Only you and Management Suite administrative users can see these tasks.
- **Public tasks:** Tasks that users with the "Edit public" right have marked public.
- **All tasks:** Both your tasks and tasks marked common.

You can drag scripts onto the **Scheduled tasks** window's left pane. Once a script is in the left pane, you can configure targets for it by dragging devices, queries, or groups to the right pane.

When you click **My tasks**, **Common tasks**, or **All tasks**, the right pane shows this information:

- **Task:** The task names.
- **Start On:** When the task is scheduled to run. Double-click a task name to edit the start time or to reschedule it.
- **Status:** The overall task status. View the right pane **Status** and **Result** columns for more details.
- **Owner:** The name of the person who originally created the script this task is using.

When you click a scheduled task, the right pane shows this summary information:

- **Name:** The task state name.
- **Quantity:** The number of devices in each task state.
- **Percentage:** The percentage of devices in each task state.

When you click a task status category under a task, the right pane shows this information:

- **Name:** The device name.
- **IP address:** The device IP address.
- **Status:** The task status on that device (for example, "Waiting").
- **Result:** Whether the task ran successfully on the device.
- **Return code:** The task's return code on the device.
- **Hostname:** The computer name reported by the device.
- **LDAP object name:** If the device was targeted through LDAP, the LDAP object name.
- **Query name**: If the device was targeted through a query, the query name.
- **Message:** Custom messages from the device. These are used with tasks that run a DOS batch file. Include a command that launches sdclient.exe with a /msg="<Message you want to send>" command-line parameter.
- **Log file:** If a device failed to complete the task, the path to the task log file for that device is here.

Before you can schedule tasks for a device, it must have the standard LANDesk agent and be in the inventory database.

To schedule a task

1. In the Scheduled tasks window, click one of these toolbar buttons: **Create software distribution task, Schedule custom script, Thin client, Custom data forms, Agent configuration**, or **Schedule inventory scan**.
2. Enter the information necessary for the task type you selected.
3. Click the **Schedule** button. This displays the **Scheduled tasks** window and adds the script to it, where it becomes a task.
4. In the **Network view**, select the devices you want to be task targets and drag them onto the task in the **Scheduled tasks** window.
5. In the **Scheduled tasks** window, click **Properties** from the task's shortcut menu.
6. On the **Schedule task** page, set the task start time and click **Save**.

You can add more devices to the task by dragging them from the network view and dropping them on the task you want in the **Scheduled tasks** window.

Canceling a task

You can cancel waiting or active tasks. The way to cancel a task depends on the task type, as described below.

- **Software distribution tasks:** Use the cancel button on the toolbar. This toolbar button is only available for software distribution tasks.
- **Custom scripts:** From the shortcut menu of the script you want to cancel, click **Current status**. The **Task status** dialog has **Discontinue task** and **Cancel task** buttons. Click the button you want.
- **Waiting tasks:** From the shortcut menu of the task you want to cancel, click **Properties**. On the **Schedule task** page, click **Leave unscheduled**.

Assigning targets to a task

Once you've added a script to the **Scheduled tasks** window, you can assign targets to it. Drag targets from the network view onto the task that you want in the **Scheduled tasks** window. Targets can include individual devices, device groups, LDAP objects, LDAP queries, and inventory queries. Queries and groups are powerful options that let you have a dynamic list of devices that can change for recurring tasks. For example, as the device target list from a query changes, any tasks using that query will automatically target the new devices.

If a device is targeted more than once, such as when two target queries have overlapping results, the core server detects the duplication and won't run the task multiple times for the same device.

When using queries for task targets, the query won't run until the task is started. The **Scheduled task properties** dialog won't show the target devices until after the task is launched.

Applying scope to tasks

For scheduled tasks, multiple Management Suite users can add targets to a task. However, in the **Scheduled tasks** window, each Management Suite user will only see targets within their scope. If two Management Suite users with scopes that don't overlap each add 20 targets to a task, each Management Suite user will see only the 20 targets they added, but the task will run on all 40 targets.

Selecting targets for your task

Each task you create needs a set of targets that the task will run on. Tasks can have two types of targets, static and dynamic.

- **Static targets:** A list of specific devices or users that doesn't change unless you manually change it. Static targets can be LDAP users or devices from Directory Manager or devices from the console's network view.
- **Dynamic targets:** A dynamic list of devices that allows policy-based distribution tasks to periodically check the target list for any changes. Dynamic targets include query results and LDAP groups/containers or network view groups.

Dynamic policy targets are unique, in that Management Suite updates the results of these queries periodically. As new devices meet the query criteria, recurring tasks using those queries get applied to the new devices.

You can specify static policy targets in these ways:

- **Network view devices :**A static set of devices from the core database.
- **LDAP users or devices:** A static set of user and/or device objects.

You can specify dynamic policy targets in these ways:

- **Network view group:** A dynamic set of devices from the core database.
- **LDAP group/container:** A dynamic set of user, machine, or group objects.
- **Database query:** A set of devices generated by a query against the core database.
- **User group:** A group of users selected from an LDAP-compliant directory.

- **LDAP query:** A set of users, devices, or both, generated by a query on an LDAP-compliant directory.

Targeting devices through a directory

In order for devices to receive policies that are targeted through Active Directory or NetWare Directory Services, they have to be configured to log in to the directory. This means that they need to have all the correct device software installed, and they need to actually log in to the correct directory so that their fully distinguished name will match the name that was targeted through Directory Manager.

Windows 95/98 devices need to be configured to log into the domain where the Active Directory resides. Windows NT and Windows 95/98 don't include Active Directory support. You must install Active Directory support on devices that log in to a directory and require policy-based management. As of this printing, more information on installing Active Directory device support was available here:

http://www.microsoft.com/technet/archive/ntwrkstn/downloads/utils/dsclient.mspx

For each Windows device, there must be a computer account on the Active Directory domain controller. This means that the computer being used as the device must be logged into the domain where the Active Directory exists. You can't simply map a network drive using the fully-qualified Windows domain name. The policy won't take effect this way.

To use Directory Manager to create a query

1. Click **Tools > Distribution > Directory manager**.
2. Click the **Manage directory** toolbar button.
3. Enter the directory URL and authentication information and click **OK**.
4. Click the **New query** toolbar icon.
5. Create your query. For more information, see "LDAP queries" on page 108.

What you see when tasks run

The **Scheduled tasks** window always shows job status. If you're scheduling device configurations or OS deployments, you'll also see the **Client setup utility** dialog. As the scheduler service proceeds through the target list, you'll see the devices to be configured, devices being configured, and devices completed lists. For more information, see "About the Client Setup Utility dialog" on page 635.

If you're scheduling Targeted Multicast distributions, you'll see the **Multicast software distribution status** window. This window shows multicast status. For more information, see "About the Multicast software distribution status window" on page 697.

If you're scheduling custom scripts, you'll see the **Custom job processing** window showing scheduled, working, and completed targeted devices, in addition to a line-by-line script status as it executes.

Monitoring task status

When a task starts processing, targeted devices move through various task states. You can monitor the task state for targeted devices by clicking an active task in the **Scheduled tasks** window. Devices will be in one of these categories:

- **All devices:** All targets for the task.
- **Active:** Targets that are currently being processed.
- **Pending:** Targets that haven't been processed yet.
- **Successful:** Targets that completed the task successfully.

- **Failed:** Targets that failed the task.

These are the states the device can be in, and the category they are visible in:

- **Waiting:** Ready to process a task. (**Pending**) category
- **Active:** Processing the current task. (**Active**) category
- **Done:** Task processed successfully. (**Successful**) category
- **Busy:** Device is already processing a different task and couldn't process the current task. (**Failed**) category
- **Failed:** Didn't complete processing the task for some reason. (**Failed**) category
- **Off:** Device was off or unreachable. (**Failed**) category
- **Canceled:** The user cancelled the task. (**Failed**) category

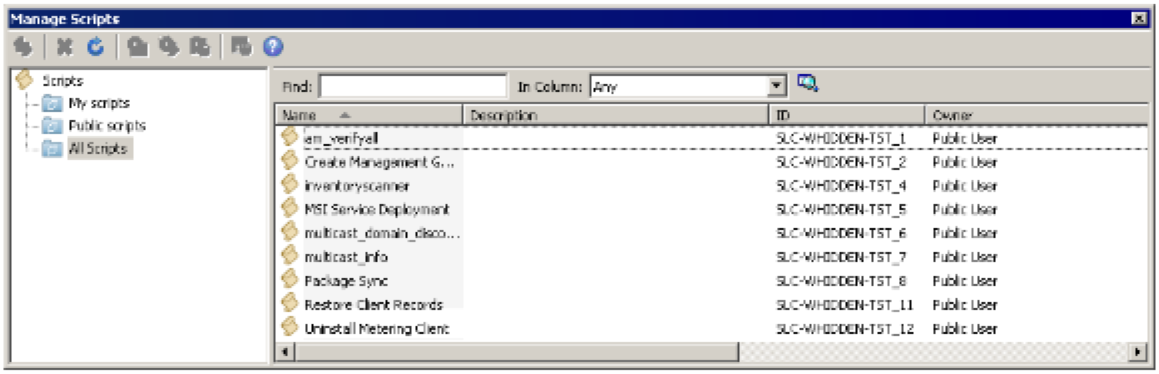
Viewing task logs

If a device fails to process a task, the **Scheduled tasks** window stores the task log. Available logs appear in the **Log file** column next to a device. In the log file you can see the task command that failed.

Using the default scripts

Management Suite ships with a default set of scripts that are listed below. You can use them to help you complete some Management Suite tasks. These scripts are available under the **All scripts** tree in the **Manage scripts** window (**Tools > Distribution > Manage scripts**):

- **am_verifyall:** Verifies all packages installed via policies on clients.
- **Create Management Gateway client certificate:** Creates a security certificate so a device can use a Management Gateway.
- **inventoryscanner:** Runs the inventory scanner on the selected devices.
- **multicast_domain_discovery:** Does a Targeted Multicast domain representative discovery. For more information, see "Using Targeted Multicast with software distribution" on page 159.
- **multicast_info:** Runs a troubleshooting script that shows what information the Scheduled Tasks window will pass to Targeted Multicast, including target device IP addresses and subnet information. Creates a file called C:\MCINFO.TXT.
- **Package sync:** Runs a policy check to see if any new policies need to be applied or made available.
- **Restore client records:** Runs the inventory scanner on selected devices, but the scanner reports to the core the device was configured from. If you have to reset the database, this task helps you add devices back to the proper core database in a multi-core environment.
- **Uninstall metering client:** Removes the software metering agent on target devices. This agent was used in Management Suite prior to version 8.



Name	Description	ID	Owner
am_verifyall		SLC-WHIDDEN-TST_1	Public User
Create Management G...		SLC-WHIDDEN-TST_2	Public User
inventoryscanner		SLC-WHIDDEN-TST_4	Public User
MSI Service Deployment		SLC-WHIDDEN-TST_5	Public User
multicast_domain_disco...		SLC-WHIDDEN-TST_6	Public User
multicast_info		SLC-WHIDDEN-TST_7	Public User
Package Sync		SLC-WHIDDEN-TST_8	Public User
Restore Client Records		SLC-WHIDDEN-TST_11	Public User
Uninstall Metering Client		SLC-WHIDDEN-TST_12	Public User

Understanding bandwidth options

When configuring local scheduler commands, you can specify the minimum bandwidth criteria necessary for the task to execute. The bandwidth test consists of network traffic to the device you specify. When the time comes for the task to execute, each device running the local scheduler task will send a small amount of ICMP network traffic to the device you specify and evaluate the transfer performance. If the test target device isn't available, the task won't execute.

You can select these bandwidth options:

- **RAS:** The task executes if the device's network connection to the target device is at least RAS or dialup speed, as detected through the networking API. Selecting this option generally means the task will always run if the device has a network connection of any sort.
- **WAN:** The task executes if the device's connection to the target device is at least WAN speed. WAN speed is defined as a non-RAS connection that's slower than the LAN threshold.
- **LAN:** The task executes when the device's connection to the target device exceeds the LAN speed setting. LAN speed is defined as anything greater than 262,144 bps by default. You can set the LAN threshold in agent configuration (**Tools > Configuration > Agent > Configuration, Bandwidth detection** page). Changes won't take effect until you deploy the updated configuration to devices.

Using the rollup core to globally schedule tasks

If you have a rollup core in your LANDesk environment, tasks you create on it are globally scheduled and can have targets from multiple child cores. When you create a task on the rollup core and schedule it, the rollup core checks the target list to see which targets belong to which child core server. The rollup core then sends each child core server the task and its unique portion of the overall target list. Each child core server runs the task in the background and reports task status to the rollup core.

If a child core server has targets but doesn't have a rollup core certificate, which is necessary for a child core to process globally scheduled tasks, the rollup core runs the task on those targets instead.

Globally scheduled tasks and task status doesn't appear in the child core's **Scheduled tasks** window. The easiest way to view this information is from the task details on the rollup core. If you want to see delegated task status on a child core that is processing the task, you can use the Delegated Tasks report.

Note: Tasks scheduled from a 9.0 rollup core, including security-related tasks, won't work on version 8.7 and 8.8 cores.

To view delegated task status on a child core

1. On the child core, click **Tools > Reporting / Monitoring > Reports**.
2. In the reports window, click **Reporting > Management Suite > Task status**.
3. Double-click the **Delegated Tasks** report, and enter the date range you want.
4. Click **OK** to see the report.

To reduce network traffic, task status on delegated tasks isn't reported in real-time to the rollup core. Instead, task status is updated every two minutes by default. Do the following to change this interval.

To change the task status check interval

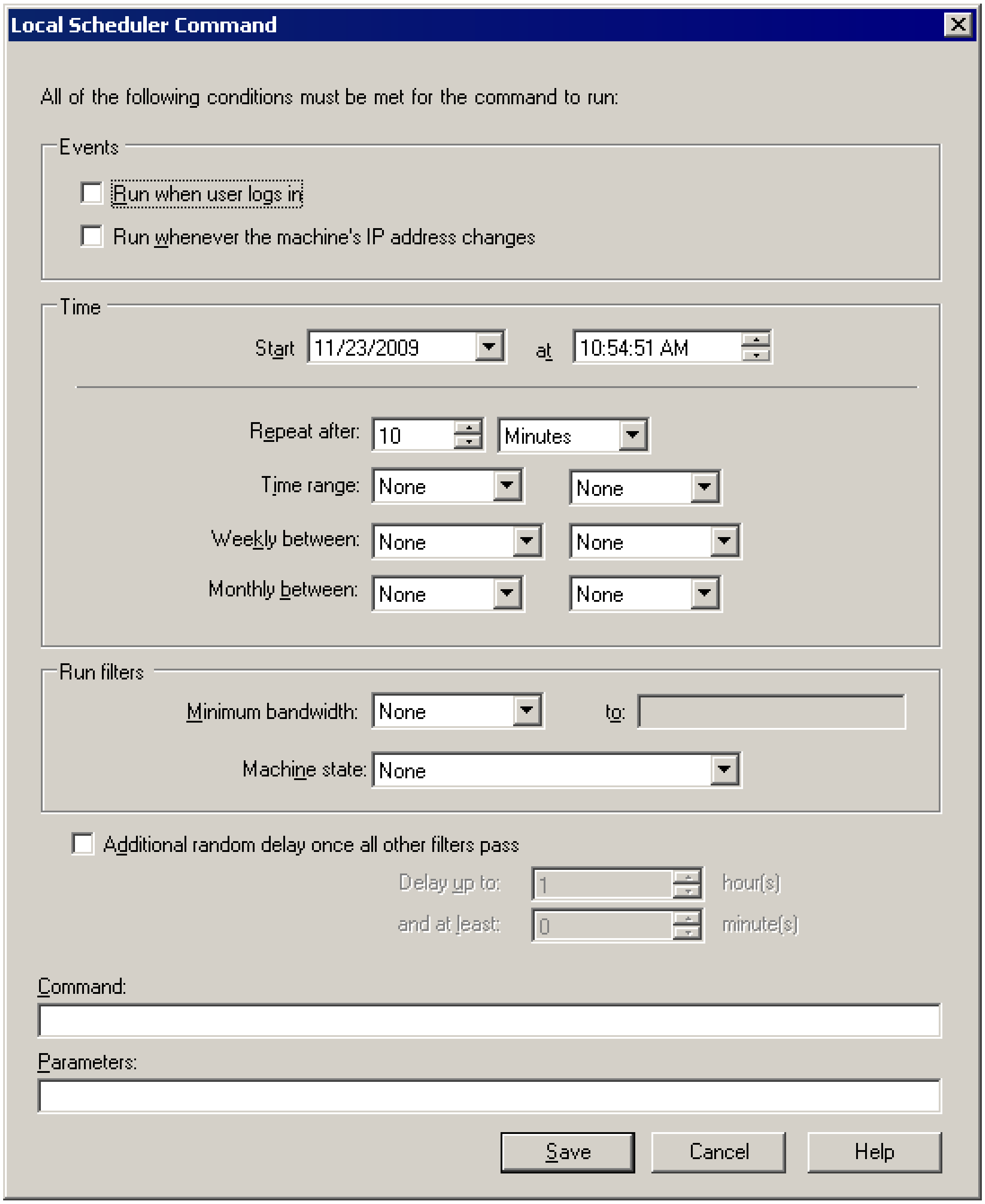
1. On the rollup core, click **Start > Programs > LANDesk > LANDesk Configure Services**.
2. On the **Scheduler** tab, click **Advanced**.
3. Click **Delegate task status check**, and click **Edit**.
4. Enter the number of seconds you want the scheduler to wait between task status checks, and click **OK**. The default is 120 seconds.
5. From the **Scheduler** tab, **Restart** the scheduler service on the rollup core.

Using the local scheduler

The local scheduler is a service that runs on devices. It's part of the common base agent and you can install it through device setup. Usually the local scheduler handles Management Suite tasks, such as running the inventory scanner periodically. Other tasks that you schedule, such as software or OS deployments, are handled by the core server rather than the local scheduler. You can use the local scheduler to schedule your own tasks to run periodically on devices. Once you create a local scheduler script, you can deploy it to devices by using the **Scheduled tasks** window.

The local scheduler assigns each task an ID number. Local scheduler scripts have an ID range that is different from the default local scheduler scripts that Management Suite uses. By default, you can only have one custom scheduler script active on each device. If you create a new script and deploy it to devices, it will replace the old script (any script in the custom local scheduler ID range) without affecting the default local scheduler scripts, such as the local inventory scan schedule.

When selecting schedule options, don't be so restrictive that the task criteria are infrequently met, unless that's your intention. For example, while configuring a task, if you select Monday as the day of the week and 17 as the day of the month, the task will only execute on a Monday that's also the 17th of the month, which happens very infrequently.



Local Scheduler Command

All of the following conditions must be met for the command to run:

Events

□ Run when user logs in

□ Run whenever the machine's IP address changes

Time

Start 11/23/2009 at 10:54:51 AM

Repeat after: 10 Minutes

Time range: None None

Weekly between: None None

Monthly between: None None

Run filters

Minimum bandwidth: None to:

Machine state: None

□ Additional random delay once all other filters pass

Delay up to: 1 hour(s)

and at least: 0 minute(s)

Command:

Parameters:

To configure a local scheduler command

1. In the **Managed scripts** window (**Tools > Distribution > Manage Scripts**), from the My scripts shortcut menu, click **New local scheduler script**.
2. Enter a **Script name**.
3. Click **Add** to define the script options.
4. Configure the local scheduler options as described earlier.
5. Click **Save** to save your script.
6. Use the **Scheduled tasks** window to deploy the script you created to devices.

Installing the local scheduler service on an unmanaged Device

The LANDesk Local Scheduler service can be installed on an unmanaged device. Only two files are required for local scheduler functionality:

- LocalSch.exe
- LTapi.dll

To install the LANDesk Local Scheduler service on an unmanaged server or workstation, follow the steps below.

1. Create the following folder.
```
%ProgramFiles%\LANDesk\LDClient
```
2. Copy LocalSch.exe and LTapi.dll to this folder.
3. Click **Start > Run** and type the following command.
```
“%ProgramFiles%\LANDesk\LDClient\localsch.exe” /i
```

Uninstalling the Local Scheduler service

To uninstall the LANDesk Local Scheduler service, follow the steps below.

1. Click **Start > Run** and type the following command.
```
“%ProgramFiles%\LANDesk\LDClient\localsch.exe” /r
```
2. Delete the files and folders.

LocalSch.exe command-line parameters

In additional to monitoring and running local tasks, LocalSch.exe can be used to install or remove the service, add new tasks, and list all of the currently configured tasks.

The following are the command line options supported by the local scheduler application.

```
LocalSch.exe [/i] [/r] [/d] [/tasks] [/isinstalled] [/del] [/removetasks]
 [/exe=<executable>] [/cmd=<command line>] [/start=”<date/time>”] [/freq=xxx]
 [/user] [/bw=xxx|<server>] [/tod=<begin>|<end>] [/dow=<begin>|<end>]
 [/dom=<begin>|<end>] [/ipaddr] [/taskid=<id>] [/range=<min>|<max>]
```

/i – Install service

Installs the local scheduler service on the device. After being installed the local scheduler will still need to be started.

/r – Remove service

Removes the local scheduler service from the machine. The local scheduler service should be stopped before removing the service.

/d – Run in debug mode

Runs the local scheduler in a debug mode. When run in debug mode, the local scheduler runs as a normal Windows process rather than as a service or pseudo service. This mode does not result in any additional debug output.

/isinstalled – Is installed check

Checks to see if the local scheduler service is installed on the local computer. This method will return S_OK, or zero, if the local scheduler is installed. If the local scheduler is not installed a non-zero value will be returned.

/tasks – List tasks

This command will output the currently configured tasks to stdout but can only be seen in a command prompt if piped to more.

```
LocalSch.exe /tasks | more
```

The output can be redirected to a text file, tasks.txt for example, using the following command line:

```
LocalSch.exe /tasks > tasks.txt
```

Adding a task with LocalSch.exe

The rest of the command-line parameters are used for adding a local task. When adding a local task, you must specify the executable using the /exe parameter. If the user or process executing the command line doesn't have administrator rights, the task won't be scheduled. If the current user doesn't have administrator privileges, the task won't be created.

In addition to the command line options outlined below, the /taskid option may be used to specify the task.

/exe=<executable> - Scheduled application

Specifies the application that is to be launched when the scheduled time arrives. If this parameter isn't provided, the local task won't be created.

/cmd=<command line> - Application command line

Specifies the command line to be used when the scheduled application is launched. If this parameter is not specified, the scheduled application will be launched without command line parameters.

/start="<date/time>" – Start time

Specifies the start time for the application. If this parameter isn't specified, the application will be launched as soon as possible. If any filters are specified they must be satisfied before the application is launched. The start time is specified is in local system time of the computer and has the following format:

```
/start="06 Nov 2001 17:39:47" /bw=WAN|myserver.domain.com
```

This format is a shortened version of the format used by HTTP. The month is always specified using a three-letter ASCII abbreviation: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec. If the format of the date is specified incorrectly, the task won't be added.

/freq=xxx – Frequency

Specifies a periodic frequency. Frequency is the number of seconds before the task will be run again. If this parameter isn't specified or is zero, the task will only be run once.

/user – User filter

Specifies that a user filter should be created for the task. A user filter will prevent the task from being run until a user is logged onto the system.

/bw=xxx|<network host> - Bandwidth filter

Specifies the bandwidth needed to a specific network host. The bandwidth can be specified as LAN, WAN, or RAS. If another bandwidth value is used the local scheduler will default to RAS bandwidth. The task won't be run until the local scheduler detects that the specified type of bandwidth is available between the device and the specified network host.

For example, the following filter would specify not running the task until at least WAN connectivity is available to the myserver.domain.com computer.

```
/bw=WAN|myserver.domain.com
```

/tod=<begin>|<end> - Time of day filter

Specifies a time of day filter. The task won't be run unless the time of day is between the specified begin and end hours. Time of day values are specified as the hour 0 through 23. For example, the following filter would specify running a task between 7 p.m. and 10 p.m.

```
/tod=19|22
```

/dow=<begin>|<end> - Day of the week filter

Specifies a day of the week filter. The task won't be run unless the weekday is between the specified begin and end days. Day of week values are specified as an integer with 0 being Sunday. For example, the following filter would specify running a task between Sunday and Thursday.

```
/dow=0|4
```

/dom=<begin>|<end> - Day of month filter

Specifies a day of the month filter. The task won't be run unless the day of the month is between the specified begin and end days. The day of month filter is specified using numeric value between 1 and 31. For example, the following filter would specify running the task between the 16th and 28th of the month.

```
/dom=16|28
```

/ipaddr - IP address change filter

Specifies that the task should be run whenever the IP address of the machine changes. This functionality requires the IP Helper libraries and is not available on Windows 95 systems and on Windows 98/NT systems without Internet Explorer 4 or later installed.

Deleting a task with LocalSch.exe

The local scheduler provides the ability to delete one or more tasks. The following parameters are used when deleting tasks.

/del – Delete task or tasks

Deletes the task specified by the /taskid parameter or deletes all tasks within the /range max and min values inclusive. The task IDs can be determined by either looking at the tasks using /tasks command line option or by using a constant /taskid when adding a task.

/removetasks – Remove all tasks

Removes all currently scheduled local tasks.

/taskid – Specifying the task ID

Specifies the ID of the task that is being deleted. Task IDs can be determined by looking at the tasks currently scheduled (see /tasks above). The ID is specified as an integer value.

/range=<min>|<max> – Range of task IDs

Specifies a minimum and maximum value of a range of task IDs. It can be used with the /del command to remove all tasks with task IDs within the given range.

Normally when generating a task an ID is randomly assigned, using the current time (time_t) value as the task ID. A randomly assigned ID will never be less than 100000. This command line parameter can be used to specify the ID for the task. Task ID values 0 -1000 are reserved for internal LANDesk use. Task ID values 1001-2000 are reserved for use by the management console's local scheduler interface.

Character parsing and the command line

The local scheduler uses standard white space-delimited parsing for the command line. This means that if any of the parameters contain white space they need to be enclosed in quotation marks. Certain parameters, such as /start, always contain white space and hence always need to be quoted. Other parameters, such as /exe and /cmd, may or may contain white space and may or may not need to be quoted.

The following example shows a command line that does not need quotation marks.

```
LocalSch.exe /exe=c:\windows\system32\cmd.exe
```

The following example shows a command line that does need quotation marks.

```
LocalSch.exe /exe="%ProgramFiles%\MyProgram\myprog.exe" /cmd="/apm /s /ro"
```

Quoting already quoted parameters

If the parameters that are to be passed to /cmd= are already quoted, then three quotes are required. One set to quote the entire string. Another to quote the quoted values, and the quoted values.

For example, the following command line shows an example of parameters that need to be surrounded by three quotation marks.

```
LocalSch.exe /exe="%ProgramFiles%\LANDesk\File Replicator\LANDeskFileReplicatorNoUI.exe"
/cmd="""%ProgramFiles%\LANDesk\File Replicator\LDHTTPCopyTaskConfig.xml""
""%ProgramFiles%\LANDesk\File Replicator\replicator.log"""
```

In the above command, the two parameter are paths to files. Because both paths are in the “Program Files” directory, they paths have spaces and must be quoted in order to be proper parameters for LANDeskFileReplicatorNoUI.exe. So each quoted parameter is surrounded by a second set of quotes, and then the entire string is surrounded by quotes.

Quoting redirection operators

Quotes must also surround any switches that contain a redirection operator. Redirection operators include the following symbols: <, >, |. The /bw switch uses a | character called a pipe or bar. It is important to remember that the | character is used in the command prompt to pipe the output to another application. To prevent this character from being parsed by the command line, it must be surrounded with quotes.

For example, the following command uses a /bw parameter with a | character and needs to be quoted.

```
LocalSch.exe /exe=C:\ldclient\myprogram.exe /cmd="/apm /s /ro" /bw="LAN|server"
```

Remote control

Use LANDesk Management Suite's remote control feature to easily resolve device problems from one location. You can only remote control devices that have the remote control agent installed. During a remote control session, the remote device actually has two users, you and the end user. You can do anything at the remote device that the user sitting at it can do. All of your actions are in real-time on that device.

Management Suite enables you to remote control these device types:

- Windows NT/2000/2003/XP/Vista/7 devices
- Windows 95/98 devices
- Mac OS 9.2, 10.3 and greater devices

The remote control viewer application runs on both Windows and Mac OS 10 devices.

Read this chapter to learn about:

Using the remote control viewer

Use the remote control viewer to remotely access a device. You can only remote control devices that have the remote control agent installed. During a remote control session, the remote device actually has two users--you and the end user. You can do anything at the remote device that the user sitting at it can do.

You can do a lot more than just remote control a device from the viewer window. Once the viewer connects to a device, you can choose from these tasks:

- **Remote control:** Remotely view and control a device.
- **Chat:** Remotely chat with a device.
- **File transfer:** Remotely transfer files to and from your computer to another device. In essence, this works as though you've mapped a drive to remote device.
- **Reboot:** Remotely reboot a device.
- **Draw:** Displays drawing tools you can use to draw on the remote screen.

You can do multiple viewer tasks on a device at the same time. When you activate a viewer task, the interface for that task appears in the viewer window.

Once you've taken control of a remote device, its screen appears in the viewer window. Because the viewer window often isn't as big as the remote device's screen, you'll either need to use the autoscroll feature to scroll up, down, and side to side, or use the **Move Remote Screen** icon to maneuver more easily around the different areas of the remote screen. Also, autoscroll automatically scrolls the window as the mouse pointer approaches the viewer window's edge.

You can also increase the viewer window displayable area by disabling items in the View menu, such as connection messages, the toolbar, or the status bar. Use the **View** menu's **Full screen** option to completely remove the viewer window's controls. If the remote screen's resolution exceeds yours, autoscroll will still be necessary.

If you want to speed up the viewing rate or change the viewer window settings, use the items under the **Options** menu. To remotely chat, transfer files, or reboot the device, use the items under the **Tools** menu or the toolbar.

Connecting to devices

Before you can do any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see connection messages and status in the **Connection messages** pane, if that is visible. If it isn't, you can toggle it by clicking **View > Connection messages**.

To connect to a device

1. In the network view, from the shortcut menu for the device you want to remote control, click **Remote control, Chat, File transfer,** or **remote execute.**
2. Once viewer window appears and connects to the remote device, you can use any of the remote control tools available from the viewer's **Tools** menu, such as chat, file transfer, reboot, inventory, or remote control.
3. To end a remote control session, click **File > Stop connection**.

Remote controlling devices

Once you've connected to a device, often you'll want to view it remotely.

To view a remote device

- Click **Tools > Remote control**. If options in the **Tools** menu are dimmed, that means you aren't connected to a device.

To view different areas of a remote device screen

1. Move the mouse pointer to the edge of the viewer window. The window scrolls automatically.

OR

1. Click the **View another part of the remote screen** icon.
2. Your cursor becomes a hand that you can click, drag, and release to view various areas of the remote screen.

Using the drawing tools on remote devices

Once you're remotely viewing a device, you can use the drawing tools on it. The drawing tools can help you explain to users what you're doing or highlight information on the remote screen for users to look at. When you use a tool to draw on the screen, both you and the remote user can see what you've drawn. The drawn images stay on both your screens until you click the eraser in the drawing tool palette.

You have three drawing tools to choose from:

- **Pencil:** Use the pencil tool to make freehand drawings. You aren't limited to a shape with the pencil tool.
- **Box:** Use the box tool to draw a rectangle around something on the screen. Click where you want a corner of the rectangle to be, and while holding down the mouse button, drag it over the area you want boxed. Release the mouse button when you're ready for the rectangle to be drawn.
- **Pointer:** Use the pointer tool to point at objects on screen. When you hold down the left mouse button, the pointer tool is active and a red dot appears under the mouse pointer that makes it easy for users to see where the pointer is. When you release the left mouse button, the dot disappears. You can't change the dot color and it doesn't leave a trail like the pencil tool does.

You can also use the line thickness and line color drop-down lists to change how your drawings will look. Changes to these items only affect new things that you draw. When you're done drawing, click the eraser button on the drawing palette or close the palette.

Adjusting remote control settings

Use the **Options** dialog's **Change settings** tab (**Tools > Options**) to adjust the remote control settings.

- **Allow autoscroll:** Enables the viewer window to scroll as you move the cursor closer to the window border. The closer you move to the border, the faster the scrolling occurs.
- **Lock out the remote keyboard and mouse:** Locks the remote device's keyboard and mouse so that only the user running the viewer can control the remote device. Note that special key combinations in Windows such as "CTRL-ALT-DEL" or the "Windows Key+L" aren't locked out.
- **Synchronize clipboards to paste between local and remote computers:** Synchronizes the keyboards between the local and remote device so you can paste information between the two devices.
- **Hide the remote computer screen:** Hides the remote device's screen so only the user running the viewer can see the user interface display on the remote device.
- Always ask to clear remote computer's screen when starting remote control: Asks the remote user if it's OK to blank their screen during remote control. When selected, the **Hide remote computer screen** option's state doesn't matter.
- **Lock the remote computer when the session ends:** When the session ends, activates the operating system's lock feature.
- **Auto keyboard mapping:** You should keep this option checked. It remaps the target device's keyboard so it matches the administrators. This helps ensure what the administrator is typing appears correctly on the target device. This is especially useful when the administrator and target keyboards are based on different alphabets or languages.
- **Enable old agent compatibility (pre-8.5 agents):**LANDesk changed remote control security and added a new remote control viewer in version 8.5. If you have remote control agent versions on your network that are pre-8.5, you can check this option to allow the new remote control viewer to communicate with these older agent versions.

Using alternate names

Depending on how you've configured the remote control agent on managed devices, users on a device that's being remote controlled can double-click the remote control status icon in the Windows system tray and see the computer name and user name of the administrator that is remotely controlling them. If you don't want your real computer or user names to be visible from remote devices for security reasons, you can specify an alternate user name and/or computer name that appears in the remote control status dialog on remote devices.

To use alternate names

1. Click **Tools > Options**.
2. On the **Change settings** tab, select **Use alternate names**.
3. Specify the names you want users at remote devices to see.
4. Click **OK**.

Optimizing remote control performance

Use the **Options** dialog's **Optimize performance** tab **(Tools > Options)** to optimize remote control performance for these connection types:

- Slow connection (modem)
- Medium connection (broadband)
- Optimize for fast connection (LAN)
- Custom connection

Changing the optimization setting dynamically adjusts color reduction, wallpaper visibility, and remote windows appearance effects (the ones you can adjust in **Display Properties > Appearance > Effects**), such as transition effects for menus and tooltips.

Remote control always uses a highly efficient compression algorithm for remote control data. However, even with compression, it requires a lot of data to send high color depth information. You can substantially reduce the amount of remote control data required by reducing the color depth displayed in the remote control viewer. When the viewer reduces the color depth, the viewer has to map the full color palette from the remote desktop to a reduced color palette in the viewer. As a result, you may notice colors in the remote control window that don't accurately reflect the remote desktop. If that's a problem, select a higher-quality compression setting.

Another way you can optimize performance is to suppress the remote wallpaper. When you do this, remote control doesn't have to send wallpaper updates as parts of the remote desktop are uncovered. Wallpaper often includes bandwidth-intensive images, such as photographs. These don't compress well and take time to transfer over slower connections.

The final way you can optimize performance is to use a mirror driver on the remote device. For more information, see the next section.

Using the mirror driver

The mirror driver provides many benefits. The main benefit is that it provides a Microsoft-supported way of capturing screen output without requiring modifications to the existing video driver. This allows the remote control mirror driver to behave in a standard way that can cause fewer problems on devices.

The other benefit is that the mirror driver doesn't use as much processing power from the target device. If you're remote controlling devices that have a 1.5 GHz or slower processor, the mirror driver can provide noticeable performance improvements over faster network connections. On slower network connections, remote control performance is limited more by bandwidth than processor utilization.

The standard remote control agent is always installed on devices. When the mirror driver is installed with it, the standard agent and the mirror driver coexist. You can't uninstall the standard remote control driver and use only the mirror driver.

Changing viewer hot key settings

The remote control viewer supports the following hot keys:

- **Enables hot keys** (Ctrl + Alt + H): Enables/Disables hot key availability. Hotkeys are enabled by default.
- **Close viewing session** (Ctrl + Alt + S): Disconnects the current viewing session. The remote control viewer window stays open.
- **Send Ctrl-Alt-Delete** (Ctrl + Alt + D): Sends Ctrl+Alt+Delete to the target device.
- **Lock out remote keyboard and mouse** (Ctrl + Alt + K): Enables/Disables the target device's local mouse and keyboard.
- **Toggle full-screen** (Ctrl + Alt + M): Toggles the remote control viewer between windowed mode and full screen mode.
- **Send Ctrl+Esc** (CTRL + Alt + E): Sends CTRL+ESC to the target device.
- **Toggle mouse and drawn mode:** Toggles between drawing mode and normal mouse pointer mode.
- **Refresh screen:** Retransmits screen data from the remote computer.
- **Refresh data:** Sends a refresh command (F5) to the remote computer.
- **Disconnect session:** Ends the current remote control session. The viewer window stays open.

You can change a hot key by clicking in the box next to it and pressing the new key combination. The print screen or pause/break keys can't be part of a key combination.

Sending CTRL+ALT+DEL to Vista and Windows 7 devices

The default local security policy on Windows Vista and Windows 7 won't allow CTRL+ALT+DEL from a remote control viewer. To change this, do the following.

To allow CTRL+ALT+DEL on Vista and Windows 7 devices

1. In the **Start** menu's search box, type **gpedit.msc** and press **Enter**.
2. Navigate to **Local Computer Policy > Administrative Templates > Windows Components > Windows Logon Options > Software Secure Attention Sequence**.
3. Double-click **Disable or Enable Software Secure Attention Sequence**.
4. Click **Enabled**, and in the drop-down list click either **Services** or **Services and Ease of Access applications**.
5. Click **OK**.

Chatting with remote devices

You can use the remote control viewer to remotely chat with a user at a remote device. This feature is useful if you need to give instructions to a remote user whose dial-up connection is using the only available phone line. Users can respond back using the chat window that appears on their screen. You can only use chat on devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

If you want to save the messages from a chat session, you can. Any text appearing in the gray area of the chat session will be saved to a text file.

To chat with a user at a remote device

1. Click **Tools > Chat**. A section of the viewer window turns into a chat area.
2. In the lower left section of the chat area, type in a short message. Click **Send**.

Your message will appear on the remote device's screen. A user can respond by typing a message and clicking **Send**. The user also can click **Close** to exit out of a chat session.

To save messages from a chat session

1. In the chat area of the viewer window, click **Save messages**.
2. In the **Save as** dialog, type in a filename and click **Save**.

Transferring files to remote devices

You can use the remote control viewer to transfer files to and from your computer to the remote device. In essence, this works as though you've mapped a drive to the remote device. You can only transfer files to/from devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

To transfer files to a device

1. Click **Tools > File Transfer**. Windows Explorer appears.
2. Select a file to transfer by clicking the filename. From the file's shortcut menu, click **Copy**.
3. Scroll down the Windows Explorer tree to **LANDesk Remote Control**. You should see the name of the remote device you're currently controlling.
4. On the remote device, select a folder to paste the file to, then right-click and click **Paste**.

Similarly, you can also transfer files from a remote device to your computer.

Running programs on remote devices

You can launch programs on remote devices. Use the Run box on the viewer toolbar to enter the remote program's path and filename. Since the program will be launched on the remote device, the path and filename you enter must be present on the remote device.

To run a program on a remote device

1. In the viewer's **Run** box, enter the program path and filename. If you don't know either, you can drop down the list and click **Browse**. This opens a dialog that allows you to browse the remote device's folders.
2. Click the **Remote execute** button to the right of the **Run** box.

Rebooting remote devices

You can use the remote control viewer to remotely reboot a device. You can only remotely reboot devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

To remotely reboot a device

1. Click **Tools > Reboot**.
2. In the **Timeout (seconds)** edit box, enter the time that a user will have before the device is rebooted. The maximum delay is 300 seconds.

3. In the **Remote user prompt** box, type in a brief warning message that a user will see on the device before it's remotely rebooted.
4. You can save your settings by clicking **Save these settings**.
5. Click **OK**.

The warning message will appear on the device, with a countdown showing how much time remains before the reboot. The user has the option of clicking **OK** to immediately reboot, or **Cancel** to not accept the request. A message box will appear on your computer telling you if the user cancelled the request. If the reboot has taken place, you'll see a message in the session messages area of the viewer window.

Changing device remote control security

Management Suite has a high level of control over devices when granted access rights. The device controls remote access security. It stores its remote access security settings in the registry.

You can change remote control settings and security model on clients by updating the agent configuration settings (**Tools > Agent configuration**), and from the updated configuration's shortcut menu, clicking **Schedule update**. Once you deploy the update to devices, their agents will use the settings you specified.

For more information, see Deploying remote control.

Using remote control logging

By default, Management Suite logs remote control actions, including the device remote controlled and the console doing the remote controlling. You can disable remote control logging if you want or purge remote control log entries older than a date you specify. The remote control agent on each managed device stores log information in C:\Program Files\LANDesk\ldclient\issuser.log. The inventory scanner reads this file and stores the data in the core database.

If logging is enabled, you can view these remote control reports (**Tools > Reporting / Monitoring > Reports**), and in the **Reports** tool, click **Reports > Standard reports > Remote control**:

- Remote Control History by Client
- Remote Control History by Console
- Remote Control History for Managed Computer
- Remote Control Summary

To enable or disable remote control logging

1. In the Management Suite console, click **Configure > Remote control logging**.
2. Check or clear the **Enable remote control history** option, depending on your preference.

To purge the remote control log

1. Click **Configure > Remote control logging**.
2. Enter the date you want purged. All entries older than this date will be deleted.
3. Click **Delete history** to execute the purge.

If managed devices are using the "Windows NT security" remote control model, there are some additional steps you need to take to make sure that the remote control reports show the right information. With the "Windows NT security" model, both the remote control operator and managed devices must be members of the same Windows domain. You also need to make sure the domain accounts for all remote control operators are in the **Remote control operators** group in the **Remote control** agent configuration page. If you don't do this, the remote control report will show the local user as the remote control operator, rather than the actual operator.

Changing the remote control mode on target devices

The LANDesk remote control agent on devices accepts two types of connections:

- Direct connections from the LANDesk remote control viewer window.
- Management Gateway connections through a management gateway.

The remote control agent only listens for one type of connection. If you want to change the connection type the agent listens for, double-click the remote control status icon in the target device's system tray and click **Switch mode**. This toggles the agent between direct mode and gateway mode. Text in the remote control status dialog shows which mode the remote control agent is currently in. You can either have remote users toggle this for you or you can do it through a remote control session. If you do it through a remote control session, the session will disconnect once you click the **Switch mode** button.

LANDesk System Manager doesn't support the Management Gateway, so this button will always be dimmed on devices managed by System Manager.

Customizing the viewer and remote control agents

The remote control viewer has command-line options you can use to customize how it works. You can also adjust the remote control agent registry keys on devices if necessary. Normally these registry keys are set by the remote control agent configuration that you deploy to devices.

Viewer command-line options

You can launch the remote control viewer using a command-line option that immediately opens a viewer window, connects to a specific device, and activates the viewer features you want, such as remote control, chat, file transfer, or device reboot. The remote control program, isscntr.exe, is in the main ManagementSuite program folder.

Remote control command-line options use the following syntax:

```
isscntr /a<address> /c<command> /l /s<core server>
```

If your core server uses certificate-based security or integrated security for remote control, you must use the /s parameter to specify the core server.

Option	Description
/a<address>	Contact a device at a particular TCP/IP address. The TCP/IP address may include both numeric- and name-style addresses, separated by semicolons. You can also specify the hostname.
/c<command>	Start the remote control viewer and run a particular feature. (See command names below.) You can specify multiple /c arguments on one command line. For example:

Option	Description
	isscntr /agamma /c"remote control" /c"file transfer" You can choose from these features: **Remote control**: Open a remote control window **Reboot**: Reboot the given device **Chat**: Open a chat window **File transfer**: Open a file transfer session **System info**: Opens a window displaying information about the device, including OS, memory, and hard drive space.
/l	Limit the viewer interface so it only displays the features you specify with /c.
/s<core server>	If you're using certificate-based security, use this option to specify the core server to authenticate with. This option is helpful if you're remote-controlling clients in a multi-core environment. If your core server uses certificate-based security or integrated security for remote control, you must use the /s parameter to specify the core server.

Example 1

Opens the viewer window. Any changes made, such as sizing the connection messages window or setting performance options are retained from the last time the viewer window was used.

```
isscntr
```

Example 2

Launches a remote control session connecting to the device named "gamma." (Note that there is no space and no punctuation between "/a" and "gamma.")

```
isscntr /agamma /c"remote control"
```

Example 3

Launches a remote control and chat session connecting to the device named "gamma". Remote control first attempts to try to resolve the name "gamma". If this fails, it attempts to connect to the numeric address 10.10.10.10:

```
isscntr /agamma;10.10.10.10 /c"remote control" /c"chat"
```

Port 9535 is used to communicate between the viewer and agent computers. If devices running issuser.exe are configured to use a port other than 9535, the port must be passed as part of the address given to isscntr.exe. For example, to remote control a device with address 10.4.11.44, where issuser.exe is configured to use port 1792 as the verify port, the command line would be:

```
isscntr /a10.4.11.44:1792 /c"remote control"
```

Macintosh agents still use ports 1761 and 1762 to communicate, but you can still use isscntr.exe in Management Suite 8.7 to remote control.

The NetWare agent uses port 1761.

Troubleshooting remote control sessions

This section describes problems you may encounter when remote controlling a device and possible solutions.

I can't remote control a device

Check that the device has the LANDesk agents loaded.

To check that the LANDesk agents are loaded:

- In the console's network view, click **Properties** from the device's shortcut menu. Click the **Agents** tab and view the loaded agents.

To load the remote control agent

- Create an agent configuration task in the console and push it to the device, or map a drive from the device to the core server and run the appropriate device configuration task.

Can't transfer files between the console and a target device

Check to see if you're running Norton AntiVirus*, and if its Integrity Shield is turned on. If the Integrity Shield is turned on, you must have temporary privileges that let you copy to the directory that the Integrity Shield is protecting.

Software distribution

This chapter explains how to use LANDesk Management Suite to distribute software and files to devices throughout your network.

Read this chapter to learn about:

Software distribution overview

Software distribution enables you to deploy software and file packages to devices running the following operating systems:

- Windows 95B/98SE
- Windows NT (4.0 SP6a and higher)
- Windows 2000/2003/XP/Vista/7
- Mac OS X 10.4x and 10.5x (using the current agent for Macintosh)
- Max OS X 10.2x. and 10.3.x (using the legacy agent for Macintosh)
- RedHat Linux 7.3,8.0, 9, and Enterprise Linux v3/v4/v5 (AS, ES and WS)
- Suse Linux Server 9 and 10, and Linux Professional 9.3

Devices receiving the software distribution packages must have the following LANDesk agents installed:

- Standard LANDesk agent (formerly known as CBA)
- Software distribution agent

Software distribution features include:

- LANDesk Targeted Multicasting® features that minimize bandwidth use when distributing large packages to many users—without dedicated hardware or router reconfigurations
- Delivery methods enable detailed control over how tasks complete
- Easy task scheduler integrates with the inventory database to make target selection easy
- Real-time status reporting for each deployment task
- Policy-based distributions, including support for create push tasks supported by policy
- Distribution to Mac OS 9.22 and Mac OS X devices
- Mobile device support, including bandwidth detection, checkpoint restart, and the ability to complete the job using a policy
- Ability to distribute any package type, including MSI, setup.exe, and other installers

If you don't have an existing package that you want to deploy, you can use Management Suite package-building technology to create a standalone executable program for the required software installation. Once you have a package, store it on a Web or network server called a "delivery server." Through the console, you can schedule distribution using the **Scheduled tasks** window. The core server communicates the package's location (URL or UNC path to the device), and the device then copies only the files or the portions of the files it needs from the delivery server.

For example, if you're reinstalling a software program because some of its files were corrupted or missing, the system copies only the damaged or missing files, not the entire program. This technology also works well over WAN links. You can store the package on multiple servers, and then schedule devices to use the server appropriate to their needs (that is, location proximity, bandwidth availability, and so on).

Software distribution will also resume interrupted package downloads. For example, if a mobile device was in the process of downloading a large package and that device disconnects from the network, once the device reconnects the download resumes right where it left off.

In Management Suite, software distribution consists of these main steps:

1. **Create or obtain a software package**. The software package can be one or more MSI files, an executable, a batch file, a Macintosh package, a Linux RPM package, a Windows script host package, an application virtualization package, or a package created with the legacy Management Suite package builder. Put the package on your delivery server.
2. **Create a distribution package (Tools > Distribution > Distribution Packages**). The distribution package contains the files and settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, command-line parameters, additional files needed to install the package, and so on. These settings are stored in the database and create a distribution package. Once you create a distribution package, the information is stored in the database and can easily be used in multiple tasks.
3. **Create a delivery method (Tools > Distribution > Delivery Methods**). The delivery method defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Options include Targeted Multicast and push and/or policy distributions. Don't create a delivery method every time you want to distribute a package. Delivery methods allow you to define best practices for deploying software. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.
4. **Schedule the distribution job in the Scheduled tasks window (Tools > Distribution > Scheduled Tasks**). Here you specify the distribution package, the delivery method, the devices that need to receive the distribution package, and when the task should run.

5. When the scheduled time occurs, the scheduler service will start the scheduled task handler which deploys the package using the options selected in the delivery method. These may include:
    - If a delivery method that uses multicast is selected, multicast is used.
    - If a push delivery method is selected, the service contacts the software distribution agent on each device and informs it that the package is ready for installation.
    - If a policy base delivery method is selected, the package becomes available for download.
6. The software distribution agent obtains the package from its local cache, a peer on the network, or the delivery server and processes it on the device by installing or removing the packaged files.
7. After the package is processed, the software distribution agent sends the result to the core server, where it's recorded in the core database.

Separating distribution tasks into two parts, distribution packages and delivery methods, simplifies the distribution process. Now you can create delivery method templates that are independent of a particular package. For example, you could create a default Targeted Multicast delivery method template, and whenever you have a package you want to multicast, you can deliver the package using that template without having to reconfigure the distribution package or the delivery method.

If you have different people in your organization that create packages and distribute packages, these changes help simplify job roles and task divisions. Package creators can now work independently from package deliverers.

Understanding package types

Software distribution supports these package types:

MSI

These are packages in the Windows Installer format. You must use a third-party tool to create MSI packages. These packages consist of a primary .MSI file and can include supporting files and transforms. Transforms customize how MSI packages are installed. If your MSI package consists of multiple files, make sure you add all of them in the **Distribution package** dialog.

Executable

In order for an executable package to be used by software distribution, it must meet the following criteria:

- The executable must not exit before the installation is complete.
- The executable must return zero (0) for a successful installation.

As long as the executable meets these two criteria, any executable can be used for installing the package. You can include additional files for executable packages.

Batch file

Batch file packages are based on a Windows/DOS batch file. You can include additional files for these distribution packages. The successful completion status of the batch file package is based on the value of the errorlevel system environment variable when the batch file has finished running.

Using batch files in tasks on Windows 95/98 devices
In Windows 95/98, when command.com launches a batch file that contains a Windows executable, the batch file will launch the executable and continue executing commands in the batch file without waiting. The core will receive a result when the batch file ends, not necessarily when the Windows executable ends. In this case, the core won't know if the Windows executable ran correctly and it will report a successful completion if the rest of the DOS commands ran successfully.

If the batch file launches a DOS executable, the batch file will then wait for the executable to finish before continuing on. For DOS executables, the core will receive a result when all processes have ended.

Macintosh

Any Macintosh file can be downloaded, though Management Suite won't download directories. Install packages (.PKG) can contain directories. They must be compressed. If the file downloaded has an extension of .SIT, .ZIP, .TAR, .GZ, .SEA, or .HQX, Management Suite will decompress the file before returning. (Users should make sure that Stuffit Expander* has its "check for new versions" option disabled; otherwise a dialog may interrupt script execution.)

Linux RPM

These are packages in Linux RPM format. These packages must be stored on a Web share for Linux RPM distribution to work.

LANDesk Application Virtualization:

LANDesk Application Virtualization uses Thinstall technology to virtualize an application, storing it in a single self-contained executable file with the application and the .DLL/device driver dependencies. When run, virtualized applications run in an isolated environment without making changes to the Windows installation they are run on.

Virtualized applications run on locked-down devices without requiring additional privileges.

Virtualized applications generally consist of one or more executable files. Software distribution can be used to deploy virtualized application executable files to managed devices. Any of the software distribution delivery methods are used with virtualized application packages, including the Run command from the source. When deploying a run from source virtualized application package, managed devices use an application shortcut icon to run the virtualized application executable file over the network.

Windows Script Host Package (.WSF):

Windows Script Host Packages (WSH) are Microsoft Software's new alternative to batch files but are often used to automate similar tasks such as mapping drives, copying files, or modifying registry keys. The WSH files are most commonly used with Jscript (.JS) and VBScript (.VBS). One major advantage of the Windows Script Host package over the .bat package is that they allow the user to combine multiple languages into a single file by using the language independent file extension (WSF). These packages are often can be created in notepad, HTML editor, Microsoft Visual C++, or Visual InterDev.

SWD package

These are packages built with the legacy LANDesk Enhanced Package Builder (installed separately). Although the Enhanced Package Builder is no longer shipped with Management Suite, LANDesk Software continue to support the distribution of files having been created with it. They are executable files that have properties that uniquely identify them as software distribution (SWD) packages.

Understanding the available delivery methods

Software distribution provides these delivery methods:

- **Push:** The packages may be multicast out to the managed devices. The core server then initiates package installation at the managed devices.
- **Policy:** The core server makes the packages available for download. When a managed device checks for available policies, the package will be returned. Depending on the policy type, devices may install the package automatically or make the package available to users for them to install when they want.
- **Policy-supported push:** The combined push distribution and policy model. First, software distribution attempts to install the package on all devices in the target list. This way, you can do an initial deployment using Targeted Multicast. Second, any devices that didn't get the package or that later become part of the target list (in the case of a dynamic target list) receive the package when the policy-based management agent on the device requests it. Generally, this is the recommended delivery method.
- **Multicast (cache only):** Multicasts the package to the target devices, no other action is taken on the managed device. The result is the package is cached locally on managed devices. Use this option to multicast the package to a few devices on each multicast domain. You can then create a task that uses the **Peer download (only install from cache or peer)** option. This allows you to regulate network bandwidth used for the distribution so it doesn't span multicast domains.

Note: LANDesk has included default delivery method configurations for each of these delivery method types. These default methods have default settings that should work well in most environments. If you want to modify one of these defaults, you may want to use copy and paste to create a duplicate delivery method that you can then rename, preserving the defaults for future reference.

Software distribution core server components

The following components of software distribution run or reside on the core server:

- **LANDesk scheduled task handler:** This program (ScheduledTaskHandler.exe), launched by the scheduler service, starts a distribution job.
- **LANDesk scheduler service:** The console stores information about scheduled jobs in the database. The scheduler service (SCHEDSVC.EXE) monitors the information in the database to determine when tasks should be run.
- **Distribution package:** When you select a software distribution package in the **Distribution package** window, it stores this definition in the database. This definition is used by Management Suite when creating the commands that will be sent to the devices to install the packages.
- **Software distribution packages:** A package can be one or more MSI files, an executable, a batch file, a Macintosh package, a Linux RPM package, a Windows script host package, an application virtualization package, or a package created with the legacy Management Suite package builder. In most cases, the software package needs to contain everything necessary to install the application you're distributing.

Setting up the delivery server

The delivery server is the server that stores the software distribution packages. It can be either a Web server or a Windows file server. We recommend that for best results, the packages be URL-based. In general, properly configuring a URL is less work than configuring a UNC path.

HTTP package shares need to have the Internet Guest Account added with at least read privileges, since the packages will be accessed via anonymous HTTP.

UNC package shares need to have the Domain Computers group added with at least read privileges.

To configure a Web server for software distribution

These steps explain how to create a virtual directory on a Web server and enable it for browsing. In general, virtual directories need to allow reading and directory browsing, and anonymous access to the virtual directory must be enabled. Execute must not be set or the share won't work correctly. You also may want to disable write permissions so devices can't change the directory's contents.

1. Create a directory on the Web server where you want to store your software distribution packages. The usual location for such a directory on an IIS Web server is a subdirectory in the c:\inetpub\wwwroot directory.
2. Copy the packages to this directory.
3. From the Control Panel, double-click **Administrative Tools** and then **Internet Services Manager**.
4. In the right panel, double-click the icon with the device's name and then click **Default Web Site**.
5. In an empty area in the right panel, right-click and select **New,** then click **Virtual Directory**.
6. From the wizard, click **Next** and then enter an alias for your directory. Click **Next**.
7. Either enter the path or browse to a path and click **Next**.
8. In the Access Permissions dialog, enable **Run script** and **Browse**. This enables you to browse packages when creating a distribution package. Click **Next** and **Finish**.
9. From the shortcut menu for the virtual directory you just created, click **Properties**.
10. On the **Documents** tab, clear the **Enable default content page** option and click **OK**. Default pages can interfere with the share's ability to provide a directory that can be browsed.
11. On the **Directory Security** tab, click the **Edit** button in the **Authentication and access control** box. Make sure **Integrated Windows authentication** is checked. Also make sure **Digest authentication for Windows domain servers** is cleared.
12. To enable **Port 80** on the Web server, in the left panel, right-click **Default Web Site**.
13. Click **Properties**. In the **Web Site Identification** dialog, the **TCP Port** box should display 80. If it doesn't, click **Advanced** to add the port.
14. Ensure that the Web site is available by opening a browser and entering the URL for your Web server and virtual directory. For example, if the name of your Web server is Test and the name of the virtual directory is Packages, enter the following URL:

    http://Test/Packages

    A list of the packages you have copied to this directory should appear.

The size and number of packages you put in this directory is limited only by available disk space. Subdirectories can be created to logically group packages. Each subdirectory that's created must have the access permissions set, as described in the "To configure a Web server for software distribution" task above.

Once you copy the packages to a package share on a Web server, they're staged and ready to be copied to the target devices. When scheduled, the URL or UNC path of the package is passed to SDCLIENT.EXE (the device agent) as a command-line parameter. SDCLIENT.EXE manages the file transfer, starts the installation, and reports the status. Although the HTTP protocol is used for the file transfer, the status report is returned through the standard LANDesk agent.

The Web server communicates with the device to ensure that the package copies correctly. If the package transmission is interrupted during the download, the Web server can use the HTTP protocol to restart the download at the point where it stopped. The Web server doesn't check, however, to ensure that the package was installed correctly. That traffic is TCP-based, and it returns the status to the core server using the standard LANDesk agent.

Configuring a file server for software distribution

Devices that don't have a browser must receive distribution packages from a UNC path on a Windows network server. This can be the same folder as the one you set up on your Web server. If you're using preferred servers, you can configure authentication credentials for your UNC package share there, without having to configure a null-session share.

If you aren't using preferred servers or preferred server credentials, you'll need to make your package share null-session, which allows users to access the share without having to provide alternate credentials. Use the SYSSHRS.EXE utility to create a null-session share folder.

To configure a network server for software distribution

1. To set up a shared folder on your network server, right-click the folder you want to share and then click **Sharing**.
2. Click **Share this folder** and click **Permissions**.
3. Add the **Everyone** and the **Guest** groups, but grant them only read permissions. In a domain environment, also add the **Domain Computers** group and grant only read permissions. Apply the changes.
4. Configure preferred package server credentials as described in "Configuring preferred package servers" on page 156.
5. Copy the software distribution packages to this folder on the network server.

The size and number of packages you store on the network server is limited only by the available disk space.

Configuring IIS Web servers for software distribution

When hosting packages on a Microsoft IIS Web server, there is some additional configuration you need to do:

- Configure the virtual directory that hosts your packages.
- Register a MIME type with IIS.

IIS 6 handles virtual directories differently than IIS 5 (IIS 5 was the Windows 2000 Web server). On an IIS 6 server, if you select a directory and from its shortcut menu make it a Web share, the directory registers itself in IIS 6 as a Web application rather than a virtual directory. The problem is that as a Web application, when trying to select an executable file, the Web server attempts to run the file as a Web application rather than download the file to the user.

The resolution is to go into IIS, change the shared directory from a Web application to a virtual directory, and turn off execute permissions.

When hosting files on an IIS 6 server, files without a registered MIME file type will result in an HTTP error 404, File Not Found. This will resulting in the multicast and/or installation of the file failing unless you register MIME file types.

To register MIME file types

1. Launch Internet Information Services (IIS) Manager.
2. Expand the local computer in the tree.

3. Click **Web Sites > Default Web Site**.
4. From the package Web share's shortcut menu, click **Properties**.
5. Click the **HTTP Headers** tab.
6. Click **MIME Types**.
7. Click **New**.
8. In the **Extension** box, enter an asterisk (.*).
9. In the **MIME Type** box, type **application/octet-stream**.
10. Click **OK** twice and apply the changes.

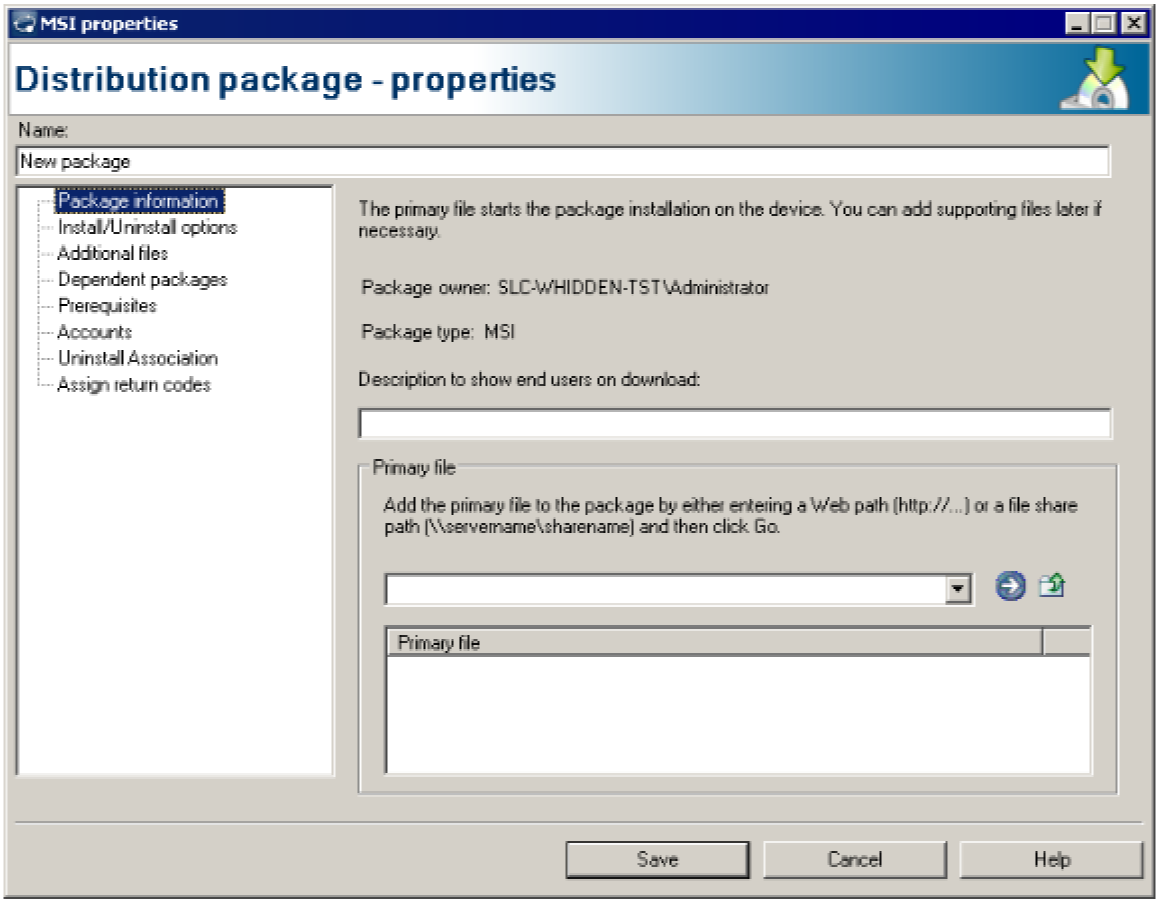
Distributing a package

A distribution package consists of the package file you want to distribute, any additional files needed by the package, and settings that describe the package components and behavior. You must create the package before you can create the distribution package definition for it.

These instructions explain how to create a software distribution package. For the package to execute correctly, the software distribution package must exist on either a network or Web server and the devices must have the software distribution agent installed.

There are three main steps required to distribute a package to devices.

Step 1: Create a distribution package for the package you want to distribute.



Name: New package

The primary file starts the package installation on the device. You can add supporting files later if necessary.

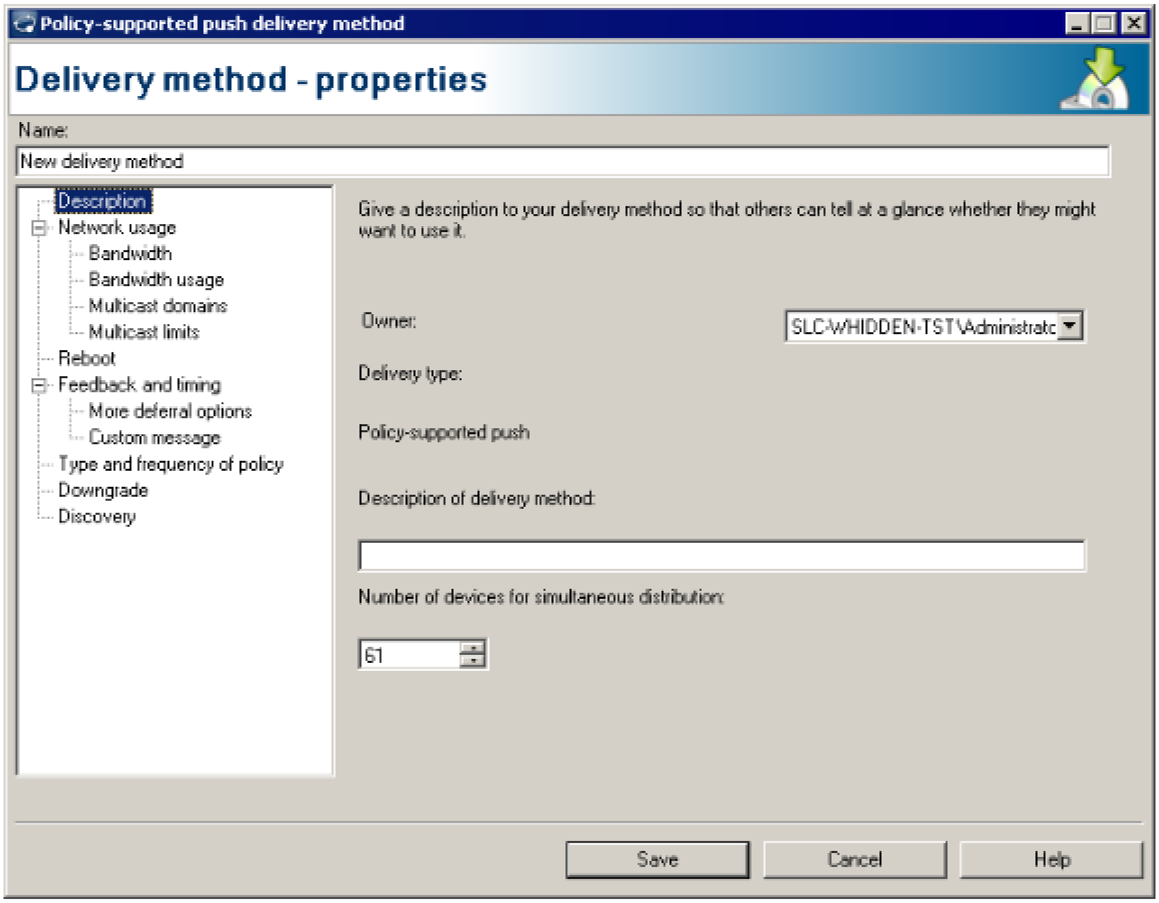
Package owner: SLC-WHIDDEN-TST\Administrator

Package type: MSI

Description to show end users on download:

Add the primary file to the package by either entering a Web path (http://...) or a file share path (\\servername\sharename) and then click Go.

Step 2: Choose the delivery method.



Name: New delivery method

Give a description to your delivery method so that others can tell at a glance whether they might want to use it.

Owner: SLC-WHIDDEN-TST\Administratc

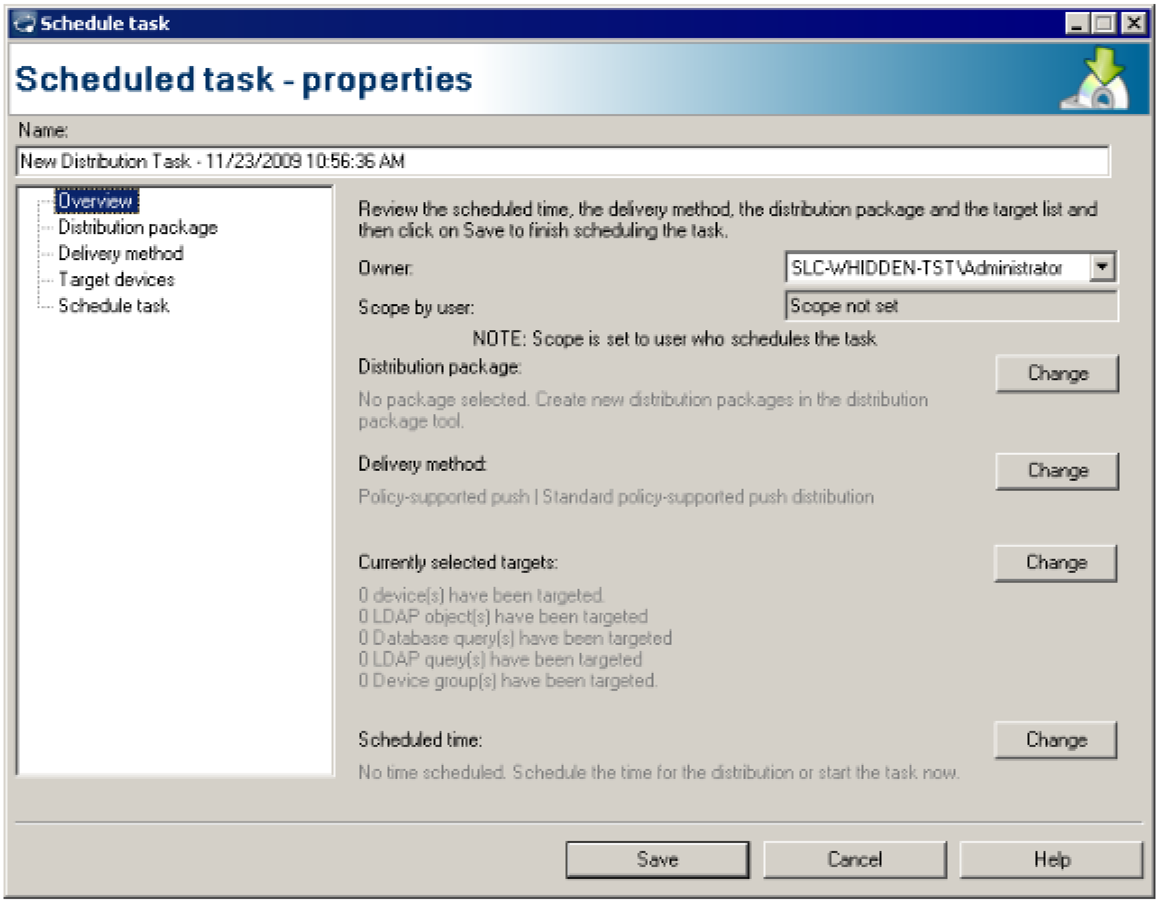
Delivery type:

Policy-supported push

Description of delivery method:

Number of devices for simultaneous distribution: 61

Step 3: Schedule the package and delivery method for distribution.



Name: New Distribution Task - 11/23/2009 10:56:36 AM

Review the scheduled time, the delivery method, the distribution package and the target list and then click on Save to finish scheduling the task.

Owner: SLC-WHIDDEN-TST\Administrator

Scope by user: Scope not set

NOTE: Scope is set to user who schedules the task

Distribution package:

No package selected. Create new distribution packages in the distribution package tool.

Delivery method:

Policy-supported push | Standard policy-supported push distribution

Currently selected targets:

0 device(s) have been targeted.
0 LDAP object(s) have been targeted
0 Database query(s) have been targeted
0 LDAP query(s) have been targeted
0 Device group(s) have been targeted.

Scheduled time:

No time scheduled. Schedule the time for the distribution or start the task now.

To create a distribution package

1. Create the package you want to distribute.
2. Click **Tools > Distribution > Distribution Packages**.
3. From the shortcut menu of the package group you want, click **New distribution package** > the package type you want to create.
4. In the **Distribution package** dialog, enter the package information and change the options you want. Note that you must enter the package name, description, and primary file. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the package type and owner you selected.

Note: LANDesk has included default delivery method configurations for each delivery method type. These default methods have default settings that should work well in most environments. If you want to modify one of these defaults, you may want to use copy and paste to create a duplicate delivery method that you can then rename, preserving the defaults for future reference.

To create a delivery method (only necessary if a default delivery method isn't ideal in your environment)

1. If you've already configured a delivery method that you want to use, or you are using one of the default delivery methods, skip to the next procedure, "To schedule a distribution task."
2. Click **Tools > Distribution > Delivery Methods**.

3. From the shortcut menu of the delivery method you want to use, click **New delivery method**.
4. In the **Delivery Method** dialog, enter the delivery information and change the options you want. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the delivery method and owner you selected.

To schedule a distribution task

1. Click **Tools > Distribution > Scheduled tasks**.
2. Click the **Create software distribution** task toolbar button.
3. On the **Distribution package** page, select the distribution package you created.
4. On the **Delivery Method** page, select the delivery method you want to use.
5. Click **Save** to save your changes.
6. From the network view, drag targets onto the task in the **Scheduled tasks** window. Targets can include individual devices, computer groups, LDAP objects (user, machine, and group), LDAP queries, and inventory queries.
7. From the task's shortcut menu, click **Properties**.
8. The **Target devices** page shows the devices that will receive this task.
9. On the **Schedule task** page, enter the task name and the task schedule.
10. Return to the **Overview** page and confirm the task is configured how you want it to be.
11. Click **Save** when you're done.

View the task progress in the **Scheduled tasks** window.

Working with distribution owners and rights

In environments where there are many Management Suite users, it can get confusing knowing which distribution packages, delivery methods, and scheduled tasks each user is responsible for. To help with this problem, Management Suite makes the user that created the distribution package, delivery method, or scheduled task the default owner of that item. Only the owner and RBA Administrators/Software distribution configuration users can see these private items.

Private items appear under the **My delivery methods**, **My packages**, or **My tasks** trees. Administrative users can see items for all users under the **All distribution packages**, **All delivery methods**, and **All tasks** trees.

When users create a distribution item, the **Description** page has an **Owner** option. Users can select **Public** if they want all console users to see that item. Administrators can select a specific user in addition to **Public**.

For more information on using role-based administration with software distribution, see "Software distribution" on page 56.

Using multiple distribution packages in a task

Push, policy, and policy-supprted push software distribution tasks can include a preliminary package and a final package. When using multiple packages, the packages are installed in order one at a time. The previous package must return a successful task status on all targeted devices before the next package begins installing.

Preliminary and final packages are useful in cases where you want to run commands before and/or after the main package. For example, you could create a batch file package that executes commands to configure the target device for the main package. After the main package finishes installing, you could specify a final batch file package that does any post-configuration. Any package type can be a preliminary or final package, but the delivery method must be push. The policy-supported push delivery method doesn't support preliminary and final packages.

You can specify preliminary and final packages when you schedule a distribution task. The **Scheduled task - properties** dialog's **Distribution package** page has the **Preliminary package** and **Final package** options. Before you can click one of these options, you must go to the **Delivery method** page and select a push delivery method. To do this, click **Push** for the **Delivery type** and click the **Delivery method** that you want to use.

To use multiple distribution packages in a task

1. Create the packages you want to use in the task.
2. Click **Tools > Distribution > Scheduled tasks**. Click the **Create software distribution task** toolbar button.
3. On the **Delivery method** tab, click **Push** as the **Delivery type** and click the **Delivery method** that you want to use.
4. On the **Distribution package** tab, click the **Package type** and **Distribution package** that you want to use.
5. Click **Preliminary package**, **Main package**, or **Final package**, depending on when you want that package installed, and click **Set**.
6. Repeat steps 4 and 5 for any other packages you want installed for this task. You can only have one package in each stage and you must always have a **Main package**.
7. Finish configuring the task and schedule it.

About file downloading

Software distribution has several methods for getting the file down to the device for installation. These include:

- Obtaining the file from the multicast cache
- Obtaining the file from a peer
- Downloading directly from the remote source

When a file needs to be downloaded, the device software distribution agent, SDClient, first checks the cache to determine if the file is located in the cache. The cache is defined as either C:\Program Files\LANDesk\LDClient\sdmcache or the path stored in the "Cache Directory" under the multicast registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM\Distribution\Multicast

The structure of files in the cache will be identical to the structure of the files on the Web or network server. This allows multiple packages to have files with the same name and not cause problems.

If the file isn't in the cache, SDClient will typically attempt to download the file from a peer in the network. You can configure the delivery method to require a peer download.

If the file can't be obtained from a peer, SDClient will download the files directly from the UNC or URL source. You can configure the delivery method so that if the file is to be obtained from the source, only one device in the multicast domain will download the file from the source location. Under most circumstances when downloading from a UNC share, this requires the UNC share to be a NULL session share. If the file to be downloaded is URL-based, SDClient will download the file from the Web site.

In either case, SDClient will put the file in the multicast cache. After it is put in the multicast cache, SDClient processes the downloaded file.

When a file is downloaded into the cache it will remain in the cache for several days, but is eventually deleted from the cache. The amount of time that the file will remain in the cache is controlled by the delivery method used when deploying the package.

Updating package hashes

Because many package files are obtained from peers in the network, the files are verified prior to installation. The integrity of the files are verified by comparing the MD5 hash of the file to the MD5 hash generated at the core server.

When a distribution package is first scheduled, Management Suite downloads the files and calculates the hash values associated with the primary file and any additional files used by the distribution package. If the hash stored with the package doesn't match the hash value SDClient computed on the target device, the download isn't considered valid.

If you make any changes to the package outside of Management Suite, such as updating the package contents, you need to reset the hash, or any scheduled tasks using the updated package will fail.

To reset a package hash

1. Click **Tools > Distribution > Distribution packages**.
2. From the shortcut menu for the package whose hash you want to update, click **Reset file hashes**. This can take a few minutes on large packages.

Running packages from the source server

Software distribution normally downloads package files to the local device's cache and then installs the package from the cache. This may not work well if a package or application expects installation files to be in a specific folder structure, such as with the Microsoft Office installer, or if the application installation doesn't use all source files for every installation.

For cases like these, you can instead have the local software distribution agent run the file directly from the source, whether that's a preferred server or the source specified in the package. When you enable run from source, software distribution won't download package files to the local cache, nor will it run the package from a peer.

When using run from source with packages stored on Web shares, the primary file must be an MSI file or SWD package. With UNC shares, the primary file can be any file type.

To create a delivery method that uses run from source

1. Click **Tools > Delivery methods > Network usage**.
2. Click **Use run from source to deploy files**.
3. Finish configuring the delivery method.

Using software distribution with packages on a distributed file system (DFS)

Distributed file systems (DFS) use several servers to provide files that are available from a single file share. Software distribution's default method of bandwidth detection in a DFS scenario ends up using the root server to calculate bandwidth, which may not be the actual server that provides the file. Software distribution now provides an optional way of calculating bandwidth. With this new method, bandwidth detection retrieves a small portion of the actual file being distributed. This way, software distribution calculates bandwidth from the server providing the file.

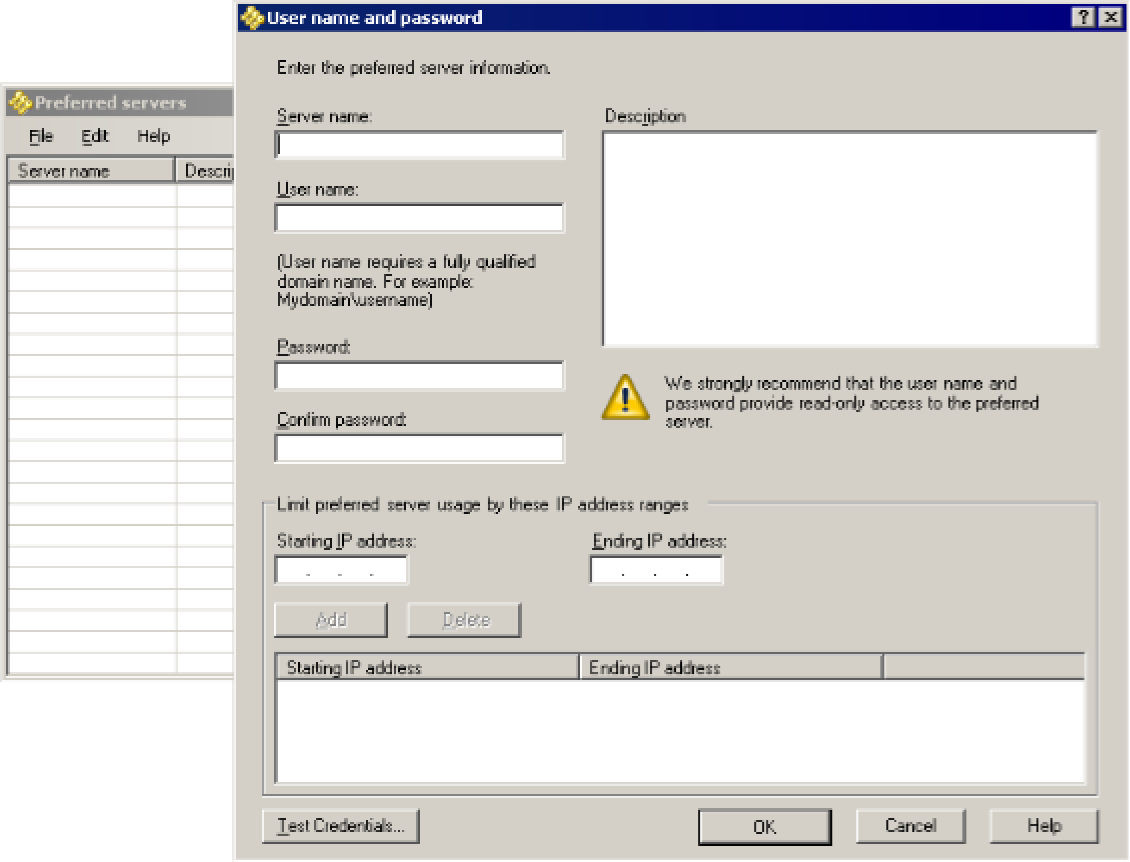
This alternate bandwidth detection method isn't enabled by default. You can enable this option from the ntstacfg.in# file in the core server's ldlogon folder. Once you update this file, the changes become part of new or updated agent configurations. You must redeploy your agent configuration to devices for the change to take effect.

Look for this section in ntstacfg.in# and make the necessary changes.

```
; The following registry values control detecting bandwidth by file download
; change the UseDownloadForBandwidth value to 1 to enable use of file download for
bandwidth detection
; the DownloadSize value should be entered as a Hex value between 400 and FFFF(1024 bytes
to 65535 bytes).
REG1=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\UseDownloadForBandwidth,
0, , REG_DWORD
REG2=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\DownloadSize, 2000, ,
REG_DWORD
```

Configuring preferred package servers

You can specify the preferred server that devices will check for software distribution packages. This can be important in low-speed WAN environments where you don't want devices downloading packages from off-site servers. When you specify preferred servers, you can also specify the credentials managed devices should use to authenticate with each preferred server. You can also specify the IP address ranges that preferred server will be available to.


Preferred servers
File
Edit
Help
Server name
Descri
User name and password
Enter the preferred server information.
Server name:
Description
User name:
(User name requires a fully qualified domain name. For example: Mydomain\username)
Password:
Confirm password:
We strongly recommend that the user name and password provide read-only access to the preferred server.
Limit preferred server usage by these IP address ranges
Starting IP address:
Ending IP address:
Add
Delete
Starting IP address
Ending IP address
Test Credentials...
OK
Cancel
Help

When using preferred servers with a distribution job, only the server portion of the UNC or URL file/package path is replaced; the rest of the path must be the same as what was specified in the distribution task. If the file isn't on the preferred server, it will be downloaded from the location specified in the distribution package. The only distribution method that doesn't support preferred servers is Multicast (cache only).

The core server also uses preferred servers. The core server uses distribution package hashes to verify distribution packages in scheduled tasks. The core server will first try to generate these hashes from a preferred server. Using a local preferred server makes the hashing process much quicker. If the package isn't available on one of the preferred servers, the core server falls back to generating the package hash from the path specified in the distribution package. You generally won't want the core server pulling a large package over the WAN link for hashing, so hashing files on a server that's local to the core will be much faster and use less low-speed bandwidth.

Managed devices store the preferred server list locally in the preferredserver.dat file. To create this file, a device communicates with the core server and then makes a filtered list of preferred servers (based on IP address range limits, if any). The device then does a bandwidth check to each preferred server and saves the top three servers in the preferredserver.dat file. Note that the bandwidth check doesn't produce guaranteed reliable results. For example, a server that's close by may have a high load at the time the agent checks, so it may get bumped off even if normally it's the best candidate.

The distribution agent updates the preferredserver.dat file every 24 hours or when the IP address changes. Not every device has to go through this process. Devices share their preferred server lists with peers. This is the process managed devices go through to maintain a current preferred server list:

1. If preferredserver.dat is in the local file cache, the distribution agent uses it.
2. If preferredserver.dat is on a peer, the agent retrieves the file from that peer.
3. If preferredserver.dat isn't available locally or on a peer, the device contacts the core server, creates a filtered preferred server list, and saves that locally as preferredserver.dat.
4. If preferredserver.dat is empty or if none of the preferred servers respond, the agent checks for a preferred server list in the local registry.

If none of these steps results in an available preferred server, the local agent uses the distribution path specified in the distribution job.

To configure preferred package servers

1. Click **Configure > Preferred server**.
2. Click **Add** to add a new server, or click an existing entry and click **Edit**.
3. Enter the server information. If you want to use IP address ranges that you want this server to be available to, enter them and click **Add**.
4. Click **Test credentials** to make sure the credentials you provided work.
5. Click **OK**.

Storing preferred package servers in the registry

The easiest way to manage preferred servers is with the **Server credentials** dialog (**Configure > Preferred server**). If you want to configure a fallback list of preferred servers that will be used if there are no servers in the preferredserver.dat file, you can create the following registry key on managed devices, and set the value to the preferred package server name. You can specify multiple package servers by separating them with semicolons.

- HKEY_LOCAL_MACHINE\Software\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\PreferredPackageServer

Here's a sample registry entry:

- [HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution]"PreferredPackageServer "="Server1;Server2;Server3"

Customizing the number of servers stored in preferredserver.dat

By default, the preferredserver.dat file contains three servers whose test results gave the highest bandwidth at the time of the bandwidth check, in order. You can change the number of servers stored in preferredserver.dat by updating this line in the ntstacfg.in# file in the core server's ldlogon folder. Valid numbers range from 0 to 7. Once you update this file, the changes become part of new or updated agent configurations. You must redeploy your agent configuration to devices for the change to take effect.

```
; Settings for the lddwnld/ldredirect files, the DynamicPreferredServers is the
; maximum number of preferred servers that will be stored. Set this to 0 to disable
; the dynamic preferred server functionality.
REG51=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\DynamicPreferredServers,
3, , REG_DWORD
```

Customizing preferred server prioritization

In order to prevent delays when the most preferred servers do not have a package, the redirection logic will start to prefer servers that have been actually providing files to the device. You can change the preferred server prioritization in preferredserver.dat by updating these lines in the ntstacfg.in# file in the core server's ldlogon folder:

```
; In order to prevent delays when the most preferred servers do not have a package
; the redirection logic will start to prefer servers that have been actually
; providing files to the client. The following registry options control when a
; server is moved up the list. The ServerHistoryUseCount value indicates the number
; of times a server must be used before it will be moved to the start of the list,
; the ServerHistoryCacheTime value indicates how long it should be remembered (in
seconds).
REG52=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHistoryUseCount, 3,
, REG_DWORD
REG53=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHistoryCacheTime,
3600, , REG_DWORD
```

Understanding UNC authentication

When you add preferred servers (**Configure > Preferred server**), you also provide credentials that devices should use when accessing the preferred server. For security reasons, make sure these credentials provide read-only access. Devices obtain these credentials from the core and use them to authenticate with that preferred server. When using preferred servers added to the **Server Credentials** dialog, you no longer have to configure your package shares to be null-session shares, as was necessary with previous versions. As long as the credentials you provide for the preferred server work with the package share (Click **Test credentials** in the **User name and password** dialog), managed devices should be able to access the share.

About byte-level checkpoint restart and dynamic bandwidth throttling

Management Suite 8 and later versions support distribution byte-level checkpoint restart and dynamic bandwidth throttling. Checkpoint restart works with distribution jobs that SWD first copies to the device cache folder (by default, C:\Program Files\LANDesk\LDClient\SDMCACHE). When a bandwidth controlling option is selected, the files get copied to the device cache first, and checkpoint restart allows interrupted distributions to resume at the point where they left off.

Dynamic bandwidth throttling specifies that the network traffic a device creates has priority over distribution traffic. This option also forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted. If you select this option and leave the **Minimum available bandwidth** percentage at 0, once the device initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops. Increasing the minimum available bandwidth preserves approximately the amount of device bandwidth you specify for distribution if the distribution needs network bandwidth and there is contention for bandwidth on the device.

If you're reinstalling or repairing an SWD package or an MSI package, you may not want to use the dynamic bandwidth throttling option, because these package types normally only download the files they need. Using dynamic bandwidth throttling in this case would force a full download of the package when a repair might normally only require a small portion of the package.

Dynamic bandwidth throttling isn't available on Windows 95, Macintosh, or DOS devices. Windows 98 and Windows NT devices can use dynamic bandwidth throttling if they have Internet Explorer version 4 or later installed.

You can configure collective bandwidth throttling so that only one device from the multicast domain will download from the remote source. You can also configure the amount of bandwidth used when downloading from the source. This feature is available on all versions of Windows systems. Collective bandwidth throttling isn't available on Macintosh or DOS systems.

Using Targeted Multicast with software distribution

LANDesk Targeted Multicast technology makes it possible to distribute large packages to many users across the network with a minimum of network traffic. Targeted Multicast features require no additional hardware or software infrastructure, and require no router configurations to allow multicast packets. You get the extraordinary benefits of multicast technology with none of its traditional headaches.

Targeted Multicast is designed to work with your existing software distribution packages. When you use Targeted Multicast, you can easily distribute software, even in WAN environments with multiple hops and low connection speeds (56k). Targeted Multicast uses HTTP for delivery from a Web site to a subnet representative. Management Suite's inventory scanner provides all the subnet information to the Targeted Multicast service.

Targeted Multicast provides unique benefits that standard methods of "multicast" don't provide. Inventory-based targeting of devices enables you to send a package to a selected group of computers that fit specific criteria via a multicast. Targeted Multicast is also simplified because there's no need to configure routers to handle deliveries.

When compared to conventional software distribution methods, Targeted Multicast significantly reduces the time and bandwidth needed to deliver software packages. Instead of sending a package across the wire for each device, only one transfer is made for each subnet. Bandwidth savings increase as the number of devices on each subnet increases.

You can activate Targeted Multicast from the delivery method properties by checking the **Use Multicast to deploy files** option on the **Network usage** page of the **Delivery methods** properties. Multicast is available in policy supported push, push, and multicast (cache only) delivery methods. Underneath the **Network usage** page you will find several pages that allow the multicast to be configured.

When you start a distribution using Targeted Multicast, you'll see the **Multicast software distribution** window. This window contains detailed information about how the distribution is proceeding. For more information about what each field means, click the **Help** button on the **Multicast software distribution** window.

Both Windows and Macintosh OS 10.2 devices support Targeted Multicast. Additionally, you can multicast OS deployment images.

Using peer download

Peer download is a Targeted Multicast option that forces targeted devices to install a package from the devices' local cache or from a peer on the same subnet. This option conserves network bandwidth, but for the package installation to be successful, the package must be in the local cache or a peer's cache.

If you don't select the **Peer Download** option, the Targeted Multicast device agent will still attempt to conserve bandwidth by checking the following locations for package files in this order:

1. Local cache
2. Peer on the same subnet
3. Package server

Copying files to the local multicast cache folder

You have the option of copying one or more files to the local multicast cache folder using multicast. This option copies a file to the target devices' local cache. It doesn't install the file or do anything else with it. This option is useful for getting files to multicast domain representatives or a device in each multicast domain. You can do an initial deployment to domain representatives and then redo the deployment with the peer download option to ensure devices only download the package from a peer on their subnet.

Configuring Targeted Multicast

Before using Targeted Multicast, you need to make sure the Targeted Multicast components are in place on the subnet you're distributing to. Targeted Multicast requires Management Suite 8 agents and a multicast domain representative.

To manually specify which computers will be multicast domain representatives

1. In the network view, click **Configuration > Multicast Domain Representatives**.
2. Add domain representatives by dragging the computers you want to be representatives from the network view into this category.

Targeted Multicast will use the first computer that responds per subnet in the **Multicast domain representatives** group.

Only Windows computers can be multicast domain representatives. If you are using multicast to distribute packages to Macintosh computers, make sure there is at least one Windows computer in the multicast domain that can act as a domain representative for the Macintosh computers. If you only have a few Windows computers in a predominantly Macintosh environment, it's best to manually specify Windows domain representatives in the Multicast Domain Representatives group.

You can throttle multicasts by changing the bandwidth sliders in the **Bandwidth usage** page under the **Network usage** page on the **Policy-supported Push**, **Push**, and **Multicast** delivery method windows.

You can also customize Targeted Multicast options in the Configure Management Suite Services dialog. To configure the Targeted Multicast service, click **Configure > Services > Multicast** tab. Click **Help** on that tab for more information.

Running an application under the context of the currently logged-on user

LANDesk Management Suite performs most application installations and other tasks using full system privileges. Some application installations and other tasks need to be performed as the system's current user. As part of the release of LANDesk Management Suite 8.7 SP2, a new utility, the STARTASUSER.EXE application, is available that makes it possible to run an application under the context of the currently logged-on user.

STARTASUSER.EXE will launch the supplied command line in the context of the user currently logged onto the system. STARTASUSER.EXE supports the following command line format:

```
startasuser.exe [///silent] [///timeout=x] [///?] command line...
```

If no user is logged onto the system when STARTASUSER.EXE launches, the application returns the standard Windows ERROR_NOT_LOGGED_ON (1245) error.

All of the command-line options for the STARTASUSER.EXE application are preceded with three forward slashes (///); this is done to prevent confusion with command line options of the launched application.

The command line options are outlined in more detail below.

///silent

This option results in the created process being started as hidden, this should prevent any windows of the application displaying.

///timeout=x

This option controls the timeout (in seconds) for the launched application. If the launched application has not completed before the specified timeout has occurred, the startasuser.exe application will exit with the standard windows error WAIT_TIMEOUT (258).

///?

This option causes command line usage to be displayed to stdout. Because STARTASUSER.EXE is a windows application, the help will not display in the command prompt by default. Use the following command line to display help from within a command prompt:

```
startasuser.exe ///? > more
```

command line…

After any STARTASUSER.EXE options, specify the full command line for the application to be run.

The following two examples show how to use the STARTASUSER.EXE application to launch an executable or install an MSI.

To run an executable (in this case, regedit) as the currently logged-on user

1. Create a batch file with the following command line:
   startasuser.exe ///timeout=300 regedit.exe
2. Save the batch file on a file server set up for use with software distribution.
3. In the LANDesk Management Suite console, click **Tools > Distribution > Distribution packages**.
4. From the **My distribution packages** group shortcut menu, click **New distribution package > New batch file package**.
5. Add the batch file saved in step two as the main distribution package.

6. Save the distribution package.

This package can now be used in a software distribution task and will result in the regedit application being launched in the context of the user currently logged on.

To install an MSI package as the currently logged-on user:

1. Create a batch file with the following command line:
   startasuser.exe msiexec.exe /I <name>.msi
2. When creating the batch file replace <name> with the name of the MSI package to be launched. Add additional MSI command-line options if needed.
3. Save the batch file on a file server set up for use with software distribution.
4. On the same file server, preferably at the same location, add the MSI package and any additional files.
5. In the LANDesk Management Suite console, click **Tools > Distribution > Distribution packages**.
6. From the **My distribution packages** group shortcut menu, click **New distribution package > New batch file package**.
7. Add the batch file saved in step two as the main distribution package.
8. Save the distribution package.

This package can now be used in a software distribution task and will install the MSI package using the currently logged on user.

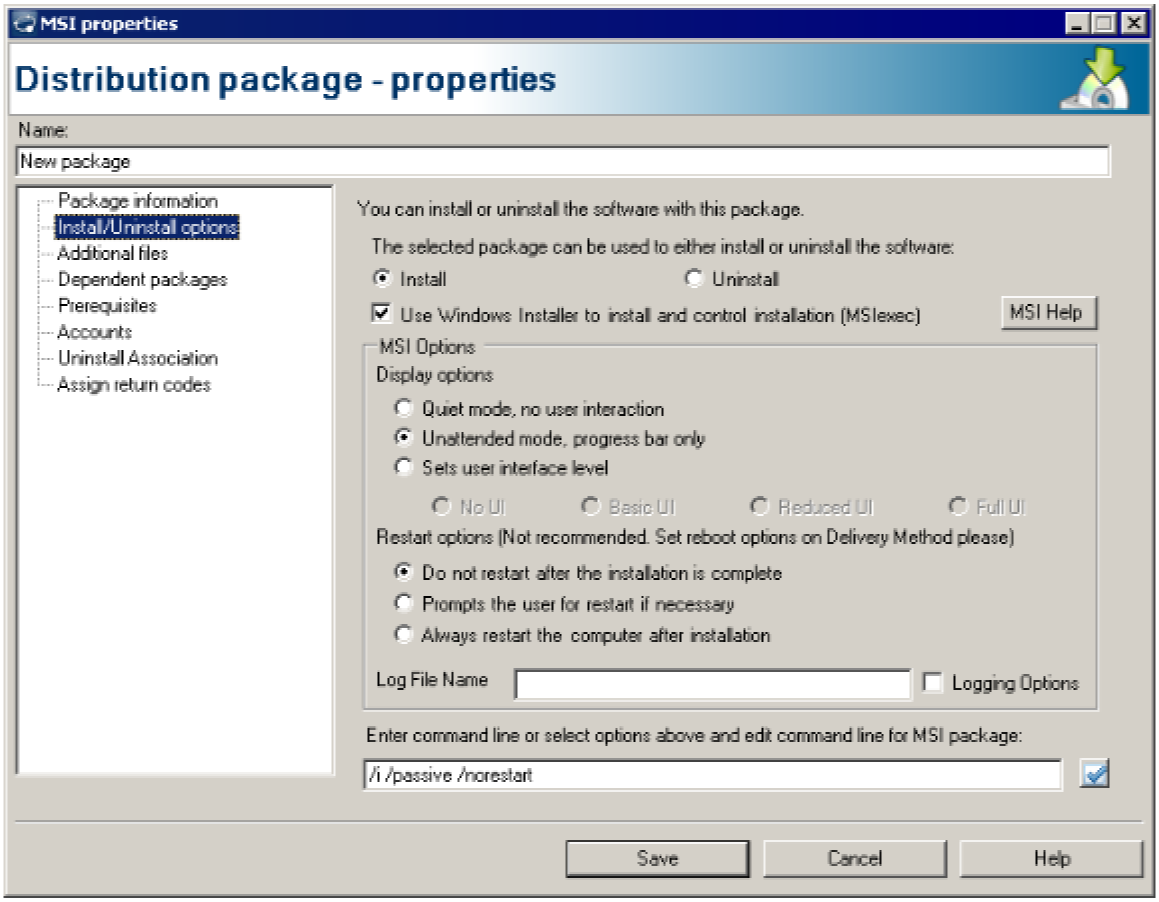
Using MSI distribution packages

Management Suite supports MSI installation with full status reporting and MSI package recognition. The MSI distribution package type is the Management Suite preferred method of software distribution. Understanding the MSI parameters will help you set up MSI packages and delivery methods.

Using MSI command-line parameters with software distribution

When installing an MSI distribution package, Management Suite leverages the MSI API calls. MSI installations use two different types of command-line parameters:

- Option parameters
- Property reference parameters



MSI properties

Distribution package - properties

Name: New package

You can install or uninstall the software with this package.

The selected package can be used to either install or uninstall the software:

● Install ○ Uninstall

☑ Use Windows Installer to install and control installation (MSIexec)

MSI Options

Display options

○ Quiet mode, no user interaction

● Unattended mode, progress bar only

○ Sets user interface level

○ No UI ○ Basic UI ○ Reduced UI ○ Full UI

Restart options (Not recommended. Set reboot options on Delivery Method please)

● Do not restart after the installation is complete

○ Prompts the user for restart if necessary

○ Always restart the computer after installation

Log File Name ☐ Logging Options

Enter command line or select options above and edit command line for MSI package:

```
/i /passive /norestart
```

Option parameters

Option parameters are the switches that are used by the Microsoft installation tool, Msiexec.exe. For example, the /q switch, is a common switch for Msiexec that silences an unattended installation.

In the **Distribution package-properties** dialog, you can enter MSI option parameters in the **Install/Uninstall options** page's **Command line** field. Click the checkmark button next to the field to validate the command line. More information on Msiexec options can be found at: http://support.microsoft.com/?kbid=227091.

Property reference parameters

Property references, also known as public properties, are specific to the MSI file. The parameters are passed to the MSI installation APIs directly. They can be used in the **Command line** field of an MSI distribution package's **Install/Uninstall options**.

The syntax of property references is PROPERTY=VALUE. A common property reference is the Transforms property. This is the property that calls up a .mst (transform) file. More information on property reference parameters can be found at: http://support.microsoft.com/?kbid=230781.

The information on an application's public properties can be obtained from the software installation documentation, the application's official web site, or by contacting the software vendor directly.

Running an MSI silently

In Management Suite, running an MSI silently is automatically handled under the **Install/Uninstall options** for a delivery method. To run an MSI silently, go to the **Install/Uninstall options** page for the desired delivery method and click **Quiet mode, no user interaction**.

Automating an MSI installation

For many MSI's, silencing the MSI also automates the installation. In such cases, all you need to do to automate an MSI installation is select **Quiet mode, no user interaction** in the delivery method.

Sometimes a property reference is required for the installation to complete. In such cases the MSI installer will prompt for a value. During an automated installation, no such prompt will occur. The MSI installation will fail with the standard MSI error 1603, Fatal error during install. Required public properties should be assigned a value in the distribution package's **Command line** field.

Using a transform file with an MSI installation

Answer files for MSI's are called transform files and end with a .mst extension. Not all MSI installations need a transform file; however, a transform file can be used if there are too many property references that need their values changed or assigned. If supported by the application, an answer file may be created to pass in all property reference parameters.

If a transform file is required but not provided during the installation, error 1603, Fatal error during install, will be the result. Often the software vendor will have the information needed or a tool to create a transform file for their specific MSI. For example, to deploy the volume license version of Microsoft Office 2003, a transform file should be used. Microsoft has a tool called the Custom Installation Wizard that installs as part of the Office 2003 Resource Kit. The Office 2003 Resource Kit can be downloaded from the following web site:

- http://download.microsoft.com/download/0/e/d/0eda9ae6-f5c9-44be-98c7¬ccc3016a296a/ork.exe

If the vendor doesn't have the needed information or such a tool, Microsoft provides a tool called Orca that can create a transform file. For additional assistance, refer to the Orca help file.

Handling reboots with an MSI installation

Management Suite handles MSI reboots using the **Reboot** page in the delivery method properties. LANDesk will automatically pass both the REBOOT=REALLYSUPPRESS and the /NORESTART parameters when **Never reboot** is selected in the delivery method.

The **Always reboot** option passes the /FORCESTART parameter.

Reboot only if needed allows the MSI to handle the reboot. If feedback is enabled, the user can be prompted as to whether to reboot. It is important to know that MSIs support custom actions. If a custom action initiates a reboot, Management Suite can't prevent this.

MSI checklist

If a deployment involves an MSI, follow this checklist.

- I have the correct version of the installation files, including the MSI and all additional files, for a volume license deployment.
- I have the information from the software vendor on how to automate and silence the software installation and configuration, and how to handle reboots.

- I know what public property parameters I need to pass to the MSI.
- I know whether this MSI needs a transform file to install and if so I have created one.

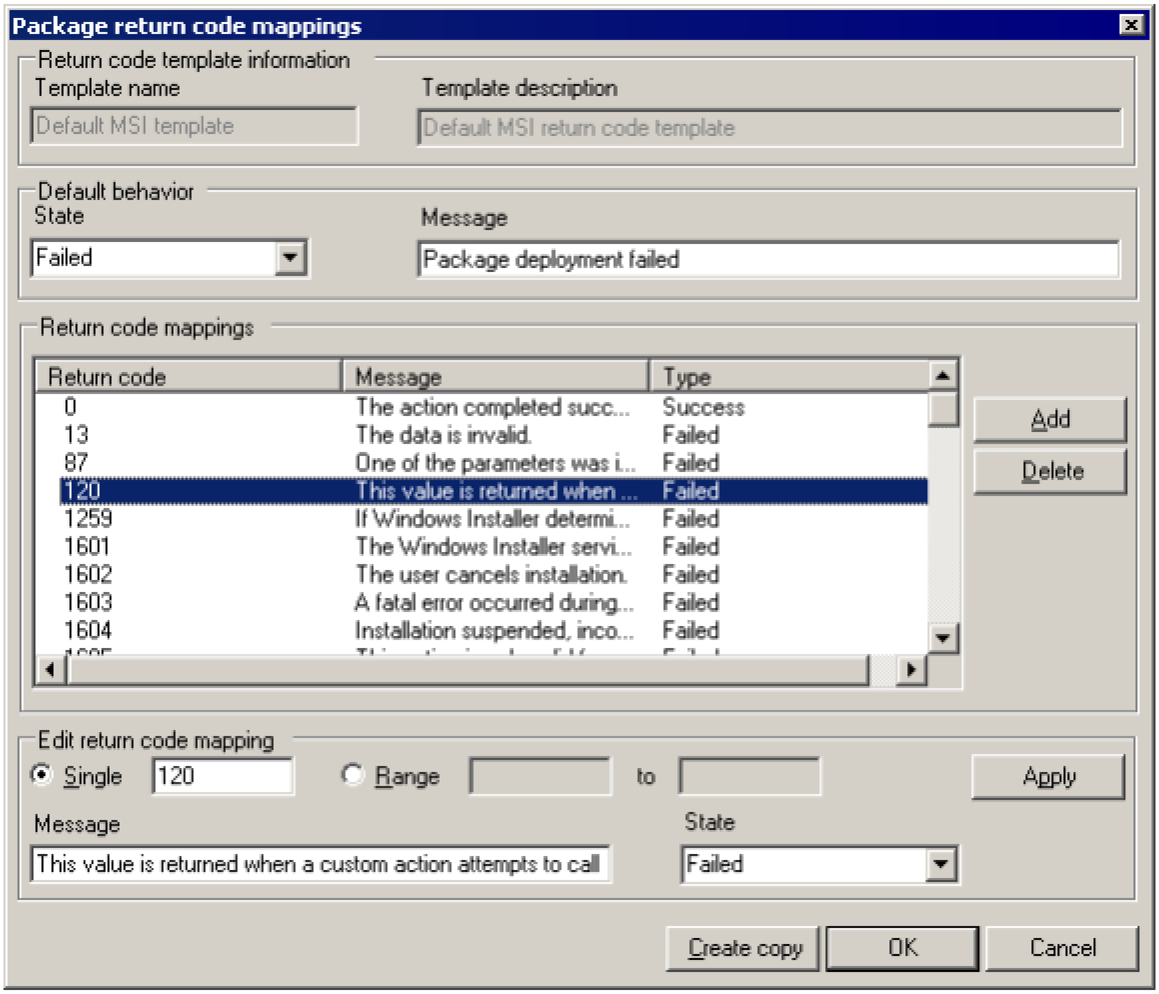
Assigning return codes

The Assign return codes dialog box is used to send status back to the Core Server based on whether or not a distribution task was successful. In the past Management Suite only read 0 as a success and anything else would be treated as a failure. This would pose issues for administrators as the application may have installed without error, however, because the return code was sent back as a number other than 0 Management Suite would indicate failure.

Vendors maintain lists created by product developers of all possible return codes and the specific outcome developers were coded to indicate. Now Management Suite has added the ability for administrators to look up return code lists and build templates that can be associated with individual or multiple packages. Each return code can be designated by the administrator to indicate success or failure and send back a custom message indicating specific results of the installation. Management Suite now ships with a Windows installer process for Office 2003 and Office XP templates. For more information on the return codes included in this template go to: http://support.microsoft.com/kb/290158.

In addition to using this feature with third-party vendor applications, Return code templates can also be created for proprietary in house applications written by internal developers. Management Suite provides a default template as well as the ability to create new custom templates, copy the default or custom templates, or make modifications to any templates through the Return code template manager. When templates are created, a specific template can be associated with a specific package on the Assign return codes dialog box through the Package return code mappings window. Modifications to templates can also be made from this location.

Users have the option to add all possible return codes indicating success or failure or only add additional return codes that indicate success. In the instance that only success codes are added, any return codes not referenced in the template are automatically mapped as failures.



Package return code mappings

Return code template information

Template name: Default MSI template

Template description: Default MSI return code template

Default behavior

State: Failed

Message: Package deployment failed

Return code mappings

Return code	Message	Type
0	The action completed succ...	Success
13	The data is invalid.	Failed
87	One of the parameters was i...	Failed
120	This value is returned when ...	Failed
1259	If Windows Installer determi...	Failed
1601	The Windows Installer servi...	Failed
1602	The user cancels installation.	Failed
1603	A fatal error occurred during...	Failed
1604	Installation suspended, inco...	Failed

Edit return code mapping

● Single 120 ○ Range to

Message: This value is returned when a custom action attempts to call

State: Failed

There are two default templates included with Management Suite:

- **Default MSI template:** Contains over 50 mappings that cover standard MSI return codes.
- **Default non MSI template:** Contains a single mapping for return code 0, "The action completed successfully." All non-zero error codes return "Package deployment failed."

One of these templates is automatically assigned to the distribution package based on its type. You can change the template mapping in a distribution package's properties.

To use the Return code template manager

1. Click **Tools > Distribution > Distribution packages**.
2. On the **Distribution packages** toolbar, click the **Return code template manager** button.
3. In the **Return code template manager** dialog, click **Add, Modify, Delete, Import**, or **Export**.
4. Click **Save**.

To add a new return code mapping template

1. Click **Tools > Distribution > Distribution packages**.

2. On the **Distribution packages** toolbar, click the **Return code template manager** button.
3. In the **Return code template manager** dialog, click **Add**.
4. Enter a **Template name** and **Template description**.
5. Select a **Template filter type**.
6. Click **OK**.
7. In the **dfg** dialog box, if you want to change the default message for success or failure, select a **State** and enter a corresponding **Message** for that state.
8. Add a new mapping by clicking **Add**.
9. At the bottom of the dialog, enter the numeric return code or return code range.
10. Enter a **Message** and select a **State**.
11. Repeat steps 8-10 as necessary.
12. Click **OK**. Your new template appears in the list.

To apply the return code mapping to a distribution package

1. Click **Tools > Distribution > Distribution packages**.
2. Double-click the package you want to modify.
3. In the package properties tree, click **Assign return codes**.
4. Click the return code template you want to apply.
5. Click **Assign**.
6. Click **Save**.

Exporting and importing return code templates

Return code templates are stored in the core database, but you can export templates to an XML file and import them at other servers. If a distribution package is being synchronized through core synchronization, its assigned return code template is part of the synchronization data.

To export a return code template

1. Click **Tools > Distribution > Distribution packages**.
2. On the **Distribution packages** toolbar, click the **Return code template manager** button.
3. Click the template you want to export.
4. Click **Export**.
5. Browse for a path and enter a **File name**.
6. Click **Save**.

To import a return code template

1. Click **Tools > Distribution > Distribution packages**.
2. On the **Distribution packages** toolbar, click the **Return code template manager** button.
3. Click **Import**.
4. Browse for the XML file containing an exported template.
5. Click **Open**.

Using the software deployment portal

The Portal window is accessible through Desktop Manager on managed devices. The portal lists all software distribution package tasks that have been distributed using a policy based delivery method.

When you launch the Software Deployment Portal, it prompts you to wait while it synchronizes with the policy server to refresh the application list. During this time the policy sync is running and downloading any new policies. The required policies aren't displayed on the Software Deployment Portal window and start installing automatically (unless deferred by the end-user). The other tasks are displayed in the Software Deployment Portal window.

The managed device includes a policy invoker service that examines policies that are downloaded. The policy tasks are stored in a small database when retrieved. The invoker service monitors this database and updates that status of policies as they move from one state to another. It also reads the status of policies to determine if an installation needs to take place. The invoker doesn't install packages. It calls the software distribution agent (sdclient.exe), which does the install.

In addition to the policy update that happens when a user opens the Software Deployment Portal, these agent configuration options also affect policy update intervals:

- At logon if the **When user logs on** option is selected.
- When a user's IP address changes if the **When UP address changes** option is selected.
- At the local scheduler interval you specify when you click the **Change settings** button. By default, managed devices use the local scheduler to get policy updates once a day.

You can change these policy update settings on the agent configuration dialog's **Software distribution > Policy Options** page.

Distributing software to Linux devices

Once you've deployed the Linux agents, you can distribute software to your Linux devices. The initial Linux agent deployment uses an SSH connection. Once the agents are installed, the core server uses the standard LANDesk agent to communicate with the Linux server and transfer files. To distribute software to a Linux device, you must have Administrator rights.

You can only distribute RPMs to Linux devices. The Linux agents will automatically install the RPM you distribute. The RPM itself isn't stored on the server after installation. You can install and uninstall the RPM you specify using software distribution. You can only use push delivery methods with Linux software distribution. For Linux software distribution, the settings in the push delivery method are ignored, so it doesn't matter which push delivery method you select or what the settings in it are.

The distribution follows this process:

1. The core server connects to the Linux device through the Standard LANDesk agent
2. The device downloads the package
3. The device runs a shell script that uses RPM commands to install the RPM package
4. The device sends status back to the core server.

You can store Linux RPMs on HTTP shares. Linux software distribution doesn't support UNC file shares. For HTTP shares, make sure you've enabled directory browsing for that share. If you use an HTTP share on a Windows device other than the core, you need to configure IIS with the correct MIME type for RPM files. Otherwise, the default MIME type IIS uses will cause the RPM to fail to download the file.

To configure the RPM MIME type on Windows devices

1. From Windows **Control Panel**, open **Internet Services Manager**.
2. Navigate to the folder that hosts your distribution files. From that folder's shortcut menu, click **Properties**.
3. On the **HTTP Headers** tab, click the **File Types** button.
4. Click **New Type**.
5. For the **Associated Extension**, type **rpm**. Note that rpm is lowercase.
6. For the **Content type**, type text/plain.
7. Click **OK** to exit the dialogs.

Once you've hosted the files on your package share, create a new Linux distribution package in the **Distribution packages** window, associate it with the delivery method you want, and schedule the delivery.

Understanding Linux software dependencies

When you click **Save** in a Linux package's **Distribution package-properties** dialog, software distribution parses the primary RPM and any dependent RPMs you selected for dependencies those RPMs require. These dependencies then appear in the **Missing libraries** dialog. Checking a dependency in this dialog tells software distribution to not prompt you about it again. You can check dependencies you know are installed on managed devices. This dialog is for your information only. If a dependency is missing on a target device and you didn't specifically include that dependency as a dependent package, the RPM probably won't install successfully.

Troubleshooting distribution failures

Software distribution provides the ability to distribute packages to a large number of devices at once. If there is a problem with the package, or the software being deployed conflicts with already existing software, you have the ability to cause problems at thousands of devices at once. When planning a deployment using software distribution, take care to not overwhelm the help desk.

Before deploying a new package, test it with some test systems. Ideally, these test systems should include all of the operating systems and applications that are used in your environment. Once the package is deployed, confirm that all of the systems and applications are still working as expected.

Once the package has been validated against test systems, do a limited deployment. Target a small number of devices in your environment. When deciding how many devices to target, the rule of thumb is not to target more devices than your help desk can handle. Once the package has been deployed to these devices, let the software sit for a couple of days to see if users encounter any problems.

After the initial deployment, you can begin rolling out the software to other devices in the enterprise. The speed at which these roll outs occur should be based upon how much device variety the enterprise has and how much of a load the help desk can handle.

Here are some other problems you might encounter:

Scheduled task can't find package

If the scheduled task indicates that the package can't be located, make sure that the package can be viewed from the device.

If the package is URL-based, you can check to make sure it is accessible by using a Web browser. Remember, if your DNS is set up to resolve the package, you'll need to verify that the package has been distributed to all of the Web servers.

If the package can be viewed from the device but still does not download properly, the problem may be that the URL or UNC based package share doesn't allow anonymous access. Check the permissions on the UNC or URL share and make sure it allows anonymous access. For UNC locations, make sure it has properly been configured as a null session share.

Bandwidth detection doesn't work

One of the most common problems that can occur is having PDS set up for bandwidth detection. In device setup, one of the common base agent options is to choose between PDS and ICMP for device bandwidth detection. When a device is configured to use PDS for bandwidth detection, it will only detect between RAS and non-RAS connections. So, if you configure a distribution to only work with high speed connection and the package installs on a computer with a WAN connection, check and make sure it is configured to use ICMP and not PDS.

Policy-based management

LANDesk Management Suite enables you to manage sets of applications on groups of devices using policy-based management feature.

Read this chapter to learn about:

About policy-based management

Policy-based management (known as application policy management in earlier Management Suite releases) helps you easily manage sets of applications on groups of devices. Like any other scheduled task, policies require:

- An SWD package, MSI, executable, batch file, or Macintosh package that you create.
- A delivery method that supports policies, either policy or policy-supported push.
- Policy targets for the distribution packages, such as the results of an LDAP or core database query.
- A scheduled time at which the policy should be made available.

Policy-based management periodically reruns queries you have configured as part of the policy, applying your policies to any new managed devices. For example, perhaps you have a Department container in your LDAP directory that contains user objects. Any user whose Department object is "Marketing" uses a standard set of applications. After you set up a policy for Marketing users, new users who are added to Marketing automatically get the correct set of applications installed onto their computer.

Use the console to configure application policies, which are stored in the core database.

Policy-based management can deploy these file types:

- MSI
- Executable
- Batch file
- Macintosh
- Linux RPM
- LANDesk Application Virtualization
- Windows Script Host Package (.WSF)
- Legacy SWD package

Here's the task flow for policy-based management:

1. Make sure the software distribution agents are on your devices.
2. If you don't have a package for the application you want a policy for, create one. For more information, see "Software distribution" on page 143.
3. Use the distribution packages window create a package definition for the package.
4. Create or select an existing policy-based delivery method.

5. Create a software distribution task in the **Scheduled tasks** window and select the package and delivery method from above.
6. Select the targets for the policy, this can include any combination of individual devices, database queries, device groups, LDAP items, and LDAP queries.
7. Schedule the task to run. When run, the distribution package will be made available for pull.
8. The policy-based management service on the core server periodically updates the policy target list by reevaluating the LDAP/database query results. This helps ensure that the core database has a current set of targeted users/computers.
9. A user logs on to a device, connects to the network, or otherwise starts the policy-based management agent.
10. The core server's policy-based management service determines the applicable policies based on the device's device ID and the logged-in user or LDAP device location.
11. The policy-based management service sends the policy information back to the policy-based management agent.
12. Depending on how you've configured the device to handle policies, the user selects the policies to run or the policies run automatically. Only recommended or optional policies are available in the list on the device. When an unprocessed recommended policy is in the list, it's checked by default. Periodic policies appear in the list once their execution intervals have lapsed. Selected policies execute sequentially.
13. The policy-based management agent sends the policy results to the core server, which stores the results in the core database. Policy-based management status is reported to the core server using HTTP for enhanced reliability. This status is reported in the Scheduled tasks window.

Configuring policies

Policy-based management requires a supported distribution package type for any policy you create. You can either create the packages ahead of time or you can create the packages while creating the policy. We recommend that you create the packages ahead of time to test them and ensure that they work before using them in a policy.

Normal distributions and policies can use the same distribution package. The difference is in the deployment, not the package creation. There are two delivery methods that support policy based distribution:

- **Policy delivery methods:** The policy-only distribution model. Only devices meeting the policy criteria receive the package.
- **Policy-supported push delivery methods:** The combined push distribution and policy model. First, software distribution attempts to install the package on all devices in the target list. This way, you can do an initial deployment using Targeted Multicast. Second, any devices that didn't get the package or that later become part of the target list (in the case of a dynamic target list) receive the package when the policy-based management agent on the device requests it.

The main difference between standard delivery methods and the policy-based delivery method is the policy-based **Delivery methods** dialog has a **Job type and frequency** page.

The job type and frequency options affect how target devices act when they receive the policy:

- **Required:** The policy-based management agent automatically applies required policies without user intervention. You can configure required policies to run silently. Any UI that appears on the device while a required task is installing should be non-blocking; in other words, the application being installed shouldn't require user input.
- **Recommended:** Users have the choice of when to install recommended policies. Recommended policies are selected by default on the device UI.

- **Optional:** Users have the choice of when to install optional policies. Optional policies aren't selected by default on the device UI.

You can also configure how frequently a policy can run:

- **Run once:** Once a policy successfully runs on a device, the device won't run that policy again.
- **Periodic:** When a recommended or optional policy is specified as being periodic, it will be removed from the UI when it's successfully processed and will be shown again in the UI after the specified interval has elapsed.
- **As desired:** Can be installed by users at any time.

To create a policy-based distribution

1. In the console, click **Tools > Distribution > Delivery methods**.
2. From the shortcut menu for either **Policy-based distribution** or **Policy-supported push distribution**, click **New delivery method**.
3. Configure the delivery method options you want. Click **Help** for more information on each page.
4. Set the **Type and frequency of policy** options you want.
5. Click **OK** when you're done.
6. Click **Tools > Distribution > Scheduled tasks**.
7. Click the **Create software distribution task** toolbar button.
8. Configure the task options you want and click **OK**.
9. With the policy-based distribution task selected, drag the policy targets to the right window pane.

Policy-based distributions take effect as soon as the policy task is started and there are targets resolved. Policy-supported push distributions take effect after the initial push-based distribution completes.

Adding static targets

Policy-based management can use static targets as policy targets. Static targets are a list of specific devices or users that doesn't change unless you manually change it. Add static targets by selecting individual devices from the network view as targets. Individual LDAP devices can't be added as static targets.

Adding dynamic targets

Policy-based management can use queries to determine policy targets. As of Management Suite 8, queries are stored only in the core database. For more information on queries, see "Database queries" on page 104.

Dynamic targets can include network view device groups, LDAP objects, LDAP queries, and inventory queries.

In order for devices to receive policies that are targeted through Active Directory or NetWare Directory Services, they have to be configured to log in to the directory. This means that they need to have all the correct agent software installed, and they need to actually log in to the correct directory so that their fully distinguished name will match the name that was targeted through Directory Manager and Scheduled Tasks Application Policy Manager.

Windows 95/98 and NT devices need to be configured to log in to the domain where the Active Directory resides. Windows NT and Windows 95/98 don't include Active Directory support. You must install Active Directory support on devices that log in to a directory and require policy-based management application policy management. As of this printing, more information on installing Active Directory client support was available here:

http://www.microsoft.com/technet/archive/ntwrkstn/downloads/utils/dsclient.mspx

In order to target a device from LDAP, each Windows NT/2000/2003/XP device must have a computer account on the Active Directory domain controller. This means that the computer being used as the device must be logged in to the domain where the Active Directory exists. You can't simply map a network drive using the fully-qualified Windows NT domain name. The policy won't take effect this way.

To use Directory Manager to create a query

1. Click **Tools > Distribution > Directory Manager**.
2. Click the **Manage directory** toolbar button.
3. Enter the directory URL and authentication information and click **OK**.
4. Click the **New query** toolbar icon.
5. Create your query. For more information, see "LDAP queries" on page 108.

Adding additional targets

When creating a policy-based task, it is often a good idea to initially deploy the policy to a small target set. This is done so that if problems are encountered when deploying the policy it will only impact a small set of users. Once the results of the deployment to the small set of users have been validated, add additional targets to the policy. When new targets are added to an active policy task, the policy immediately becomes available to the newly-targeted devices or LDAP items.

Applying scope to application policies

Multiple scopes can filter the policy-based management target details pane for a target lists. However, the final scope that a policy uses is always the scope of a task owner. If the policy task is listed in **Common tasks**, and another Management Suite user with a different scope looks at the target details pane for the task (let's call this second person a target list "editor"), the target details pane is filtered by the editor's scope. In this case, the editor may not see all the targets the policy will be applied to in the target details pane, because the editor's scope may not allow them to see all targets in the creator's scope.

What users see on their devices

Application policies are always processed using a pull model. Devices check with the core server for new policies that might apply to them. When this check occurs, a dialog appears at the device showing only unprocessed, recommended and optional policies, not required policies. When an unprocessed, recommended policy appears in the UI, it is checked by default to encourage the end user to process it.

Once a policy is processed, it may still show up in the UI if it's set up to run periodically. If this is the case, it will continue to be selected, even if it's a recommended policy. A policy may also continue to appear in the UI if it wasn't applied correctly.

Users can manually launch the policy-based agent by clicking **Start > Programs > LANDesk > Policy-based delivery**.

Using the local software deployment portal

The software distribution agent on managed devices also provides a software deployment portal. The portal checks the local software distribution cache for policies that apply to the local device/user. The portal then displays a Web page listing available policies. Users can select a policy from the list and click **Download selected** to install the packages associated with the policy.

To use the software deployment portal

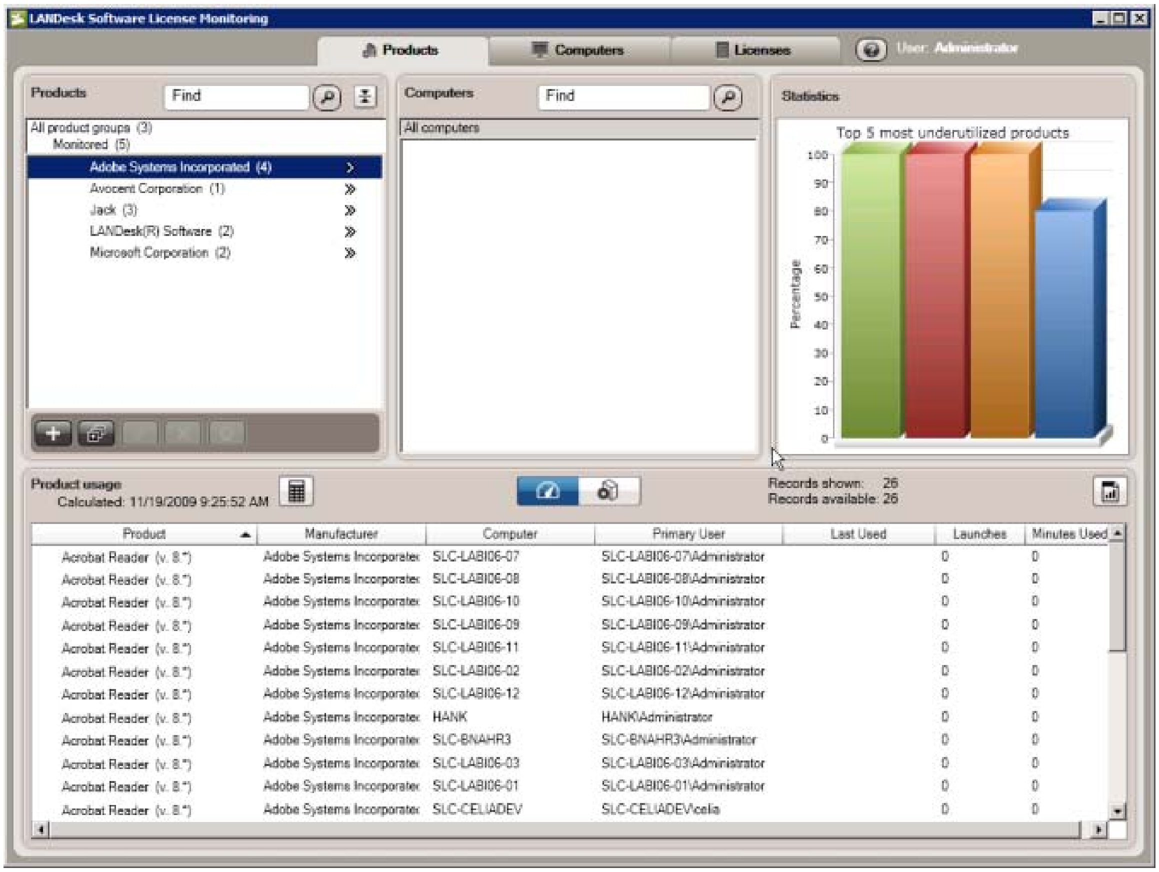
1. On the managed device, click **Start > Programs > LANDesk Management > LANDesk Software Deployment Portal**.
2. Click the policy you want to apply.
3. Click **Download selected**.

Software license monitoring

Software license monitoring gives you the tools to manage software assets so you can track software usage, monitor license compliance, and control costs in your organization.

IT administrators and software asset managers find it challenging to track product licenses installed on numerous devices across a network. They run the risk not only of over-deploying product licenses, but also of purchasing too many licenses for products. You can avoid these problems by using the software license monitoring console to monitor and report on product licenses and usage across your organization.

The software license monitoring console displays data from multiple perspectives (by products, computers, or licenses) and presents reports in multiple formats (such as HTML, PDF, and CSV). As you filter the data to find the products or licenses you want in a report, click the **View as report** button to create a report of the data currently being displayed.



Product	Manufacturer	Computer	Primary User	Last Used	Launches	Minutes Used
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-07	SLC-LABI06-07\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-08	SLC-LABI06-08\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-10	SLC-LABI06-10\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-09	SLC-LABI06-09\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-11	SLC-LABI06-11\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-02	SLC-LABI06-02\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-12	SLC-LABI06-12\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	HANK	HANK\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-BNAHR3	SLC-BNAHR3\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-03	SLC-LABI06-03\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-LABI06-01	SLC-LABI06-01\Administrator		0	0
Acrobat Reader (v. 8.*)	Adobe Systems Incorporatec	SLC-CELIADEV	SLC-CELIADEV\celia		0	0

More extensive reports are available in the LANDesk Management Suite Reports tool.

Software license monitoring features include:

- Passive, low-bandwidth monitoring. The software monitoring agent passively monitors product usage on devices, using minimal network bandwidth. The agent monitors usage for mobile devices that are disconnected from the network, and then sends the data to the core server when the device is connected to the network.

- Automatic product discovery scans for installed applications on managed devices, gathering data based on which files are associated with those applications. Product data is matched with a normalized database of over 22,000 product definitions.
- Product license downgrading. For some products, a newer version of a product can loan a license to older versions, keeping your devices license-compliant at all times.
- Easily accessible reporting on application usage and license compliance.
- Extensive data reporting features, including number of times each licensed application was launched, last date used, and total duration of application usage.
- Easy configuration of license parameters, including purchase information, license type, quantity, and serial number.
- Installation tracking and reconciliation, including items you track such as the license holder and physical location of the device the license is installed on, as well as additional notes.
- Integration with LANDesk Asset Manager for current, complete information about installed applications and licenses in your asset management.

Read this chapter to learn about:

What's new in this version

Software license monitoring is designed to give you accurate data about your organization's use of software licenses, in a format that is readily accessible. New features and enhancements include the following:

- **New user interface:** Software license monitoring functionality is now managed in a new console that offers three perspectives (products, computers, and licenses) to give you the tools you need for the task at hand. In each perspective, two independent controls let you filter the data that's displayed in the bottom pane of the console.
- **Improved console performance:** The software license monitoring console displays inventory data from the database, but does not perform real-time updates. The new interface is designed to be responsive so you can quickly and easily find the data you need.
- **Usage calculation on demand:** Usage is calculated regularly, when inventory maintenance is run on the database. If you want to update the current data in between calculations, click the **Re-calculate usage** button to retrieve the most current data from the database.
- **Software license compliance calculations:** License compliance is calculated regularly, when inventory maintenance is run on the database. Data is updated from the inventory scans that have been run on your managed devices. You can also run compliance calculation on-demand in between regular calculations.
- **Normalized product data and more accurate recognition:** This version of software license monitoring is enhanced by a normalized database of over 22,000 product definitions, which makes it easier to identify which software products are in use. Installed products are recognized by executable files installed, file size, and other characteristics, so products are more accurately identified.

- **Improved ad-hoc reporting:** Six types of report outputs are now available when you click the **View as report** button, giving you the data that is displayed in the console, in the format you want. In addition, Management Suite includes predefined reports for license and product usage.
- **Role-based administration filtering for users:** A user's ability to view data is tied to the role and scope assigned to that user. Depending on the user's scope, some or all product, computer, and license data is displayed in the console. Only data for computers within the user's scope is displayed.
- **Dynamic product definitions:** You can now group different versions of a software product so they are reported as the same product. For example, minor (point) revisions of a product (such as version 9.0, 9.0.1, and 9.1) can be combined in a single product definition with a wildcard (9.*) version. This reduces the number of different products you manage.
- **Flexible product types:** Product licenses are now defined as single products, dynamic products, and suite products, which include all the individual products that can be sold in a suite.

Notes about previous versions of software license monitoring

If you have used previous versions of software license monitoring, note the following changes in this version:

- **Compliance tree replaced by new console:** There is no longer a Compliance tree; this functionality is included in the new console. Computer groups are based on Management Suite groups and queries, so you can specify a scope for a product group when you define the group or query.
- **Denying use of products:** If you want to prevent users from installing or running specific software, use the **Application blocker** feature, which is now found under the Security group of tools (click **Tools > Security > Patch and compliance** in the Management Suite console). For more information, see "Creating custom definitions and detection rules" on page 324.
- **Managing software definitions:** To manage the software products that are tracked (which was formerly done by editing the LDAPPL3 files), you can now add product definitions in the software license monitoring console. When you do this, the product information is automatically added to the LDAPPL3 file so that inventory scans include the product you defined. To add products only for inventory scanning (but not for license tracking), use the **Manage software list** tool, which is a separate tool under the Reporting/Monitoring group of tools (click **Tools > Reporting/Monitoring > Manage software list** in the Management Suite console).
- **Inventory feature:** The list of files that the inventory scanner uses to identify products now includes the normalized product data that is added in this version. You can still create custom definitions, but we suggest that you look for existing product definitions before creating custom definitions.
- **Alias feature:** Aliases are now handled with wildcards in the license definition. You can associate different versions of a product under one product definition by using a wildcard (* character) in the version number. You can use the wildcard at any level, so you can combine all versions of a product (revisions 1, 2, and 3 with version "*") or all point revisions of a product version (revisions 4.0, 4.1, and 4.5 with version "4.*"). Manufacturer name aliases are now handled by the normalized software product data that is included in this product.
- **License data format:** The format of database tables containing license information has changed in this version. To import license data from a previous version, you need to export the old license data, reformat it using the new data structure, and import it into the database using the **Import licenses** button in the software license monitoring console. For instructions on importing data, see "Importing software license data" on page 189.

Integration with other LANDesk products

Software license monitoring is an important component of your overall IT asset management strategy. As a part of LANDesk Management Suite, this tool takes data from the inventory management of devices in your organization and gives you a way to determine where software is installed. As you define the software licenses you want to monitor, this tool helps you allocate licenses efficiently by providing a reporting structure that shows when you are in compliance with the licenses, and indicates where you can improve efficiency in license allocation.

To create a comprehensive software license management solution that includes discovery, advanced license definition, user entitlement, reconciliation, and license recovery, we recommend that you use LANDesk Asset Lifecycle Manager with LANDesk Management Suite. With Asset Lifecycle Manager you can define licenses in more detail, track license assignment, use automated process flows to managed licenses efficiently. Using Asset Lifecycle Manager, you can roll up license data from multiple cores and define automated flows that cover the full process of software licensing from user requests to reporting, compliance auditing, and recovery of unused software licenses.

Software license monitoring tasks

Any user with a role definition that includes software license monitoring can view and edit data in the software license monitoring console. Administrative users are assigned this role by default. Other users can be assigned View and Edit permissions for the Software license monitoring role.

There are a few basic tasks that you do to enable software license monitoring. These tasks are summarized below; specific instructions are found later in this chapter.

Gathering accurate software data

The Management Suite software monitoring agent gathers inventory data from managed devices about what software applications are installed, by which computers groups, and how often they are run. As you review this data you may find that some applications are not found or not recognized correctly. You can use the software license monitoring console to check for specific software, and if needed you can add or correct product definitions.

Choosing which software to monitor

When the inventory data has been saved to the inventory database, it is displayed in the software license monitoring console under the **Discovered** product super group. Your task is to select products from that list that you want to monitor. Those products can then be linked to your license data and can be tracked in the reports that show you how well your licenses match actual product usage.

Adding license data

You will need to add data about the software licenses you want to monitor. You can add this data manually, or import data from another source. Once you have added information about your licenses, such as how many licenses you have purchased, purchase date and expirations dates, type of license, and how the licenses are consumed, you will see compliance statistics and reports that compare the license data with actual software usage.

Creating reports

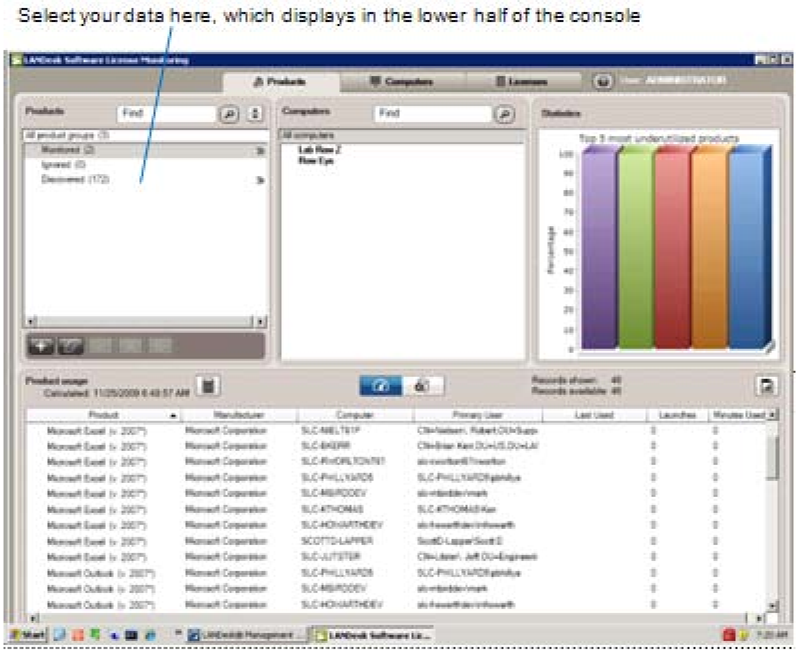
As you review software and license compliance data, you can generate a report of the currently displayed data. Reports can be formatted in six ways: HTML, PDF, CSV file, XML file, RTF document, and Excel spreadsheet (.xls) file.

When you have license and software data established in the database, you can also use the Management Suite reports feature to generate predefined reports with license and usage data. For more information, see "Reports" on page 113.

The software license monitoring console

The software license monitoring console is designed to let you view what software applications are discovered on your managed devices. The console offers three different perspectives—product, license, and computer—so you can focus on what's important to you.

After you select the perspective you want, use the top left and center panes to select data, which is displayed in the lower half of the console. As you select items, you filter the data to view specific products, computers, or licenses. When you have a group of data that you want to share, you can generate reports easily in six different formats.

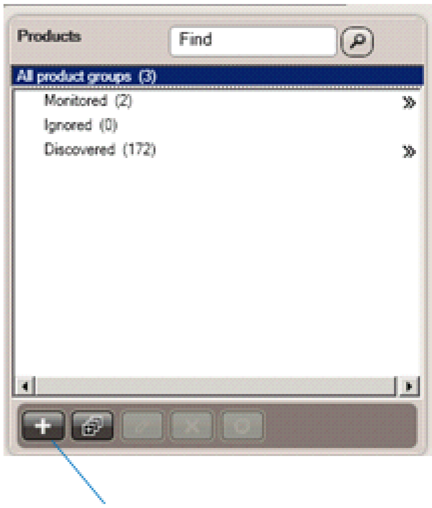

Select your data here, which displays in the lower half of the console

Product usage
Calculated: 11/25/2009 6:40:57 AM

Records shown: 40
Records available: 40

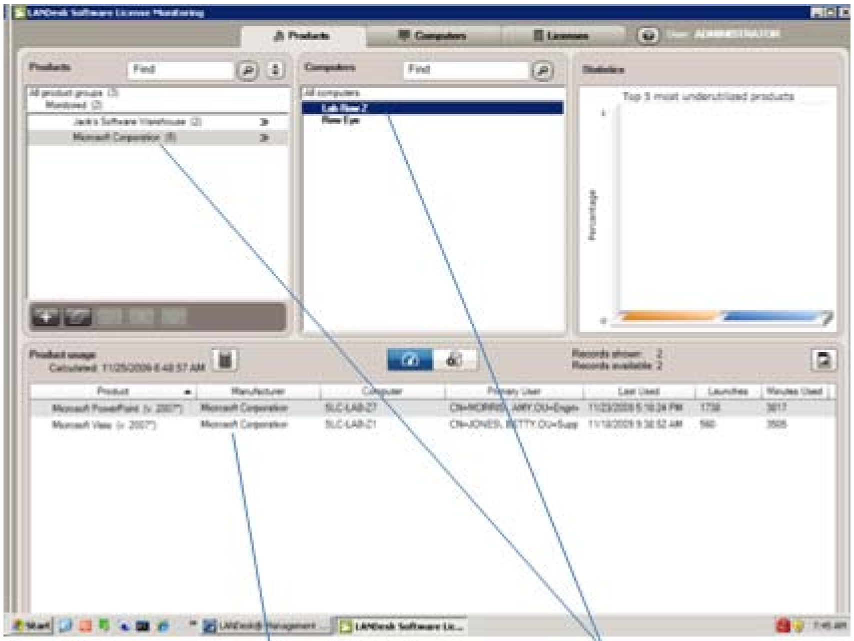
Product	Manufacturer	Computer	Primary User	Last Used	Launches	Minutes Used
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-NIELTSTP	CN=Nielsen, Robert OU=Supp		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-BKERR	CN=Brian Kerr OU=US,OU=LA		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-RHORLTONT61	slc-rnorlton\RTnorlton		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-PHILLYARDS	SLC-PHILLYARDS\phillya		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-MBRODEV	slc-mbrodev\mark		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-KTHOMAS	SLC-KTHOMAS\Kari		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-HOWARTHDEV	slc-howarthdev\nhowarth		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SCOTTD-LAPPER	ScottD-Lapper\Scott D		0	0
Microsoft Excel (v. 2007)	Microsoft Corporation	SLC-JLITSTER	CN=Litster\, Jeff OU=Engineeri		0	0
Microsoft Outlook (v. 2007)	Microsoft Corporation	SLC-PHILLYARDS	SLC-PHILLYARDS\phillya		0	0
Microsoft Outlook (v. 2007)	Microsoft Corporation	SLC-MBRODEV	slc-mbrodev\mark		0	0
Microsoft Outlook (v. 2007)	Microsoft Corporation	SLC-HOWARTHDEV	slc-howarthdev\nhowarth		0	0

After you have run inventory scans on managed devices, you will see a list of installed software under the Discovered product super group. From this group, you can choose which software products you want to monitor. You can choose to ignore some software, such as approved freeware that users may install. You don't need to monitor all software as you begin, so you can leave products in the Discovered group until you decide whether to monitor or ignore them.



Click the Add button to add products to the Ignored or Monitored list

As you navigate the window from the left pane, refine your search by using the top middle pane. For example, if you are viewing computer groups in the left pane, you can then select a product in the middle pane to see which computers have that product installed. As you select different combinations, the data in the lower pane changes to match your selections.



Product	Manufacturer	Computer	Primary User	Last Used	Launches	Minutes Used
Microsoft PowerPoint (v. 2007)	Microsoft Corporation	SLC-LAB-27	CN=MORRIS, AMY,OU=Engin	11/23/2009 5:18:24 PM	1738	3817
Microsoft Visio (v. 2007)	Microsoft Corporation	SLC-LAB-21	CN=JONES, BETTY,OU=Supp	11/18/2009 9:38:52 AM	560	3505

The data displayed in bottom pane reflects choices made in the top two panes

To use the software license monitoring console

1. Click **Tools > Reporting / Monitoring > Software license monitoring**.
2. To view different perspectives, click the **Products**, **Computers**, or **Licenses** tabs at the top of the window.
3. To quickly move to an item in any of the filter panes, type a name or partial name in the **Find** text box and click the **Find** (magnifying glass) button.

4. In the Products pane, click the **Hide automatically generated product groups** toggle button to show only the product groups you have created. Click the toggle button again to show the automatically generated groups.
5. To view a report of the data currently displayed in the lower pane, click the **View as report** button and select a report format.

The different views available in the console are described in the sections below.

Products perspective

Click the **Products** tab to view a list of product super groups in the left pane. This perspective is typically used by IT administrators. Three product super groups are displayed as defaults:

- Monitored
- Ignored
- Discovered

These default group names are displayed in a normal font. As you move products to the Monitored or Ignored super group, product groups based on manufacturer are automatically created (these are also displayed in a normal font). If you create other custom product groups, your group names are displayed in a bold font.

A custom product group includes any combination of products that suits your needs. Depending on whether you have chosen to monitor those products or ignore them, you'll see the product group displayed under the Monitored super group or the Ignored super group, or both.

To find a group or a product, click the chevrons (>>) to the right of a product group (or double-click the product group name). To return back to a product group, click the product group in the hierarchical list.

In the Products pane, a toolbar provides quick access to basic tasks:

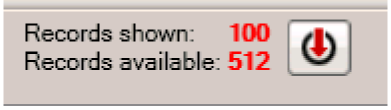
- **Add product:** Create a new custom product definition, with details about the product type and which files determine whether it is installed or has been run.
- **Add custom product group:** Create a group that contains related products you want to monitor.
- **Edit:** Modify the definition for a product.
- **Delete:** Remove a product from the Monitored or Ignored group. You can't delete a product that is referenced by a license or a suite product.
- **Move product:** Move a product from the Discovered super group to the Monitored super group. If the license for the product can be applied to multiple versions, specify the product version number with a wildcard character (*) to include multiple versions.

As you select different groups, manufacturers, or products, you'll notice that the contents of the lower pane change. There are two view options for the lower pane:

- **Product usage** displays a record for every computer on which the product has been discovered; if any type of group is selected, all products in that group are displayed with one record for each time the product is discovered. Columns include product name, manufacturer, name of the computer on which the product was found, the primary user of that computer, the date the product was last run, the number of launches since usage monitoring started or was reset, and the total number of minutes the product was used since monitoring started or was reset.
- **Product details** displays the product name, version number, and manufacturer of the selected product. From this list, you can right-click a product name and move it to the Monitored or Ignored group. You can also reset all product usage counts for this product on all computers.

Product usage view limitations

In the Product usage view, the first 100 records are displayed. To view more records, click the **Get all records** button. If you have a very large number of records, there may be a limit to how many you can view. No more than 10,000 records that can be displayed in the product usage view. If there are more than 10,000 records available, the **Get all records** button is not displayed because displaying so many records would cause the console to respond too slowly. In this case, if you want to display more than the first 100 records, you'll need to filter the data so a smaller number of records (less than 10,000) are displayed.

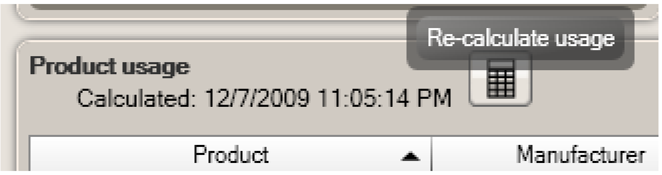

Records shown: 100
Records available: 512

Note: If your core server is running Windows 2003 Server, a limit on how much memory can be addressed by the operating system can prevent SLM from calculating usage correctly on more than 15,000 managed computers. If you need to calculate usage on more devices and if you have more than 3.6 GB of physical memory installed on your server, you'll need to change the settings in Windows 2003 Server so the OS can address more than its default limit of 3.6 GB of memory (see the article on large memory support available from Microsoft Support at http://support.microsoft.com/kb/283037).

Re-calculating usage

The data displayed in the Product usage view represents the composite of all inventory scans saved to the database. A time stamp indicates at what time the last product usage calculation was started. The product usage calculation is performed automatically, when your regular inventory maintenance is run on the database.

If you believe there is additional data from inventory scans that is not reflected in the product usage view, and you don't want to wait for the next automatic calculation, you can click the **Re-calculate usage** button to start a new calculation.


Product usage
Calculated: 12/7/2009 11:05:14 PM

If you have a large number of records, this calculation can take several minutes. Be aware that while the calculation is being performed, the reported number of available records reflects only the current number that have been processed. If the number of records changes or seems too low, the calculation has most likely not been completed. If you click the **Re-calculate usage** button again, the calculation will start over (so the number reported will change again).

Notes

- If you are unsure whether the calculation is still in progress, you can check the Windows Task Manager and look in the Processes list for ProductUsageCalculator.exe, which is the calculation executable.
- The daily time that inventory maintenance runs is specified in the inventory setting in Configure LANDesk Software Services: In the Management Suite Windows console, click **Configure > Services**, and then click the **Inventory** tab. The **Perform maintenance at** setting shows when maintenance runs.)
- In the Product perspective, you can normally right-click a discovered product in the lower pane and move it to the **Monitored** or **Ignored** group. However, while product usage is being calculated, the context (right-click) menu is inactive. If you have recently clicked the **Re-calculate usage** button, or if a calculation is in progress, you'll

need to wait until the calculation is complete before you can move products to another group.

- If you have deleted any computers from the Management Suite list of devices, the change will not be reflected in the software license monitoring console until the next time a usage calculation is performed. There will be a period of time in which the deleted computers will still be listed in the software license monitoring console.

Resetting product usage calculation

Normally, product usage is calculated from the first time a product is found in an inventory scan. Over time, you may have situations where you want to reset the calculation to get a more accurate picture of current product usage. For example, if a product has been installed for several months and used a few times on some computers, you can reset product usage calculation for that product on all managed devices. After you do this, the new usage data (number of launches and minutes used) will reflect only usage from the time you reset it.

To reset usage calculation for a product

1. In the software license monitoring console, click the **Products** tab.
2. Select a product group.
3. Click the **Show product detail records** button to display the **Product details** view.
4. Right-click the product and select **Reset product usage for this product**.

A task is scheduled to reset product usage, and the **Custom job processing** dialog box is displayed to show you the progress of the task. When it is completed, click **Close**.

If the task was not completed of any of the computers, that computer will continue to show the old usage calculations. This could happen with a mobile device that is not connected to the network at the time the task is run. Check the **Scheduled tasks** tool to make sure all devices have completed the task, and if needed, re-run the task on only those computers that failed when the task was run.

Computers perspective

Click the **Computers** tab to view a list of computer groups. This perspective is typically used by managers to view computers and software usage in their organizations. This perspective is also where you create computer groups that can be associated with licenses, if you want to track license usage for a division in your organization.

Computer groups listed here are based on the device groups or queries in your Management Suite network view. Items in **My devices** and **Public devices**, for example, can be selected as computer groups. Other groups you have created can also be selected, so you can view groups based on device type, functional groups within your organization, or other criteria you have used to create groups.

If you have defined queries in your Management Suite network view, you can use those queries to create dynamic lists in the software license monitoring console.

When you select a group in the Computers perspective, the lower pane displays all records for software installed in the computers that belong to the group.

As a default, the first 100 records are displayed in the lower pane. To view all records, click the **Get all records** button. If you have a very large number of records, you may be limited in how many records you can view. If this is the case, filter the data so a smaller number of records are available. (For additional notes, see "Product usage view limitations" on page 183.)

In the Computers pane, a toolbar provides quick access to basic tasks:

- **Add computer group:** Create a new group definition. Groups are based on the queries and device groups you have defined in the Management Suite network view.
- **Edit computer group:** Modify the details for a computer group.

- **Delete computer group:** Remove a group from the Computers list.

Resetting product usage on a computer

Normally, product usage is calculated from the first time an inventory scan is run on a managed device. Over time, you may have situations where you want to reset the calculation of all software running on a managed computer. For example, if a computer is reassigned to another user or other changes are made, you can start over with software usage calculation. After you do this, the new usage data will reflect only usage from the time you reset it.

To reset usage calculation for a computer

1. In the software license monitoring console, click the **Computers** tab.
2. Select a computer group and select one or more computers in the bottom pane.
3. Right-click the product and select **Reset product usage for selected devices**.

A task is scheduled to reset product usage, and the **Custom job processing** dialog box is displayed to show you the progress of the task. When it is completed, click **Close**.

Licenses perspective

Click the **Licenses** tab to view license data, grouped by software manufacturer, vendor, or the license groups that you create. This perspective is typically used by those who track license compliance for your organization.

This perspective is empty until you add or import license data. When you add license data, the manufacturer and vendor names are automatically used to create groups in the licenses pane. These groups are displayed in a normal font. You can also create groups to view any combination of licenses, such as all site licenses or all freeware. The groups you create are displayed in a bold font.

When you click a license group name, the licenses in that group are displayed in the bottom pane of the console. If a computer group is associated with the licenses, the licenses for only computers in that group are displayed in the bottom pane.

For example, if you monitor a software license for software that is used by your Advertising division, you can associate that license definition with an Advertising computer group. When you display that license, only the license details for the Advertising division are displayed in the lower pane.

In the Licenses pane, a toolbar provides quick access to basic tasks:

- **Add license:** Create a new license definition, with details about the number of licenses purchased, license type, manufacturer, and associated products. You can associate the license with a computer group if it only applies to computers in that group.
- **Add license group:** Create a group that contains related licenses you want to monitor.
- **Edit:** Modify the definition for a license.
- **Delete:** Remove a license from the list of licenses.
- **Import:** Import an XML file containing license data from another data source or from a previous version of Management Suite.

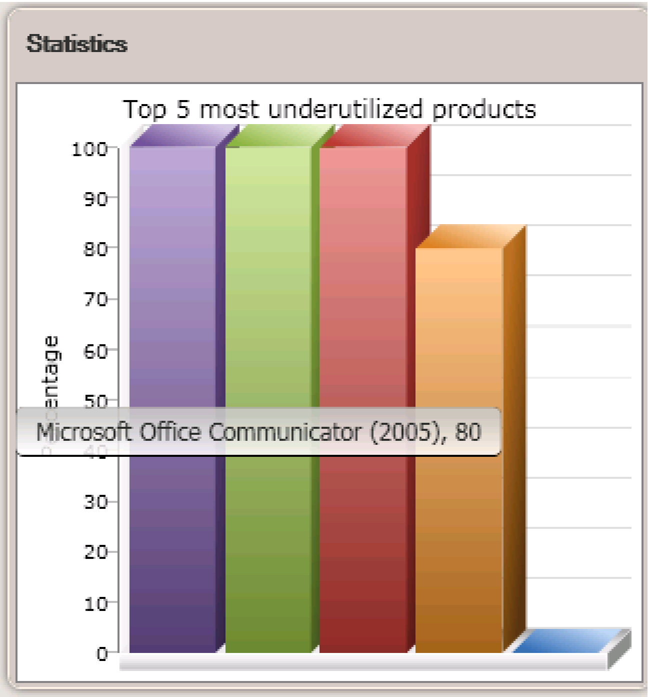
The statistics pane

The top right pane in the software license monitoring console displays charts that show you at a glance key information you can act on as you review software license usage. When you look at the Products and Computers perspectives, you'll see a chart that shows the five most underutilized products. When you look at the Licenses perspective, you'll see a chart that shows an overview of license compliance in terms of non-compliance and opportunities for saving money when licenses are underused. The graphs reference whatever data is displayed in the lower pane of the console.

Top 5 underutilized products

This graph shows up to five monitored products that are installed but not actively used. The calculation for this graph is tied to the Last used and Launches columns in the Product usage view. If there are products installed that have never been used, those products (and version numbers) are shown with the percentage of users that have never used the products. Hover your mouse pointer over the bars in the graph to view the product data.

You can use the data to review with employees in your organization whether they need to have licensed software installed on their computers, and possibly reduce costs by redistributing or not renewing those licenses.


Statistics
Top 5 most underutilized products
100
90
80
70
60
50
40
30
20
10
0
...entage
Microsoft Office Communicator (2005), 80

Compliance statistics

This graph shows three helpful situations in monitoring license compliance:

- **Non-compliant:** Shows the number of products installed on more computers than you have valid licenses. These products have a higher number in the Used column than in the Purchased column in the License details view.
- **Warning:** Shows the number of products that are within 10 percent of having all available licenses in use. This figure lets you know when you may need to purchase additional licenses or review the allocation of that software.
- **Opportunity:** Shows the number of products that are being actively used on less than 50 percent of the computers they're installed on. This gives you an indication that you

may be able to reduce costs by not renewing as many licenses for products that are unused.

For the Warning and Opportunity calculations, you can change the thresholds at which products are counted for these compliance issues. For example, you may want to know when you are within 20 percent of using all purchased licenses for a product. To modify these percentages, edit the settings in the SLM.View.exe.config file, found on the core server in the \Program Files\LANDesk\ManagementSuite folder.

Monitoring software usage

The LANDesk Management Suite software monitor scan runs when you schedule regular inventory scans. It monitors executable files that are running and compares application information on each device with a standardized database of software applications, matching the names and file sizes of executable files against the database.

Two other inventory scans help complete the picture with other data about software. These scans look at the Windows registry, uninstall keys, .msi files, shortcuts, and GUIDs to identify software products. All the scan data is then compared to give as complete a picture as possible of what software is installed on each managed device.

The software license monitoring console displays this summary of data in the Products perspective. Even if you don't have license data available, you can view this product data to find out on how many managed devices a particular software product has been discovered.

Adding product definitions

Most applications installed on your managed devices will be identified as matches with the software data included in this product, but in some cases there may be software that doesn't match the standardized data.

You can create custom products, which add product definitions for any unidentified software executable files. When you do this, the executable files in the product definition are automatically added to the list of executables that the inventory scanner looks for. You can specify which files indicate that software is discovered, and also define usage executables that are the applications used when the software is run on a computer.

To add a product definition to the database

1. Click **Tools > Reporting / Monitoring > Software license monitoring** to open the console.
2. Click the **Products** tab at the top of the window.
3. Click the **Add product** button (in the Products pane).
4. Type the name in the **Product** text box.
5. Select an entry in the **Manufacturer** list, or click the blank line and type a new manufacturer name.
6. Click a **Product type** (Single, Dynamic, or Suite). If you select **Suite**, a list of products from the manufacturer is displayed. Select the products that make up this version of the suite.
7. Type a number in the **Version** text box.
8. Click **Monitored product** or **Ignored product** to list this new product in one of those super groups.
9. (Single products only) Add filename tracking information for **Installation**. Click **Add** and specify the filename, size of the file, and version number for the product executable file. Repeat this for every product file you want to use to determine when the product is installed. Select **Match any** or **Match all** to specify whether all files must be found or only a minimum of one file must be found.

10. (Single and suite products only) Add filename tracking information for **Usage**. Click **Add** and specify the filename, size of the file, and version number of one or more files that can be used to determine when the product is used.
11. When all information is complete, click **Save**.

Monitoring software license compliance

Software license compliance is an important part of your overall IT asset management. You want to be able to show accurate compliance when your organization is audited, and if your organization has policies related to software usage, software license compliance can help ensure that employees are following your policies.

Your organization's compliance with the terms of your software licenses is dependent on:

- Accurate inventory scans that compile data on what software is discovered and being used
- Accurate data regarding the terms of the software licenses you have purchased
- Reconciliation of license data with inventory data

The first item is taken care of by the LANDesk Management Suite inventory scans that run on managed devices in your network. These scans include a software monitor scan that saves software information to the Management Suite database.

The second item needs to be added to the database from the license records that your organization has compiled. You can import data from different sources by exporting the data from an Excel spreadsheet to an XML file.

The third item is what the software license monitoring feature does when all data is available in the database. Compliance is calculated each day when regular inventory maintenance runs on the database (as specified in the Inventory tab of Configure LANDesk Software Services). The success of your software license monitoring depends on how accurately you have entered software license data, and how completely your inventory scans cover the devices in your organization.

Maintaining accurate license data

Someone in your organization maintains records of which licenses have been purchased, and this data needs to be available and accurate for compliance calculation.

If you are just starting with software license monitoring, you may want to begin with a small number of licenses, most likely the ones that need to be monitored for audits. You can enter or import that license data using the software license monitoring console. The data is then used to generate statistics (in the top right pane of the console) and reports.

Entering license data manually

If your license data is in a format not easily imported, you can enter the data manually in the Licenses perspective. The data you enter is stored in the database and is used to calculate compliance.

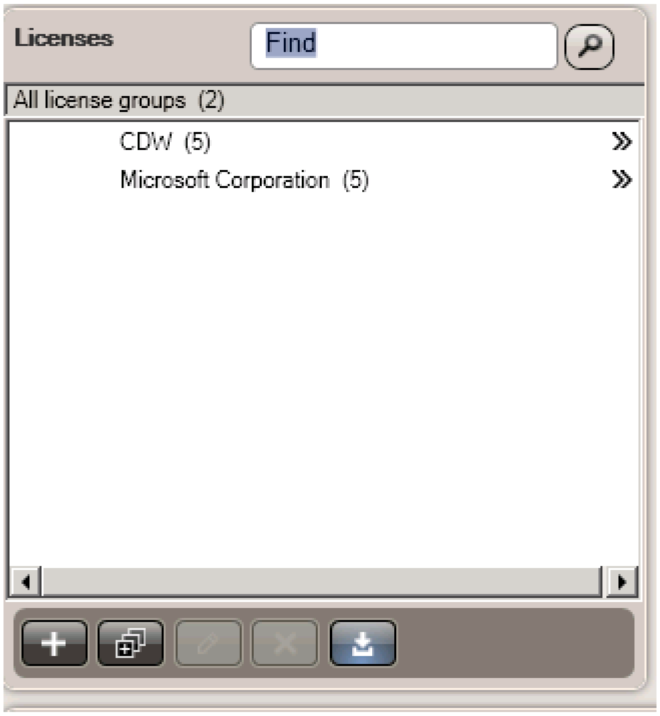
To add a license to the database

1. Click **Tools > Reporting / Monitoring > Software license monitoring** to open the console.
2. Click the **Licenses** tab at the top of the window.
3. Click the **Add license** button (in the Licenses pane).

4. Enter information in the text boxes, and click **Save** when you have finished. While you don't need to add data to all fields, you should at least enter a Name, License quantity, Manufacturer, and Primary product, and select options in Consumption and Compliance type, to have accurate compliance reporting.

Importing software license data

You can import existing license data from a previous version of LANDesk Management Suite or from another data source. The data must be saved as an XML file with a specific format. (If you are importing from a previous version, note that the format of license database tables in version 9.x is different than the format in 8.x versions, so you will need to modify the data format before importing.)



A sample Excel spreadsheet (LicenseImport.xls) is included in the LDMAIN share of the core server, for your reference. Any XML file that you use to import license data must be formatted with the same column headings, and the same order of columns, as in the sample spreadsheet. If the headings in your XML file do not match exactly, the data can't be imported.

A Product Name column is not included in the format for importing license data, so after importing your licenses you need to manually associate each license with a Primary product and, if needed, a Secondary product.

To import license data

1. From the original data source, export the license data as an Excel spreadsheet.
2. Open the sample spreadsheet (\Program Files\LANDesk\ManagementSuite\LicenseImport.xls) and note the column headings and order of columns. Edit the data in your spreadsheet so it matches the column order and column heading names in the sample spreadsheet.
3. In Excel, export your spreadsheet as an XML data file.
4. In the software license monitoring console, click the **Licenses** tab, and then click the **Import** button on the toolbar.

5. Browse to the location of the XML data file you just exported, and then click **Open**.

   The license data is added to the database and is displayed in the Licenses perspective of the software license monitoring console.

6. For each license that you import, select the license in the Licenses perspective and click the **Edit** button. Select a **Primary product** to associate with the license (if needed, select a **Secondary product** as well).

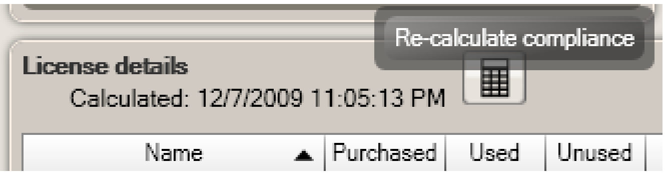
If the data does not appear in the console, or you receive an error message, any of the following items may have caused an error:

- All headings are required and must be spelled exactly including case and spacing
- If any spreadsheet columns are missing or you have extra columns, the data will not be imported
- The XML file must not be open (in Excel) when you import it

When you associate a license with a product, you can only select from products that are currently monitored. If you don't find the manufacturer or product name that you want, check in the Products perspective to make sure the product is being monitored.

Re-calculating license compliance

In the **License details** pane, a time stamp shows the last time that license compliance was calculated. This is done on a daily basis at the time inventory maintenance is run on your database. If you have added license data and want to re-calculate compliance without waiting for the scheduled maintenance, you can click the **Re-calculate compliance** button in the **License details** pane.



License details

Calculated: 12/7/2009 11:05:13 PM

If you have a large number of records, this calculation can take several minutes.

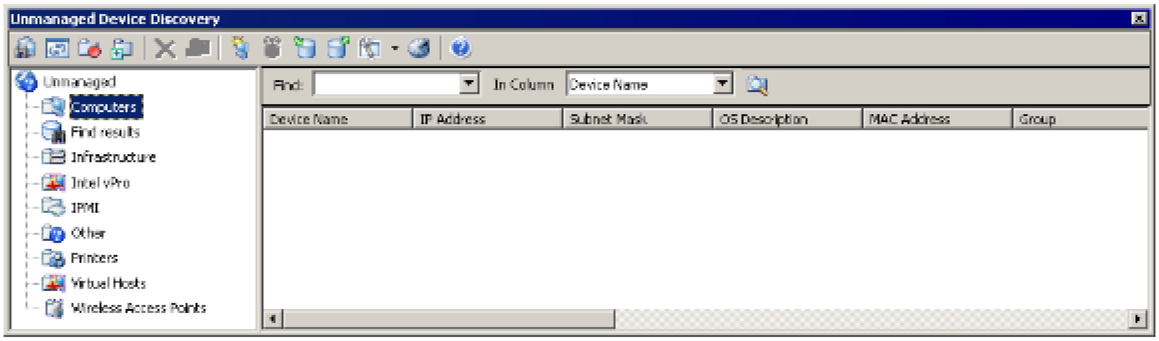
Unmanaged device discovery

The Unmanaged device discovery (UDD) tool provides a way for you to find devices on your network that haven't submitted an inventory scan to the LANDesk core database. Additionally, Extended device discovery (XDD) uses an agent installed on managed devices to find other devices sending network ARP broadcasts, as well as wireless access point (WAP) devices.

Read this chapter to learn about:

Unmanaged device discovery overview

Unmanaged device discovery (UDD) provides many ways to scan for and detect unmanaged devices on your network.



Here are the basic UDD scanning methods:

- **Network scan:** Looks for computers by doing an ICMP ping sweep. This is the most thorough search, but also the slowest. You can limit the search to certain IP and subnet ranges. By default this option uses NetBIOS to try and gather information about the device.
    - **IP OS fingerprinting:** Use nmap to try and discover more about a device, such as what operating system it is running.
    - **SNMP:** UDD uses SNMP to discover devices. Click **Configure** to enter information about SNMP on your network.
- **Standard LANDesk agent:** Looks for the standard LANDesk agent (CBA) on computers. This option discovers computers that have the LANDesk products installed.
- **NT domain:** Looks for devices in a domain you specify. Discovers members whether the computer is on or off.

- **LDAP:** Looks for devices in a directory you specify. Discovers members whether the computer is on or off.
- **IPMI:** Looks for servers enabled with the Intelligent Platform Management Interface, which allows you to access many features regardless of whether the server is turned on or not, or what state the OS may be in.
- **Intel* AMT:** Looks for Intel Active Management Technology-enabled devices. AMT devices appear in the **Intel vPro** folder.
- **Virtual hosts:** Looks for servers running VMware ESX Server. These servers appear in the **Virtual hosts** folder.

To automate unmanaged device discovery, you can schedule UDD discovery scans to occur periodically. For example, you could divide your network into thirds and schedule a ping sweep for one third each night.

If you schedule a discovery, the core server does the discovering. Unscheduled discoveries happen from the console that starts it.

Extended device discovery

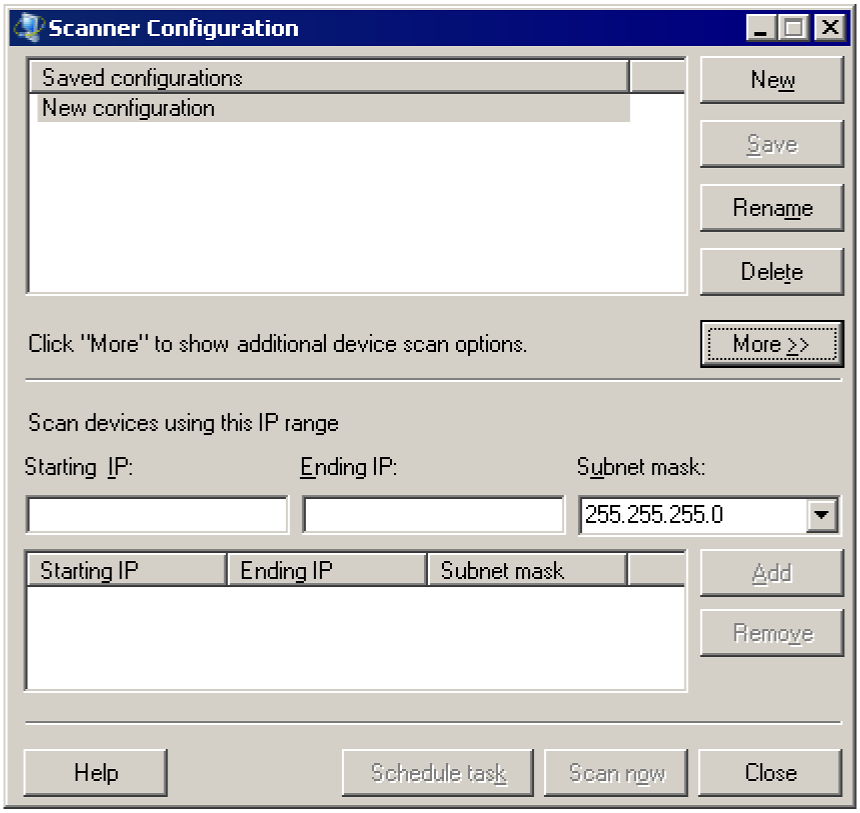
The UDD tool also supports extended device discovery (XDD) scanning. XDD relies on a device agent (deployed via an agent configuration) that listens for ARP broadcasts and WAP signals on your LANDesk network. The XDD agent on a configured device then checks to see if the broadcasting device has the standard LANDesk agent installed. If the standard LANDesk agent doesn't respond, an ARP discovered device displays in the **Computers** group with reported information in the item list view, and a WAP device displays in the **Wireless Access Points** group with reported information in the list view.

Extended device discovery is ideal in situations involving firewalls that prevent devices from responding to the normal ping-based UDD discovery methods.

Use extended device discovery to discover firewalled devices
Be aware that the normal unmanaged device discovery methods usually can't discover devices that use a firewall, such as the Windows firewall that is built into Windows XP. The firewall typically prevents the device from responding to the discovery methods that unmanaged device discovery uses. Extended device discovery helps solve this problem by using network ARP traffic to discover devices.

Discovering unmanaged devices with UDD

It's easy to discover unmanaged devices with the basic UDD scan methods.



To discover unmanaged devices with UDD

1. In the unmanaged device discovery window (**Tools > Configuration > Unmanaged device discovery**), click the **Scan network** button.
2. Click **More >>** and select the discovery option you want.
3. Enter a starting and ending IP range for the scan. You must enter a range for **Standard LANDesk agent discovery** (CBA) or **Network discovery** to work. The range is optional for **NT domain** and **LDAP**.
4. Enter a **Subnet mask**.
5. Click the **Add** button to add the scan you just configured to the task list.
6. In the task list at the bottom of the dialog, select the scans you want to run and click the **Scan now** button to scan immediately, or the **Schedule task** button to run the scans later or on a recurring schedule. The **Scan now** and **Schedule task** buttons only run scans you've added to the task list and that are selected.
7. Watch the Scan Status dialog for scan status updates. When the scan finishes, click **Close** in the Scan Status and Scanner Configuration dialogs.
8. Click **Computers** in the UDD tree to view the scan results.

Configuring Windows NT domain discovery

The Windows NT domain discovery option won't work unless you configure the scheduler service to log in to the domain with a domain administrator account.

To configure the Scheduler login account

1. Click **Configure > Services** and click the **Scheduler** tab.
2. Click **Change login**.

3. Enter a domain administrator username and password.
4. Click **OK**
5. Restart the scheduler service so the change takes effect. On the **Scheduler** tab, click **Stop**, and once the service has stopped click **Start**.

Using extended device discovery (ARP and WAP)

Extended device discovery (XDD) works outside the normal scan-based UDD discovery methods. The XDD agent can be configured and deployed to managed devices to use the ARP and/or WAP discovery methods. This section describes both discovery methods.

ARP discovery method

Managed devices configured with the XDD discovery agent for ARP discovery listen for ARP (Address Resolution Protocol) broadcasts and maintain a cache (both in memory and in a file on the local drive) of devices that make them. Networked devices use ARP to associate a TCP/IP address with a specific device network hardware MAC address. This communication happens at a very low level and doesn't rely on devices responding to pings or agent communication on specific network ports. Even heavily firewalled devices rely on ARP. Because of this, extended device discovery can help you find devices that normal discovery scans won't find.

When a new ARP broadcast is recognized by a device configured with the extended device discovery agent, the agents that heard the ARP broadcast wait two minutes for the detected device to boot and then each agent waits a random amount of time. The agent with the shortest random wait time pings the new device first, checking for LANDesk agents, and then the agent sends a UDP broadcast to the subnet to let the other agents know that it took care of the ping for that new discovered device. If you have multiple extended device discovery agents installed, this prevents devices from generating excess traffic by all pinging at the same time.

The ARP tables stored by the extended device discovery agent timeout after 48 hours by default. This means that every network device will be pinged once per time out period. Even devices that generate a lot of ARP traffic are only pinged once per timeout period.

Devices with LANDesk agents on them are assumed to be managed and aren't reported to the core server. Devices without LANDesk agents are reported to the core server as unmanaged devices. These devices appear in the **Unmanaged device discovery** window's **Computers** list. ARP-discovered devices show **True** in the **ARP Discovered** column. For ARP discovered unmanaged devices, XDD reports back the following information in the list view columns:

- IP Address
- MAC address
- First scanned
- Last scanned
- Times scanned

WAP discovery method

You can also configure managed devices to listen for wireless access point (WAP) devices on your network, and add any discovered WAP devices to the Wireless Access Points group in the Unmanaged device discovery tool.

For discovered WAP devices, XDD reports back the following information in the list view columns:

- Device name
- MAC address

- First scanned
- Last scanned
- Times scanned
- WAP status (Allowed, Rogue, Active exception)
- Signal strength (use to determine the approximate location of the WAP device)
- Encryption level (the encryption scheme used by the WAP device)
- Manufacturer

Reporting the MAC address
XDD uses the wireless detection API on devices running Windows Vista to obtain the device MAC address and display it in the list view. However, this capability is not supported on devices running Windows XP/SP2.

Configuring devices to use extended device discovery (ARP and WAP)

You can use the Agent configuration tool to configure some of your managed devices with the extended device discovery (XDD) agent so they can act as discovering devices that listen for ARP and WAP signals on the network.

You don't have to deploy extended device discovery to every managed device, though you can if you want to. Deploying the XDD agent to several devices on each subnet should give enough coverage.

To deploy the extended device discovery agent for ARP and/or WAP discovery

1. Click **Tools > Configuration > Agent configuration**.
2. Click the **New** toolbar button.
3. Enter a **Configuration name**.
4. In the **Agent configuration** dialog's **Extended device discovery** page, select one or both of the discovery methods you want to deploy.
5. Specify a setting for the discovery method(s) you've selected. You can select on existing setting from the drop-down list, or click Configure to edit a setting or create a new one for this agent configuration.
6. Finish specifying options on the agent configuration. For more information about any page, click **Help**.
7. Click **Save**.
8. Deploy the agent configuration to desired target devices on each subnet.

You can configure various extended device discovery settings for devices with the extended device discovery agent. This agent periodically synchronizes its settings with the core server.

To configure extended device discovery agent settings for ARP and/or WAP discovery

1. Click **Tools > Configuration > Unmanaged device discovery**.
2. Click the **Configure extended device discovery** toolbar button, and select which type of discovery method's settings you want to configure (ARP or WAP).
3. Specify the discovery method scan options as you like. For more information, click **Help**.
4. Click **OK** when done. The next time extended device discovery agents synchronize with the core server, your changes are applied.

Understanding IP address filtering with XDD

We don't recommend that you install extended device discovery on notebook computers, since they may connect to other networks that you don't want to monitor, such as hotel or airport networks. To help prevent discovery of devices that aren't on your network, the core server ignores IP addresses where the first and second IP address octets are plus or minus 10 from that of the core server. For example, if your core server's IP address is 192.168.20.17, extended device discovery on the core server will ignore addresses above 203.179.0.0 and addresses below 181.157.0.0.

You can disable this feature by adding the following DWORD registry key to the core server and setting its value to 0:

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\Filter

You can set the Filter value to 1 to enable filtering again.

You can adjust the first and second octet monitoring ranges by adding the following DWORD registry keys to the core server and setting their values to the numeric range that you want monitored (the default is 10 for the first and second octets):

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold1
- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold2

FilterThreshold1 contains the range for the first octet and FilterThreshold2 contains the range for the second octet.

Working with devices found through XDD

Unmanaged devices found through extended device discovery's ARP discovery method appear in the **Unmanaged device discovery** window's **Computers** list. WAP Devices found through extended device discovery's WAP discovery method appear in the **Unmanaged device discovery** window's **Wireless Access Points** list.

From these lists you can perform the normal UDD options, such as moving them to other groups. Right-click a device to access its shortcut menu and use the available options.

You can also import and export extended device discovery exceptions. An exception is a device on the network that isn't manageable or that the administrator knows about but doesn't want extended device discovery to report on.

These exceptions are in a text .CSV file format that consists of comma-separated IP and MAC addresses, in that order, one pair per line. The exceptions export includes all exceptions stored in the database. The exceptions import replaces all exceptions stored in the database with the exceptions you include in the import file.

To export all extended device discovery exceptions

1. Click **Tools > Configuration > Unmanaged device discovery**.
2. Click the **Export extended device discovery exceptions to CSV file** toolbar button.
3. Choose a folder and give the file a name.
4. Click **Save**.

To import all extended device discovery exceptions

1. Create or update a comma-separated CSV file that contains the exceptions you want.
2. Click **Tools > Configuration > Unmanaged device discovery**.
3. Click the **Import extended device discovery exceptions from CSV file** toolbar button.
4. Click **Open**.

Maintaining ARP discovered device records

UDD stores devices found through extended device discovery in the core server's database. If you have a lot of unmanaged devices on your network, this data can grow very quickly. By default, this data is kept for 24 hours. You can customize how long devices found through extended device discovery stay in the database. After the number of days you specify, devices that haven't been rediscovered within that period will be deleted.

To configure the ARP discovery history

1. Click **Tools > Configuration > Unmanaged device discovery**.
2. Click the **Configure ARP discovery history** toolbar button.
3. Change the options you want. Click **Help** for more information.
4. Click **OK** when done.

Extended device discovery reports

There are several XDD reports in the **Reports** window (**Tools > Reporting / Monitoring**, click **Reporting > Management Suite |Unmanaged Devices**) that you can view.

Extended device discovery reports include:

- **ARP discovered device history:** History of unauthorized devices.
- **Current ARP discovered devices without the agent:** Current devices where the LANDesk agent is either disabled or not working.
- **History of ARP discovered devices without the agent:** History of devices where the LANDesk agent is either disabled or not working.
- **Unmanaged devices:** Devices on the network that aren't assigned to a core server.
- **Wireless devices:** History of all wireless devices that have been discovered.

What happens when a device is discovered

When UDD or XDD finds an unmanaged device for the first time, it tries to identify the device type so it can add the device to one of the following groups:

- **Computers:** Contains devices discovered by UDD scanning methods (and the XDD agent's ARP discovery method)
- **Infrastructure:** Contains routers and other network hardware.
- **Intel vPro:** Contains Intel vPro-enabled devices.
- **IPMI:** Contains servers that have the Intelligent Platform Management Interface.
- **Other:** Contains unidentified devices.
- **Printers:** Contains printers.
- **Virtual hosts:** Contains virtual hosts.
- **Wireless Access Points:** Lists discovered WAP devices (found by the XDD agent).

These groups help keep the UDD list organized so you can more easily find the devices you're interested in. You can sort the device lists by any column heading when you click on a heading.

Moving devices to different groups
UDD may not categorize devices correctly and place them in the appropriate device groups in every instance. If this happens, you can easily drag misidentified devices to the correct group.

UDD tries to discover and report basic information about each device, including the following data that appears in the item list view in the right-hand pane of the tool window:

- **Device name:** The discovered device name, if available.

- **IP address:** The discovered IP Address. UDD always shows this. XDD does not.
- **Subnet mask:** The discovered subnet mask. UDD always shows this.
- **OS description:** The discovered OS description, if available.
- **MAC address:** The discovered MAC address, usually returned if the device has the standard LANDesk agent, NetBIOS, or if the device is on the same subnet as the core server or console that's doing the discovery.
- **Group:** The UDD group the device belongs to.
- **Standard LANDesk agent:** Shows whether the device has CBA on it. You can deploy other LANDesk agents directly to managed devices with CBA loaded.
- **All users:** Users logged in at the device being scanned, if available.
- **Group/Domain:** The group/domain the device is a member of, if available.
- **First scanned:** The date UDD first scanned this device.
- **Last scanned:** The date UDD last scanned this device. This column helps you find unmanaged devices that may not be on the network any more or that were recently found.
- **Times scanned:** The number of times UDD scanned this device.
- **Intel vPro:** Whether the device supports Intel vPro.
- **ARP discovered:** Whether the device was discovered via ARP.
- **XDD exception:** Whether the device is an XDD exception.
- **IPMI GUID:** The IPMI GUID of the device, if available.

Depending on the device, UDD may not have information for all columns. When UDD finds a device for the first time, it looks in the core database to see if that device's IP address and name are already in the database. If there's a match, UDD ignores the device. If there isn't a match, UDD adds the device to the unmanaged device table. Devices in the unmanaged table don't use a LANDesk license. A device is considered managed once it sends an inventory scan to the core database. You can't drag devices from UDD into the main console network view. Once unmanaged devices submit an inventory scan, they'll be removed from UDD and added to the network view automatically.

You can create custom groups to further categorize unmanaged devices. If you move a device to another group, UDD will leave that device in that group if UDD detects the device again later. By keeping the main **Computers** group organized and by moving devices you know you won't be managing with LANDesk into subgroups or other categories, you can easily see new devices in the **Computers** group. If you delete a group that contains devices, UDD moves the devices to the **Other** group.

You can quickly find devices matching search criteria you specify by using the **Find** toolbar field. You can search for information in a particular column, or in all columns. Search results appear in the **Find results** category. For example, use Find to group unmanaged computers that have CBA by searching for "Y" in the Standard LANDesk agent field.

You can also create an alert when UDD finds unmanaged devices. In Alerting (**Tools > Configuration > Alerting**, click **Core alert ruleset**) the alert name to configure is **Unmanaged Device discovery - unmanaged device found**.

Troubleshooting inaccurate OS version results

In some environments, an nmap mapping on an IP address that isn't in use will return a response on specific ports, confusing nmap. The ports that do or don't respond vary in different environments. If nmap isn't returning accurate OS version results, or as a best practice, nmap should be tuned to the customer environment.

To tune nmap

1. Determine several IP addresses that aren't in use in the environment.

2. At a command prompt on the core server, use the following command line to manually scan the IP addresses:

   ```
   nmap -O -sSU -F -T4 -d -v <targets> -oX test.xml > test.txt
   ```

3. Review the results and see if there are any ports that consistently respond on IP addresses that aren't in use.
4. Open Management Suite's nmap-services document (C:\Program Files\LANDesk\Management Suite\nmap\nmap-services) and comment out the ports with a # character that consistently respond.

Deploying LANDesk agents to unmanaged devices

After you've discovered unmanaged devices using the scan and discovery methods described above, you can deploy LANDesk agents to those devices using one of the following methods:

- Push-based deployments using scheduled tasks and a domain administrative account you've configured for the scheduler.
- Push-based deployments using the standard LANDesk agent. If the devices have the standard LANDesk agent, you can do a push-based deployment.
- Pull-based deployment using a login script.

For more information on deploying devices, see the LANDesk User Community at http://community.landesk.com.

When organizing devices for agent deployment, you may find it easier to sort the unmanaged device list by the standard LANDesk agent to group for standard LANDesk agent device deployments and to sort by domain for scheduled task deployments.

When deploying to Windows devices
The Windows default setting forces network logins that use a local account to log in using the guest account instead. If you aren't using a domain-level administrative account and are using a local account for the scheduler service, scheduled tasks will fail because the scheduler service won't be able to authenticate.

To deploy LANDesk agents to unmanaged devices

1. Click **Tools > Configuration > Agent configuration** and create a new configuration or use an existing one. From that configuration's shortcut menu, click **Schedule**.
2. Click **Tools > Configuration > Unmanaged device discovery**, and select the devices you want to deploy to. Drag the devices onto the **Scheduled tasks** window. If the **Scheduled tasks** window is a minimized tab, you can drag devices onto the **Scheduled tasks** tab, which opens the **Scheduled tasks** window.
3. If the devices don't have the standard LANDesk agent, click **Configure > Services**, and click the **Scheduler** tab. Make sure the scheduler account is one that will have administrative privileges on the devices you're deploying to.
4. Double-click the deployment script and set a start time. Click **OK** when you're done.
5. Watch the **Scheduled tasks** window for updates.

Restoring client records

Should you ever reset your core database and need to restore device data, you can use UDD to discover all devices on the network. You can then use the discovery results as the target for the "Restore client records" scheduled task.

If the devices have the standard LANDesk agent on them, this task has the devices send a full inventory scan to the core database that each device is locally configured for. The result of this task is those devices that have already been configured will be rescanned backed into the database and the devices will still be pointing to their correct managing core server. The task will fail on devices that haven't been managed by a core server.

To restore client records

1. Use UDD to discover unmanaged devices, as described earlier.
2. Click **Tools > Distribution > Scheduled tasks**.
3. In the **Scheduled tasks** window, click the **Schedule custom script** button.
4. Click **Restore client records**, and from its shortcut menu click **Schedule**.
5. From the UDD **Find results** tree, drag the computers you want restored onto the **Restore client records** task in the **Scheduled tasks** window.
6. From the **Restore client records** task's shortcut menu, click **Properties** and configure the task.
7. Watch the **Scheduled tasks** window for updates.

OS deployment

The LANDesk OS deployment tool groups together several features that let you deploy images remotely to new or existing devices. These features streamline new device provisioning and redeploying existing devices, with options to migrate user profiles and to image with hardware-independent templates that can be applied to different device models. With these automated features you can deploy and re-image devices without user input or the need for a technician to work at each device.

You can schedule deployments and migrations to occur after hours, and by using the LANDesk targeted multicast technology to distribute images, you won't saturate network bandwidth by deploying the same image to multiple devices.

The following features are part of the OS deployment tool:

- **OS deployment:** Create images and scripts to deploy images with DOS, Windows, and Linux preboot environments. Use agent-based or PXE-based deployment to distribute images. To begin, see "OS deployment overview" on page 202.
- **Hardware-independent imaging:** Create an imaging template that is hardware-agnostic, so you can apply one template to devices from multiple manufacturers. Create a library of drivers and associate them with specific device models; the drivers that apply to each device are injected during the imaging process. For more information, see "Hardware-independent imaging" on page 216.
- **Provisioning:** Create templates that apply a full range of device attributes and features to the imaging process. In addition to deploying OS images, you can define actions that occur before and after the OS is installed, such as installing software, patching the system, and configuring drive and network settings. You can provision new devices and have them ready for use in your environment with no downtime. For more information, see "Provisioning" on page 221.
- **Profile migration:** Capture and restore user profile data when you update a user's computer or assign them a new one. You can preserve the user's desktop, application settings, printer and network settings, and file and folder structure on the new device. For more information, see "Profile migration" on page 257.

This chapter begins with the basics of deploying OS images:

- "Troubleshooting" on page 216
- "Hardware-independent imaging" on page 216

OS deployment overview

The OS deployment (OSD) feature provides two methods of deploying OS images to devices on your network:

- **Agent-based deployment:** Uses the device's existing Windows OS and installed LANDesk agents to deploy images. For more information, see "Agent-based deployment" on page 206.
- **PXE-based deployment:** Allows you to image devices with empty hard drives or unusable OSes. Lightweight PXE representatives eliminate the need for a dedicated PXE server on each subnet. For more information, see "PXE-based deployment" on page 211.

If you use Microsoft's Sysprep utility to create your images, OS deployment creates customized SYSPREP.INF files and injects them into each device's image on a per device basis, customizing Windows computer names, domain information, and so on from the core database.

OS deployment includes a built-in imaging tool you can use to create images. OS deployment also supports third-party imaging tools that you may already be using, such as Symantec Ghost, PowerQuest DeployCenter, and Microsoft XImage.

OS deployment can image, deploy, and migrate from these boot environments:

- DOS
- Windows PE*
- Linux

* The LANDesk PE Toolkit contains Microsoft Windows Pre-installation Environment software (“WinPE”), a third party product. In order to use the LANDesk PE Toolkit, you must have a valid license to use WinPE. If you purchased a license to use WinPE from LANDesk, your use of WinPE is subject to the applicable terms and conditions of LANDesk’s End User License Agreement for the licensing of LANDesk software.

Since some of these environments require licensed software, you'll need to provide copies of the licensed software for OS deployment to validate before you can use a particular environment.

OS deployment (imaging) should be used with caution. Operating system deployment includes wiping all existing data from a device's hard drive and installing a new operating system. There is a substantial risk of losing critical data if the OS deployment is not performed exactly as described in this document, or if poorly implemented images are used. Before performing any OS deployment, we recommend that you back up all data in such a manner that any lost data may be restored.

OS deployment steps for Windows devices

When planning and implementing a Windows OS deployment operation, follow this sequence of steps:

1. If you plan to use a DOS or Windows PE imaging environment and you haven't validated your licenses already, validate them by clicking the **Validate licenses** toolbar button in the **Operating system deployment** window. Insert the operating system CDs as prompted. You only need to do this once. The Linux boot environment doesn't require license validation.
2. (Optional) Run the Microsoft Setup Manager and Sysprep utilities on the device whose image you want to capture.

3. Create or reuse an image capture script in the **Operating system deployment** window.
4. Schedule a task with the **Scheduled tasks** tool that runs the capture image script on the device whose image you want to capture. (Watch the **Custom Job Status** window updates for success or failure).
5. Create or reuse an existing image deployment script in the **Operating system deployment** window.
6. Schedule a task with the **Scheduled tasks** tool that runs the deploy image script on target devices where you want the image deployed.
7. Targeted devices running Windows OSes and LANDesk agents will begin the image deployment job when scheduled (agent-based deployment).
8. Targeted devices that are PXE-enabled will begin the image deployment job the next time they boot (PXE-based deployment).

Read the relevant sections below for detailed information about each of these steps.

OS deployment steps for Linux devices

The following is a list of constraints imposed on Linux installations.

1. The root ('/') partition must be of filesystem type ext2, ext3, or xfs.
2. The root partition *cannot* be contained in an LVM PV (Logical Volume Manager - Physical Volume), but *must* be a partition (physical, or extended) in the drive's MBR (Master Boot Record).
3. The last partition is the only partition that can be expanded; therefore it, too, must be of filesystem type ext2, ext3, or xfs.
4. You must specify which partition the root partition is on (hda3 or sda2)

Linux PE only supports IDE devices. Serial ATA and SCSI are not supported. If you want to image these devices you must use a third-party imaging tool

When planning and implementing a Linux OS deployment operation, follow this sequence of steps:

1. Create or reuse a Linux configuration image capture script in the **Operating system deployment** window.
2. Schedule a task with the **Scheduled tasks** tool that runs the capture image script on the device whose image you want to capture. (Watch the **Custom Job Status** window updates for success or failure).
3. Create or reuse a Linux configuration image deployment script with the **OS Deployment/Migration Tasks** wizard.
4. Schedule a task with the **Scheduled tasks** tool that runs the deploy image script on target devices where you want the image deployed.
5. Targeted devices running Windows OSes and LANDesk agents will begin the image deployment job when scheduled (agent-based deployment).
6. Targeted devices that are PXE-enabled will begin the image deployment job the next time they boot (PXE-based deployment).

OS image guidelines

You can create OS images with the LANDesk imaging tool or other imaging tools. When you run the OS Deployment/Migration Tasks wizard to create an imaging script, you are prompted to specify the image type and imaging tool. The wizard automatically generates command lines for the LANDesk imaging tool, Symantec Ghost 7.5, and PowerQuest DeployCenter 5.01.1.

When you install the OS deployment and profile migration component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: imageall.exe, image.exe, restall.bat, and backall.bat. If you want to use Microsoft XImage, you must copy the files ximage.exe and xmlrw.dll into the \\<core>\ManagementSuite\OSD\imaging folder.

If you have a different imaging tool, you can supply the command line for it at the end of the wizard. If you specify a custom command line, the wizard will put your custom line in the right location in the script so that you don't have to edit the script manually.

Understanding the OS deployment imaging environments

When capturing or restoring an image, OS deployment boots the target device into an imaging environment. OS deployment supports these imaging environments:

- **DOS**: License verification requires a Windows NT 4 server CD and a Windows 98 CD. This 7 MB image is the smallest one, reducing the network bandwidth used. It potentially is the slowest at creating and restoring images, and has lower hardware compatibility than the other imaging solutions.
- **Windows PE**: License verification requires a Windows PE 2005 CD and a Windows 2003 SP1 CD. This 120 MB image is the largest one. It has the best hardware compatibility and is potentially the fastest at creating and restoring images. The imaging speed benefits from 32-bit drivers and applications. This imaging environment also supports Microsoft's imaging tools. For more information on how the Windows PE environment works, see "Understanding the Windows PE preboot environment" on page 580.
- **Linux**: No license verification required. This 37 MB image typically has mid-range compatibility and speed. Since it doesn't require any license verification, it also may be one of the most convenient imaging environments.

Note that the imaging environment you choose is independent of the OS you are imaging. For example, you can use the Linux imaging environment to image Windows operating systems.

Validate the DOS and Windows PE boot environments by clicking the **Validate licenses** toolbar button in the **Operating system deployment** window. Insert the operating system CDs as prompted. You only need to do this once. The Linux boot environment doesn't require license validation. The validation dialog also lets you change the default preboot environment for devices in the PXE holding queue. Devices in the holding queue will boot into the environment you select. Your choices are limited to boot environments you have validated.

Image filenames

You should give your images unique filenames. Deploying different images with the same filename simultaneously on the same subnet can cause problems. Depending on how an imaging utility names image files and the imaging environment you're using, (DOS with multi-file Ghost images, for example), you may have only five unique characters in your filename once it is converted to a DOS 8.3 name format.

When capturing images, the LANDesk imaging tool for DOS, Windows, and Linux uses the last six characters of the computer name, followed by a two-digit image number for each file in the image. If you're capturing images from multiple devices at the same time and the last six characters of the computer name aren't unique, you'll experience errors during the capture process.

Symantec Ghost and PowerQuest DeployCenter generally use the first eight characters of the computer name for the image filename, which must also be unique for simultaneous image capture to work correctly.

When capturing images from multiple devices, you have two ways of ensuring that your images have unique names:

- Image one device at a time, renaming each image as it's created.
- Before running the job, ensure that the last six characters (LANDesk imaging tool) or first eight characters (Ghost and DeployCenter) of your Windows computer names are unique.

LANDesk agents and images

You should not include the LANDesk agents in your images. If you use a Sysprep image, OS deployment will install the LANDesk agents on the Windows-based OS after the image is restored.

If your Windows-based non-Sysprep images include LANDesk agents, you will need to delete the ldiscan.cfg file from the root of the hard drive before imaging. You will also need to delete these keys:

- HKLM\Software\Intel\LANDesk\Common API\Unique ID
- HKLM\Software\LANDesk\Common API\Unique ID

If you leave these in the image, all devices using the image will have the same core database entry. Alternatively, if you have non-Sysprep images that already have LANDesk agents on them, you can enable the **Reject duplicate identities** option on the **Duplicate device ID** dialog (**Configure > Services > Inventory > Device IDs**).

Partitions and images

By default, when OS deployment restores an image on a target device, it deletes any existing partitions on that device.

The LANDesk imaging tool supports single-partition and multiple partition images (up to four partitions). In the Linux PE environment, when using the LANDesk imaging tool, you can only capture and deploy one partition at a time.

Non-Windows images

You can use OS deployment to deploy almost any image your imaging tool supports, not just Windows-based images. When deploying non-Windows or non-Sysprep images, make sure you do not select the **Image is Sysprepped** option in the new configuration dialogs.

Customizing images with Setup Manager and Sysprep

You can use Microsoft's Setup Manager and Sysprep utilities when deploying Windows 2000/2003, Windows XP, and Windows XP x64 Edition images. Sysprep customizes a Windows installation so that when the OS reboots, it looks for an answer file (sysprep.inf) and reconfigures itself for the new device. Setup Manager creates the sysprep.inf answer file that Sysprep uses.

Before creating OS deployment scripts, you should run Microsoft's Setup Manager (setupmgr.exe) and create a sysprep.inf answer file for the images you're deploying. You can then use this file as the basis for any OS deployment scripts you create by selecting the **Use existing sysprep.inf file as a template** option on the **Specify Sysprep file information** page of the wizard. Any OS deployment script settings you make in the wizard override the equivalent options in the template sysprep.inf file.

Using Sysprep on your Windows 2000/XP images allows OS deployment to query the core database for each device you're deploying and to migrate certain user settings, such as:

- Windows computer name
- GUID (the unique identifier used to identify devices in the core database)

You can also set these options globally for images you deploy:

- Time zone
- Volume license key
- Registered name and organization
- Workgroup/Domain/LDAP Organizational Unit (OU)

OS deployment uses information from the core database and from the image deployment script to create a custom sysprep.inf for each device you're imaging. OS deployment then injects that sysprep.inf into each device's image.

Creating a Sysprep image

To create an image that uses Sysprep

1. On the device whose image you want to capture, make configuration or customization changes to prepare it for imaging.
2. At the root of the device's hard drive, make a c:\sysprep folder.
3. From a Windows 2000 or Windows XP installation CD, open \Support\Tools\DEPLOY.CAB and copy **sysprep.exe** and **setupcl.exe** to the sysprep folder you created.
4. Open a DOS command prompt and change to the sysprep folder. Run Sysprep. If you don't use the reboot option, you'll need to shut down the device from the Start menu once a message appears requesting that you shut down.
5. Boot to DOS and run your imaging tool manually.

For more information on Setup Manager and Sysprep

Refer to Microsoft's Web site for official documentation about the Setup Manager and Sysprep utilities. Sysprep has many powerful features you can use that are beyond the scope of this document.

You may also find help for issues with using Sysprep on the LANDesk Support Community Web site; go to community.landesk.com.

Agent-based deployment

You can use the agent-based deployment method to deploy OS images to devices running Windows 98, Windows 2000, or Windows XP.

For information on the other method of image deployment, see "PXE-based deployment" on page 211.

Prerequisites

If you're not using PXE to deploy images, devices must meet the following criteria:

- Be in the core database if you have multiprocessor images.
- Have the standard LANDesk agent, Enhanced Software Distribution agent, and Inventory agent loaded. OS deployment uses the Enhanced Software Distribution agent to distribute images. If you'll be multicasting images, you also need to have the Targeted Multicasting agent loaded.

What happens during an agent-based deployment

1. The core server connects to the device and runs any preconfiguration commands you specified in the image deployment script.

2. OS deployment uses the software distribution agent to distribute a virtual boot partition file to the device and modifies the boot sector to boot from this file, then reboots the device.
3. The device boots to DOS or Windows PE (depending on your choice), detects and loads a network driver, then retrieves and installs the image file from the image server.

   For non-Sysprep images, the device reboots after the imaging completes. OS deployment considers the job complete after this reboot.

   For Sysprep images, agent-based deployment continues in this manner:

4. Before rebooting and loading the image, the DOS or Windows PE agent replaces sysprep.inf with a customized file for that device.
5. The imaged device boots and customizes itself based on what is in the sysprep.inf file.
6. For Windows images, any post-image commands you specified in the image deployment script are run from the RunOnce registry key.
7. For Windows images, OS deployment runs wscfg32.exe using your default device agent configuration to reinstall the LANDesk agents.

Creating imaging scripts

LANDesk OS deployment provides OS deployment and profile migration tools that let you create and manage both imaging (image capture and image deploy) scripts and profile migration scripts.

With the OS deployment tool you can create scripts that perform the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device. Images can be captured using the built-in LANDesk imaging tool, or a third-party tool such as Ghost, PowerQuest, or another tool of your choice.
- **Capture profile:** Creates a script that captures and stores a device's unique user settings, application and desktop settings, and files. You can also use this option to access the Collection Manager dialog to create a user-initiated profile migration package that can be run locally at individual devices.
- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.
- **Restore profile:** Creates a script that restores previously captured profile data (user settings, application and desktop settings, and files to target devices.
- **Generic DOS tasks:** Creates a script that runs DOS commands (including application launches on devices).

Once you have created a script, you can schedule it to run on devices by using the **Scheduled tasks** tool.

If you are deploying an image to PXE-enabled devices, you can add image deployment scripts to the PXE DOS boot menu. This menu is DOS-based and appears on the device during a PXE boot. For more information, see "Using the PXE boot menu" on page 214.

To run the OS Deployment/Migration Tasks wizard

1. Click **Tools > Distribution > OS deployment.**
2. In the **Operating system deployment** window, right-click **All OSD Scripts** and click the script type you want to create. (You can also click the toolbar button for the script type you want to create.)

A wizard opens to guide you through the script creation.

3. Configure the script as necessary. Once complete, the script appears in the **All OSD Scripts** group in the **Operating system deployment** window.

Administrators (users with the LANDesk Administrator right) can copy scripts to user subgroups in the **User scripts** group.

Additional notes on scripts

- Script names must follow Windows file naming conventions. The wizard uses the script name you enter as the filename. If you use characters that aren't allowed in Windows filenames, you'll get an error about using invalid characters.
- All scripts are stored on the core server, in the \\<core>\LDMain\Scripts directory. If you have multiple consoles, the scripts will appear in the Manage Scripts window of each console.
- The wizard restores the settings on each page from the last script you created. If you change the script type from an imaging task to a profile migration task or a DOS task, the wizard clears the remembered settings.
- Because of changes to how administrator user account permissions are handled in Windows Vista and especially in Windows 7, you may find that master images you create that include these versions of Windows may not successfully deploy. We recommend that you visit the LANDesk Support Community website, community.landesk.com, for best-known method documents that describe master image scenarios and recommended procedures for creating and deploying images.

About Generic DOS tasks scripts

- DOS scripts reboot the selected target devices and run the commands you've specified. These remote commands are sent one line at a time.
- DOS scripts run from the virtual boot partition and go through the same network detection process as normal OS distributions do.
- The "Abort this job if any command fails" option stops execution if one of the commands returns a non-zero DOS error level code. You can view DOS task status in the Custom Job window or with a report.
- For more information about script commands, see "Using Custom Scripts," a technical document found in the LANDesk Support Community Web site (go to http://community.landesk.com and search for "using custom scripts").

Modifying scripts

You can modify your scripts at any time, either by reopening the configuration dialog and making changes, or by modifying the script directly in its .INI file and modifying any existing Sysprep settings in its associated .INF file.

With DOS scripts, the only changes you should make are between the REMPINGx=DOS and REMEXECx=reboot.com lines. The other lines in the script manage the virtual boot partition files and boot process.

To modify a script via the dialogs

1. Click **Tools > Distribution > OS Deployment**.
2. Right-click the script and click **Edit** in the shortcut menu (or double-click the script).
3. Advance through the wizard, making your changes.

To modify a script via an .INI file

1. Click **Tools > Distribution > OS Deployment**.
2. Right-click the script and click **Advanced edit**. The script's .INI file opens in Notepad. If this script has Sysprep settings associated with it, the SYSPREP.INF file also opens in Notepad.
3. Make your changes
4. Save the file(s).

Where .INI and .INF files are saved
.INI files are saved to the \\<core>\LDMain\Scripts directory. .INF files are saved to the \\<core>\LDMain\LANDesk\Files directory.

Multicasting OS images

This section discusses deploying images using the LANDesk targeted multicast technology. Multicasting is slower than a single distribution. Multicasting throttles bandwidth and stages the image on the target device's hard drive. However, multicasting to four or more devices will usually save enough bandwidth to make this worth it.

Targeted Multicasting supports only single-partition images, not multiple-partition images. Also, when using Targeted Multicasting with OS deployment, images can span up to 10 files.

When multicasting images, the image file is cached on the device before being restored. Your hard drive must have enough space for the image file and the restored files.

Before using multicasting with OS deployment, make sure the multicasting components are in place on the subnet to which you are distributing/deploying image files. Multicast OS deployments may fail if you don't specify domain representatives for each multicast domain in the network view's **Multicast Domain Representatives** group. Multicasting requires LANDesk Management Suite 6.62 or higher agents on devices, and a LANDesk Management Suite 6.62 or higher multicast domain representative on the subnet.

If you try to multicast to a subnet that does not have a Multicast Domain Representative, the deployment will start but it will not be able to finish, and you will have to create an OSD boot floppy. For more information, see "Creating an imaging boot disk" on page 569. If your routers forward UDP-directed broadcasts, and there will be Windows devices that can act as multicast domain representatives on the subnet you're deploying the image to, you should be able to use Targeted Multicasting without designating multicast domain representatives. If your routers don't forward UDP-directed broadcasts, you must manually select your multicast domain representatives for each subnet, making sure the representatives you choose aren't among the devices you're deploying images to.

You can manually specify which devices will be multicast domain representatives by adding devices to the **Configuration > Multicast domain representatives** group in the network view.

Make sure you don't image any multicast domain representatives in a subnet, because the imaging will fail and leave the devices in an unusable state.

You can throttle multicasts by changing the **Minimum number of milliseconds between packet transmissions** option in the **Configure advanced multicast options** page of the OS Deployment/Migration Tasks wizard.

If your Multicasting environment isn't configured correctly and the Targeted Multicasting fails, all target devices may be unbootable unless you follow the directions above.

Setting the Maximum Packet Size for a Targeted Multicast with OSD

If multicast fails with distribution jobs, it may be because the maximum transmission unit (MTU size on your network is fragmenting packets. Follow the steps below to adjust the MTU that multicast uses.

To set the Maximum Packet Size to 512 bytes for a Targeted Multicast script

1. Click **Tools > Distribution > OS Deployment**.
2. From the script's shortcut menu, click **Edit**.
3. In the Multicast section of the script, add the following line at the end of the section.

   MAX_PACKET_SIZE=512

   This string will set the Maximum Packet Size for the Targeted Multicast to 512 bytes. Maximum Packet Size can be set to between 256 and 1464 bytes. A setting above this range, or no setting at all, will force the default setting of 1464. A setting below this range will default to 256 bytes.
4. Save and close the script.

The MAX_PACKET_SIZE setting must be at least 28 bytes smaller than the Maximum Transmission Unit (MTU for the network the package is being distributed on. This is determined by adding the size of the IP header (20 bytes) and the UDP header (8 bytes) that are sent with each packet of data. Setting the Maximum Packet Size higher than this limit will cause your distribution to fail.

Viewing image status reports

The device being imaged sends status updates to the core server. You can track status in the Custom Job window or with a report. As OS deployment sends imaging commands to devices, the commands appear in the Custom Job window. Devices being imaged send status updates for each script command that is sent. If image deployment fails for some reason, you can see the command that failed.

Common reasons why imaging fails include:

- Partition corruption
- Problems the imaging tool can't handle
- Network adapter auto-detection can't find a network adapter
- Undetectable network adapter you specified doesn't work. If the network adapter driver you specify fails to load, that device will be stuck at the DOS prompt. You'll have to manually reboot it.

OS deployment creates a status report for each job, showing if it failed or succeeded on targeted devices.

To view a status report

1. Click **Tools > Reporting / Monitoring > Reports**.
2. Select the **OS deployment success rate** report.
3. From the list of log files, select the file for the job you're interested in viewing.
4. Click **Run**.

At the top of each report will be any jobs that failed on individual devices. Reports also show the details of each job, such as:

- **Machine Name:** For devices already scanned into the core database, this name will be the device name assigned to the device. For PXE-booted devices that haven't been inventory scanned, the machine name will be a MAC address. You can use a .CSV file to import MAC addresses into the core database. For more information, see "Using CSVIMPORT.EXE to import inventory data" on page 570.

- **Duration:** The amount of time each command took to complete.
- **Commands:** Each command that ran as part of the script. If a job failed, this column shows which command caused the failure.

PXE-based deployment

OS deployment supports PXE booting and image deployment. PXE-based deployment provides another method (in addition to agent-based deployment) of automated remote imaging of devices on your network. With PXE support, you can boot both new and existing PXE-enabled devices and either execute an OS deployment script at the device from a custom PXE DOS boot menu, or scan devices into your core database and then schedule an image deployment job with the **Scheduled tasks** tool.

PXE-based deployment is a quick and easy way to image devices in a variety of situations. For example:

- Initial provisioning of new devices
- Imaging devices in a test or training lab
- Re-imaging corrupted devices

LANDesk offers several options for using PXE to deploy OS images. For more information, see "Understanding the PXE boot options" on page 213.

PXE protocol basics

PXE (Preboot Execution Environment) is an industry-standard networking protocol that enables devices to be booted and imaged from the network, by downloading and installing an executable image file from an image server, before the device boots from the local hard drive. On a PXE-enabled device, the PXE protocol is loaded from either the network adapter's flash memory or ROM, or from the system BIOS.

PXE uses the following communication standards: DHCP (Dynamic Host Configuration Protocol), TFTP (Trivial File Transfer Protocol), and MTFTP (Multicast Trivial File Transfer Protocol).

When a PXE-enabled device boots up, it sends out a DHCP discovery request. If a DHCP server implementing PXE is found, the server assigns an IP address to the device and sends information about available PXE boot servers. After completing the DHCP discovery process, the device contacts the PXE server and downloads an image file through TFTP. The imaging script is then executed, loading the OS image from the imaging server onto the device. The image file is referenced by an OS deployment script.

If you want to learn more about PXE and its underlying technologies and functionality, read the PXE Specification v2.1 located at http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf.

Using PXE representatives

PXE support software is installed on your core server as part of the normal OSD installation. However, to enable PXE support, you must first deploy a PXE representative on each subnet of your network where you want PXE support available. PXE representatives provide scalability on your network by deploying OS images to devices in their respective subnets.

Devices on each subnet use normal PXE query and file transfer methods to communicate with their resident PXE representative, which communicates with the core server using Web services (HTTP).

Disable other PXE servers
If there is *any* other PXE server currently running on your network, you must first disable it in order to use LANDesk PXE support.

Deploying PXE representatives

You need to deploy one PXE representative on each subnet where you want to provide PXE boot support. You set up a PXE representative by running the PXE Representative Deployment script on the selected device. This predefined script is available in the **Manage scripts** tool (click **Tools > Distribution > Manage scripts**, then click the **Public scripts** folder).

You can have multiple PXE representatives on a subnet to help with load-balancing. When this is the case, the first PXE representative to respond to a device's request is the one that will be used to communicate with the core server.

We recommend that you do *not* deploy a PXE representative on your core server.

There are no special hardware requirements for the device you select to be a PXE representative, but it must meet the following software requirements:

- **Operating system:** Windows NT 4, Windows 2000, or Windows XP.

  For Windows NT and 2000, ensure that the Microsoft MSI service is running (XP includes MSI by default). If you have installed the latest service pack for either OS, MSI service should be running. Otherwise, you can deploy it to the target PXE representative from the console by following these steps: Click **Tools > Distribution > Manage scripts**, select the **MSI service deployment** task under **All scripts**, and click the **Schedule** button. In the **Scheduled tasks** windows, drag the target devices into the window, right-click the **MSI service deployment** task and select **Properties**, click **Schedule task** and specify a start time to schedule the MSI service deployment.

- **Installed LANDesk agents:** Enhanced Software Distribution agent and Inventory Scanner agent. For more information, see "Configuring device agents" on page 75.

To deploy a PXE representative

1. In the console, click **Tools > Distribution > OS Deployment**.
2. In the **Operating system deployment** window, click the **All other scripts** tree item. Click the **PXE representative deployment** script, and then click the **Schedule** toolbar button.
3. In the console's network view, select the target device on which you want to install PXE services.
4. Drag and drop the selected device to the **PXE Representative deployment** task in the **Scheduled tasks** window.
5. Right-click the **PXE Representative deployment** task, click **Properties**, and finish configuring the task.

Updating PXE representatives
If you modify the PXE boot option settings (on the **Configure > Services > OS deployment** tab), you need to update all of your PXE representatives by re-running the PXE Representative Deployment script to propagate those changes to PXE representatives on each subnet. However, re-running the script is not necessary if you simply move PXE proxies from the Available proxies list to the Holding queue proxies list. For more information about the PXE holding queue, see Using the PXE holding queue later in this chapter.

To update or remove a PXE representative

1. Click **Tools > Distribution > Manage scripts**.
2. To update a PXE proxy, select **Public scripts > PXE Representative Deployment**. Right-click the script and select **Schedule**. (Or, to remove a PXE proxy, select the **PXE Representative Removal** script instead.)

3. Drag and drop the target devices to the appropriate task in the **Scheduled tasks** window.
4. Right-click the task, click **Properties**, and finish configuring the task.

Booting devices with PXE

When a PXE-enabled device boots, the following occurs:

1. The PXE-enabled device sends out a query for PXE services running on a PXE representative on the network.
2. If a PXE representative exists on the subnet, it responds and tells the device to continue to boot using PXE.
3. A PXE boot session is initiated on the device and the PXE boot prompt displays. The default prompt message displays for four seconds and says "Press F8 to view menu." (You can modify these PXE boot prompt settings on the **Configure > Services > OS deployment** tab.)
4. If the **F8** key is pressed before the countdown expires, a preliminary PXE boot menu appears, allowing you to choose from the following boot options:
   - **Local boot:** The device boots to the local hard drive. If no OS is present, an error message appears.
   - **LANDesk managed boot:** The device is added to the console's network view (displays the device's MAC address), where you can schedule an OS deployment script to run on it.
   - **LANDesk boot menu:** The device displays the boot menu you created with the PXE Boot Menu tool, and you can select an OS deployment script to run on it. For more information, see "Configuring the PXE boot prompt" on page 213.
5. If you don't press the **F8** key before the countdown expires, the device will use the default boot option. The default boot option is determined by the following conditions:
   - If the device detects a scheduled imaging job for itself in the core database (either a failed or pending job), the default boot option becomes **LANDesk managed boot**.
   - If the device does *not* detect an image job for itself, the default boot option becomes **Local boot**.
   - The PXE DOS menu will never become the default boot option.
6. The scheduled OS deployment script runs on the device.

Understanding the PXE boot options

This section provides information on configuring the PXE boot prompt, and how to use the following PXE boot options:

- LANDesk managed boot
- PXE Boot menu
- PXE holding queue

Configuring the PXE boot prompt

You can control how the PXE boot prompt behaves when devices attempt to PXE boot.

When a PXE-enabled device boots up, a DHCP request attempts to initiate a PXE session by looking for a server (or proxy) running PXE services software (PXE and MTFTP) services. If the device discovers a PXE server, the PXE boot prompt displays on the device for a specified number of seconds. By pressing the F8 function key during this countdown, you access the PXE boot menu and can select an OS image to deploy on the device.

If you have PXE representatives running on subnets of your network, and you want to implement PXE boot prompt changes to any of those proxies, you must run the PXE Representative Deployment script on the proxy.

To configure PXE boot prompt options

1. Click **Configure > Services**, then click the **OS deployment** tab.
2. Enter a value (in seconds) in the **Timeout** option. The default value is 4 seconds. The maximum number of seconds you can enter is 60 seconds.
3. Type a message in the **Message** text box. The default message is "Press F8 to view menu." The maximum number of characters you can type is 75 characters.
4. Click **Apply** to save your changes, or click **OK** to save your changes and close the dialog.

To implement PXE boot prompt changes to a PXE representative

1. Click **Tools > Distribution > Manage scripts**.
2. Select **Public scripts > PXE representative deployment**. Right-click the script and select **Schedule**.
3. Drag and drop the PXE representative from the network view onto the task in the **Scheduled tasks** window.
4. Right-click the **PXE representative deployment** script, click **Properties**, and finish configuring the task.

Using LANDesk managed boot

LANDesk managed boot is the default boot option when a PXE-enabled device boots and detects a failed image deployment script or failed DOS task script for it in the core database. You can also select this boot option manually at the device when the boot option menu appears.

Because it allows unattended deployment, LANDesk managed boot is useful for pre-targeting devices for imaging. For example, you could pre-target new devices for a particular OS image even before they arrive by importing a .CSV file containing device MAC addresses into the core database. For more information, see "Using CSVIMPORT.EXE to import inventory data" on page 570.

To pre-target devices with the LANDesk managed boot option

1. Before the PXE-enabled devices are connected to the network, add their identifications to the core database by importing a .CSV file.
2. Schedule an image deployment job for the devices.
3. The imaging job fails because the devices are not yet connected to the network.
4. Connect the devices to your network and boot them.
5. The devices detect a failed imaging job and default to the LANDesk managed boot option.
6. The previous failed image deployment job automatically launches and images the target devices.

Using the PXE boot menu

The PXE boot menu lets you interactively select an image deployment script for a device without having to schedule an image deployment job. This method might be useful when you have to re-image corrupted devices. Before using the PXE boot menu, you must first configure it by adding the OS deployment scripts you want to display in the menu.

You build the PXE boot menu system by creating directories and placing pre-configured OS deployment scripts in those directories. The script's description appears as a menu item in the PXE boot menu on the device.

To configure the PXE boot menu

1. Click **Tools > Distribution > PXE Boot Menu**.
2. To add a new directory or subdirectory to the menu system, click the **New** toolbar button (or right-click the parent directory and select **New**).

Subdirectories can extend four levels from the top directory.

3. Type a name for the directory. For example, the directory name could describe the OS platform or version number of the images contained in that directory. You can also change the name of the directory at any time by clicking the **Rename** toolbar button (or right-clicking the directory and selecting **Rename**).
4. Click **Tools > Distribution > Manage scripts**, then drag and drop image deployment scripts to the appropriate directory in the **PXE Boot Menu** window.

A maximum of 18 scripts can be placed in each directory.

5. To save the PXE boot menu, click the **Update** toolbar button. (Note that you must click the Update button here in the console if you want changes to appear in the PXE boot menu on PXE devices when they boot.)

To access the PXE boot menu from a device

1. Boot a PXE-enabled device.
2. When the PXE boot prompt displays, press the **F8** key before the countdown expires. Select **PXE DOS menu**. The menu system that you configured in the console's PXE Boot Menu window appears.
3. To open a directory and view its subdirectories and images, type the number of the directory and press **Enter**. Navigate the menu system and find the image you want deployed on the device. You can press **B** to go back one level, or press **X** to exit the menu system.

If you exit the menu system without making a selection, the device will wait for a scheduled imaging job from the core server.

4. To select an OS image (referenced in an OS deployment script), type the number of the script and press **Enter**. The script runs and the image is loaded on the device.

Using the PXE holding queue

The PXE holding queue is another method for remotely deploying OS images to PXE-enabled devices. This method is especially useful in these situations:

- In a controlled lab environment where you frequently need all devices re-imaged with an identical image.
- For imaging "bare-metal" devices in a lab that can then be moved into their appropriate production environment.

By designating a subnet's PXE representative as a PXE holding queue, all the PXE-enabled devices on that subnet will be automatically added to the PXE holding queue in the console's network view when they PXE boot. You can also add a device to a PXE holding queue by scheduling the PXE - Add to Holding Queue script on the device, or by copying the device directly into the PXE holding queue group in the network view. Devices can then be scheduled for an image deployment job.

To configure a PXE holding queue

1. Set up PXE representatives on your network.

2. Click **Configure > Services**, then click the **OS deployment** tab.
3. Select and move PXE representatives from the **Available proxies** list to the **Holding queue proxies** list.
   The **Available proxies** list shows all available PXE representatives on your network, identified by device name. This list is generated by running an inventory scan that detects PXE software (PXE and MTFTP) protocols running on the device. The inventory scan is run automatically whenever a PXE representative is initially set up.
4. Click **Reset**. The Reset button forces all PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the PXE holding queue in the console's network view. These devices can then be scheduled for an imaging job.

The Reset button is enabled when you select a PXE representative in the Holding queue proxies list.

5. Click **OK** to save your changes and close the dialog.

The next time a device on that subnet boots, it will be added to the PXE holding queue object in the console's network view.

To deploy an image to a device in the PXE holding queue

1. Click **Tools > Distribution > Manage Scripts**.
2. Click an OS deployment script from the list, then click the **Schedule** toolbar button.
3. In the console's network view, open the **PXE holding queue** folder, then select the target devices you want to deploy the image to.
4. Drag and drop the selected devices to the **Scheduled tasks** window, and from the task's shortcut menu, click **Properties** and finish configuring the task.

Troubleshooting

Invalid OEM drivers in a Windows PE image will reset a device's boot environment and cause OSD tasks using that image to fail

If you add an invalid OEM driver to a Windows PE image and use that image for a task on a device, the device will boot into the Windows PE from that point onwards and the OSD task won't run. If this happens, do the following to fix the Windows PE image and restore the normal boot environment:

1. On the OSD toolbar, click the **Manage the drivers in the Windows PE image** button.
2. Remove the invalid OEM driver from the PXE-based Windows PE file (under \\pxeserver\..\PXE\System\images\peboot.img) and agent-based Windows PE file (under \\coreserver\ldmain\landesk\vboot\ldvpe1.img).
3. PXE boot the device to the modified Windows PE image by selecting the "LANDesk Managed WinPE" option.
4. Once the image boots, run this command: Diskinfo fix
5. Restart the device and it will boot to the previous OS normally.
6. Execute the OSD task what you scheduled.

Hardware-independent imaging

As you deploy images to your managed devices, it's challenging to maintain many different images based on different hardware configurations. New hardware requires new drivers, and existing hardware may have updated drivers you want to deploy. Rather than maintain dozens or hundreds of individual images for various hardware configurations, you can use hardware-independent imaging (HII) to deploy a base image to different devices and then automatically add the drivers that are required for each different type of hardware.

Hardware-independent imaging helps resolve common problems with imaging managed devices. For example, the hardware abstraction layer (HAL) .dll files need to be accurately chosen or the device may reboot to a black screen after imaging. Operating systems typically don't have the ability to recognize mass storage devices correctly, so it's important to have the right drivers when imaging. Also, manufacturers often have hardware-specific plug-and-play device drivers or they build driver dependencies into their applications, so it's possible to create new problems when imaging a device with the wrong drivers. With the hardware-independent imaging tool in LANDesk Management Suite you can avoid these types of problems and have greater control over the use of drivers in your managed devices.

An important consideration in using LANDesk hardware-independent imaging is that you can use it with images from any imaging tool. You can define the images with the tool you prefer, then create imaging scripts in Management Suite that incorporate the HII tool. If you already have images created with another tool, you'll be able to re-use them rather than create all new scripts.

A simplified description of the HII process is as follows. Details about the specific steps you'll need to follow and considerations for different types of images are described in the following sections.

1. When you deploy an image created using HII, the imaging script boots the device to the Windows preboot environment. In the preboot environment, the HII tool will select the appropriate HAL .dll file and load it.
2. The OS is installed on the device, but before the OS boots, the HII imaging script determines which drivers are required by the device and copies the driver files to the device's hard disk.
3. The drivers are added to the device's registry, so that when the OS boots the Windows setup detects the new drivers, installs them, and configures the device with the drivers.
4. Windows then restarts with the drivers running, and the Management Suite agent is installed.

Note: Because of changes to how administrator user account permissions are handled in Windows Vista and especially in Windows 7, you may find that master images you create that include these versions of Windows may not successfully deploy. We recommend that you visit the LANDesk Support Community website, community.landesk.com, for best-known method documents that describe master image scenarios and recommended procedures for creating and deploying images.

Tasks to set up hardware-independent imaging

To implement hardware-independent imaging with OS deployment scripts or provisioning templates, there are two general tasks you need to complete for the drivers you want to use in your images:

- Create a library of drivers that will be available to the imaging tool. These drivers are used on the hardware you want to image, and are for devices in categories such as audio, video, network, mass storage devices, and other types of devices.
- Associate specific device models with drivers in your library. When the hardware-independent imaging tool runs it will detect the device manufacturer and model, and then download the associated drivers and install them on the device during the imaging process.

These two tasks are described in the following sections. In addition, there are notes for how to incorporate hardware-independent imaging into OS deployment scripts and provisioning templates.

Creating a driver library

As you plan and define the images you want to use for managed devices, you'll decide which drivers you want to use with specific device models. To use these drivers for hardware-independent imaging, you create a library of drivers that is saved on the LANDesk Management Suite core server. The drivers are then available for any deployment or provisioning script you want to run.

To create a library, you need to have the driver files in a folder, and the driver's .inf file must be included. You can include drivers from any device or share, because the files will be copied to the core server and stored in the library.

To add a driver to the driver library

1. Click **Tools > Distribution > OS Deployment**.
2. Click the **Manage driver library** button on the toolbar.
3. Click **Add**.
4. Select the **Device type** for which you will add a driver.
5. Type the name of the device in the **Device name** text box.
   This is also a list that lets you select a device name you have previously used.
6. Click **Next**. Select the versions of Windows that the driver can be used with.
7. Type any details about the driver that you need for your reference.
8. Click **Next**. Click **Browse** and specify the location of the driver files.
   All driver files in the folder you selected are displayed.
9. Verify that the correct files, including a .inf file, are displayed in the list, and click **Next**.
10. If the driver files are valid, you will see a success message. Click **Finish** to close the dialog box.
    If you see an error icon, you'll need to find the correct driver files for the driver you have named.

    The driver you added is now displayed in the **Hardware-independent driver library** dialog box, under its corresponding device type. You can add other drivers by repeating the steps above.
11. To add the drivers to the device library, click the **Update** button. Click **Close** when you have finished managing your drivers.

Associating devices with drivers in the library

When you have created a driver library for hardware-independent imaging, you can associate specific device models with the drivers you want to use in imaging those devices. By doing this you ensure that you can use one basic image for devices from different manufacturers, because as the HII tool runs it will find the correct drivers for each different device type.

The list of manufacturers and models that you use in this process must be accurate. These strings need to match the manufacturer and model strings in the device BIOS, which is where the HII tool looks to determine the correct model name.

To associate a device manufacturer and model with a driver in the library

1. Click **Tools > Distribution > OS Deployment**.
2. Click the **Manage manufacturer and model** button on the toolbar.
3. In the **Manufacturer** column click the **Add** button.
4. Select a manufacturer name from the list, or type a new name and press **Enter**.
5. With the manufacturer selected, click the **Add** button in the **Model** column.
6. Select a model name from the list, or type a new name and press **Enter**.

7. With the model selected, click the **Add** button in the **Device name** column.
8. In the **Map model and device** dialog box, select the device type in the left column and the device name, then click **OK**.
   The devices listed here are those you have added to the driver library.
9. Repeat the steps above to make other associations between device models and the drivers you want to install on them. When you have finished, click **Exit**.

Using hardware-independent imaging with OS deployment scripts

You can incorporate hardware-independent imaging into an OS deployment script for Windows devices, if the script meets these requirements:

- It must be based on the Windows PE boot environment
- It must use Windows Sysprep to configure the OS image

To incorporate hardware-independent imaging, you need to select the HII option in the script wizard so the HII tool runs after the operating system is installed. Also, you need to select one of the following options:

- You can have the HII tool automatically select the manufacturer and model of the device you are imaging, based on the strings in the device's BIOS. Select this option if you want to use the script for devices from multiple manufacturers.
- You can specify one manufacturer and model. Select this option *only* if you will use the script on the same device model every time.

To include hardware-independent imaging in an OS deployment script

1. Click **Tools > Distribution > OS Deployment**.
2. Under **OS images**, select a script. Right-click the script and select **Edit**. Or, to create a new script, right-click **All OSD Scripts** and select **New Windows PE configuration**.
3. Click **Methods and credentials**. Select the **Images uses Sysprep** and **Use Hardware-independent imaging** check boxes.
4. Click **Sysprep options > Hardware-independent imaging**.
5. To have the HII tool automatically select the manufacturer and model of the device to be imaged, click **Auto detect**.
   The tool will read the settings in the device BIOS to find strings that match the manufacturer and model strings you have defined when you associated device models with drivers.
6. If you want to specify a manufacturer and model for the script, click **Select manufacturer and model**. Select a manufacturer and then a model from the lists. The device drivers associated with that model are listed for your reference.
7. Define all other script options you want, and click **Save** to save the script.

Using hardware-independent imaging with provisioning templates

You can incorporate hardware-independent imaging into a provisioning template for Windows devices, if the template meets these requirements:

- It must be based on the Windows PE boot environment
- It must use Windows Sysprep to configure the OS image

To incorporate hardware-independent imaging, you need to add an HII option in the **Post-OS installation** section of the template, so the HII tool runs after the operating system is installed.

There are two options for provisioning templates:

- You can have the HII tool automatically select the manufacturer and model of the device you are provisioning, based on the strings in the device's BIOS. Select this option if you want to use the provisioning template for devices from multiple manufacturers.
- You can specify one manufacturer and model, and select drivers for that model. Select this option *only* if you will use the template on the same device model every time.

To include hardware-independent imaging in a provisioning template

1. Click **Tools > Distribution > OS Deployment**.
2. Under **Provisioning templates**, select a Windows-based template. Right-click the template and select **Edit**. Or, to create a new template, click the **New provisioning template** button on the toolbar.
3. Click **Action list**, then click the **Post-OS installation** section.
4. Click **Add**. Type a name and description for the action (such as HII), and then select **Hardware-independent imaging** from the **Type** list. Click **OK**.
5. To have the HII tool automatically select the manufacturer and model of the device to be provisioned, click **Auto detect**.
   The tool will read the settings in the device BIOS to find strings that match the manufacturer and model strings you have defined when you associated device models with drivers.
6. If you want to specify a manufacturer and model for the template, click **Select manufacturer and model**. Select a manufacturer and then a model from the lists. The device drivers associated with that model are listed for your reference.
7. Click **Apply** to save the HII action with the template, then add any other actions to the template. Note that you should include a **Reboot** action in the **Post-OS installation** section *after* the HII action.
8. Modify any other variables, included templates, or other settings for the template, and click **OK** when you have finished.

Provisioning

Provisioning overview

Read this chapter for information about:

- Introduction to provisioning
- The provisioning interface
- Steps for provisioning a device
- Provisioning bare metal devices

Introduction to provisioning

LANDesk provisioning lets you define all the attributes and features of new devices before they are introduced into your environment. Provisioning uses automation to apply this set of attributes and features to the devices. With provisioning you can reduce downtime and make sure new devices are reliable and predictable when they go into your production environment. You can access the provisioning history of each device to find out when and with what it was provisioned, and, if necessary, return it to a previous state. Provisioning runs on both Windows and Linux; there is no difference in the way you create templates for either operating system.

Provisioning consists of a series of actions to be executed on a target device. **Actions** are the fundamental unit of provisioning. A **template** is a collection of actions that are executed in a pre-defined order. LANDesk provides several pre-built provisioning templates to get you started. These are optimized to work with specific hardware configurations, such as several popular Dell and Hewlett-Packard systems. You can combine these provisioning templates with your own master templates, or run these templates with little modification to generically provision a specific Dell- or HP-brand device. You can split the provisioning tasks the way you split the work when setting up a system manually.

Provisioning works equally well on new devices or dynamic devices. You can provision new devices with the precise configuration you require, setting up the configuration before the new device has even arrived. You can use provisioning to reconfigure a device from one purpose to another, changing a device's base function to handle your organization's changing demands.

You can use alerting to let you know when provisioning events occur. For more information, see "Monitoring with alerts."

Provisioning agent

The center of provisioning is the agent ldprovision, located in the /ldlogon/provisioning folder. This agent consists of small applications for each action. The agent resides on the target device. It is placed there through a PXE server or a physical boot media such as a USB drive or a CD.

The provisioning process is completed as the agent does the following:

- It requests a template's configuration settings from a web service on the core server
- It checks the preboot type tag to ensure it is running in the correct preboot environment
- It performs the actions in the order designated in the configuration
- It reboots the device (if necessary)

- It injects a version of itself into the target OS so it can continue working when the real OS loads after the reboot
- It sends feedback to the web service on the core

The agent spans any reboots required, immediately moving to the next action after the reboot. Most provisioning work can be done before you receive a new device. You can create a template and create the task for the template to run on the new device. The task will not run until the provisioning agent runs on the new device.

To fully use provisioning, users require two rights: the Provisioning - Schedule right and the Provisioning - Configuration right. Together, these rights let a user create, edit, and schedule provisioning templates. These rights are automatically enabled for any users with Administrator rights, and can be enabled for any users. For more information, see Role-based administration.

Preboot tools

Provisioning requires the ability to boot the device prior to putting an operating system on it. This can be accomplished through a PXE server or through a physical boot media (CD or USB drive). PXE is the most convenient way to boot many computers at a time into the same preboot environment. CD or USB drives are highly portable and guarantee that the computer running the preboot environment is the one the administrator intended to provision.

The preboot environment (PE) includes an operating system complete with video, networking, a small inventory scanner, and an agent capable of receiving files and executing commands. This agent executes an imaging tool or scripted install tool to install the OS on the device. The agent initiates the provisioning process. Provisioning supports the Windows and Linux preboot environments.

It is recommended that you install the new operating system using the same type of preboot environment that you are installing. For example, install Windows using the Windows PE and install Linux using the Linux PE. This is because Windows PE does not support EXT2, EXT3, or Reiser file systems, and Linux, though it supports NTFS, may cause problems with misconfiguration, particularly if PXE is isolated from the production network.

You don't need unique boot media for each client system; you can re-use the boot media for other devices.

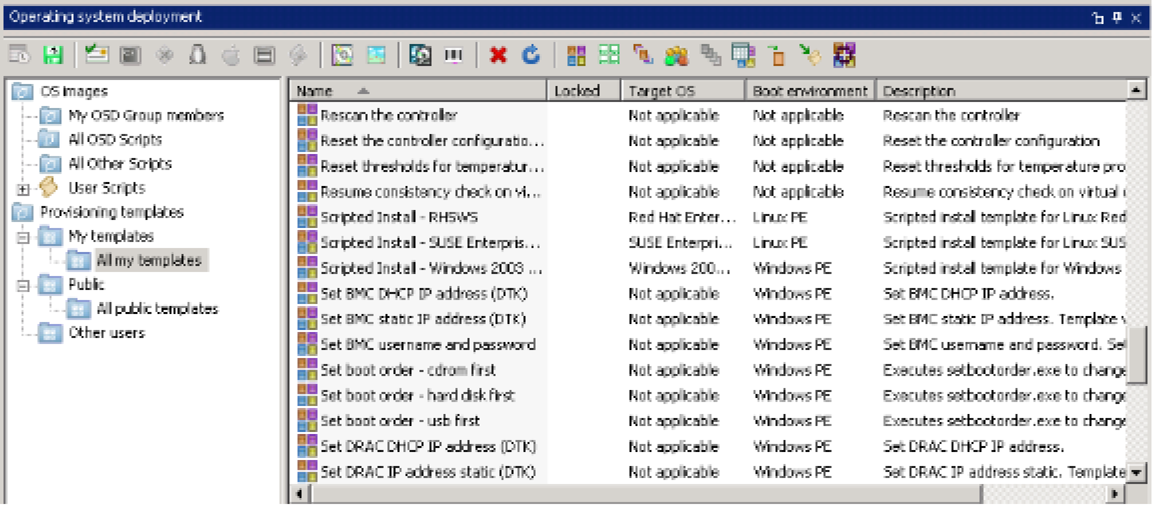
Differences between OS deployment and Provisioning

Provisioning has broader use than OS deployment. While OS deployment can be part of the provisioning process, it is only one part of provisioning. Provisioning encompasses the start-to-finish process of preparing a device for secure usage in your environment. The table below shows how provisioning differs from OS deployment.

OS deployment	Provisioning
Driven from the core	Driven from the target device
Work done after device arrives from factory	Most work can be done before device arrives
Encompasses only the OS deployment step of the provisioning process.	Comprises the end-to-end sequence of building a device
Requires one entire image; cannot be broken down	Comprised of smaller templates, which can be modified or swapped out at template level

The provisioning interface

The provisioning tools are a part of the Operating system deployment tool (click **Tools > Distribution > OS deployment**). A tree structure displays provisioning templates, and a toolbar opens dialog boxes for different tasks.



Name	Locked	Target OS	Boot environment	Description
Rescan the controller		Not applicable	Not applicable	Rescan the controller
Reset the controller configuratio...		Not applicable	Not applicable	Reset the controller configuration
Reset thresholds for temperatur...		Not applicable	Not applicable	Reset thresholds for temperature pro
Resume consistency check on vi...		Not applicable	Not applicable	Resume consistency check on virtual
Scripted Install - RHSWS		Red Hat Enter...	Linux PE	Scripted install template for Linux Red
Scripted Install - SUSE Enterpris...		SUSE Enterpri...	Linux PE	Scripted install template for Linux SUS
Scripted Install - Windows 2003 ...		Windows 200...	Windows PE	Scripted install template for Windows
Set BMC DHCP IP address (DTK)		Not applicable	Windows PE	Set BMC DHCP IP address.
Set BMC static IP address (DTK)		Not applicable	Windows PE	Set BMC static IP address. Template
Set BMC username and password		Not applicable	Windows PE	Set BMC username and password. Se
Set boot order - cdrom first		Not applicable	Windows PE	Executes setbootorder.exe to change
Set boot order - hard disk first		Not applicable	Windows PE	Executes setbootorder.exe to change
Set boot order - usb first		Not applicable	Windows PE	Executes setbootorder.exe to change
Set DRAC DHCP IP address (DTK)		Not applicable	Windows PE	Set DRAC DHCP IP address.
Set DRAC IP address static (DTK)		Not applicable	Windows PE	Set DRAC IP address static. Template

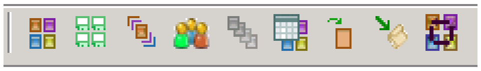
In the tree structure, available templates are organized in the following folders:

- **My templates:** Templates that you have created. Only you and administrative users can access these templates
- **Public:** Both your templates and templates marked as public.
- **Other users** (administrative users only): A list of users and their templates.

Public templates are created by users with Administrator rights and are viewable by all users. Templates in the My templates folder are visible to others but can only be edited by the template's creator or users with Administrator rights. Each time you use a template not marked public, the instance of the template is locked in history. This instance can't be deleted, but it can be hidden.

The right pane displays the selected folder's templates, with five columns that show the template properties. Double-click a template to view its complete properties, including a list of other templates that include the selected template.

The toolbar includes buttons for creating, modifying, and managing provisioning templates.



- **New provisioning template**: Lets you create a provisioning template,
- **Create provisioning boot media:** Lets you configure and create boot media.
- **Condense the template**: Combines all included templates into the selected template, so there is only one template file to execute.
- **Public variables:** Lets you view and set global variables that apply to all provisioning templates.
- **Create a template group**: Lets you organize templates by creating groups within a folder.
- **Schedule a template:** Opens the Scheduled tasks tool, allowing you to view provisioning and other management tasks. You can schedule provisioning tasks and view the status of tasks.
- **Import templates:** Imports a template into the core database.

- **Install scripts:** Lets you make installation scripts available for use in creating scripted installation actions and deploy image action in templates.
- **Update templates:** Lets you download and import templates from LANDesk, and configure the template download location as well as proxy server settings.

If you double-click a template, the Template view opens. From this view, you can modify the action list (add or delete actions, modify the action order, and so forth). You can modify variables applying specifically to this template, view and modify the list of templates included by this template, or the list of templates that include the template. You can make a template public, view its history (when the template was executed), and view or modify the template's XML code.

Creating and editing provisioning templates

The **New template** button is the starting point for creating a new template. To modify a template, right-click the template and select **Edit**. To remove a template, select it and click the **Delete** button. You can only delete templates that have never been used.

Creating template groups

You can use provisioning groups to organize your templates in ways to suit your needs. For example, you could create groups based on specific vendors, and additional subgroups based on device models. You can create subgroups up to six layers deep.

Cloning existing templates

Once a template has been used, it cannot be changed directly. It can be cloned, and then changed. For this reason we recommend that templates be smaller in nature so that if any changes are required, you can change that one component of the provisioning configuration.

The **Clone** option makes a copy of the selected template. You can modify the copy, making minor changes to the copy rather than taking the time create an entirely new template.

If you clone a public template, the copy is placed in the My templates folder
and acquires the properties of a private template.

1. Click the **Public** or **My templates** folder to display templates in the right pane.
2. Right-click a template and select **Clone**.

   A copy of the template is created in the folder, with the name of the original template and the date and time the clone was created.

3. To change the name, description, boot environment, or target OS of the cloned template, right-click the clone, click **Properties**, modify the settings, and click **OK**.
4. To modify the actions, included templates, user variables, or the XML of the cloned template, double-click the clone to open the **Template** view.

Condensing a template

Use the **Condense** button to combine multiple templates into one template. If there are other templates included with the current template, their XML code will be saved within the XML code of the template to create a single XML file. Once you condense a template, it can't be expanded into separate templates again.

Steps for provisioning a device

On the most basic level, provisioning a device is a simple process consisting of three steps. First, you create a provisioning template, then you configure the template with the features and components you want to install on the device, and then you schedule a task to run the template on the device. These steps are outlined briefly here; detailed instructions are found in the following sections.

Step 1: Creating a template

To provision a device, you create a template. A template is an XML document with a series of building blocks to be applied to the device. They build upon each other, and can consist of actions, attributes, constraints, and so forth. A template can have one or many actions.

Templates may be chained together in a provisioning task in a particular sequence. You can change the task order in a template. The sequence can be changed where applicable (for example, one cannot place a post–OS task before the installation of the OS). There are numerous pre-configured templates for various vendors (HP, Dell, and so forth).

Templates are saved as XML documents in the database.

To create a template

1. Click **Tools > Distribution > OS deployment**.
2. In the Operating system deployment tool, click **New provisioning template** on the toolbar.
3. Type a descriptive name in the **Name** text box.
4. Select the boot environment you want the template to preboot the device to (Windows PE or Linux PE).
5. Select a target operating system for the template (Windows or Linux). The boot environment and target OS should match (Windows PE and Windows OS, or Linux PE and Linux OS).
6. Type a description in the **Description** box.
7. Click **OK**.

The name and description are displayed in the list of templates.

Step 2: Configuring the template

Once the template is created, it must be configured by adding actions to it. Template actions are sorted into five sections. You can only select actions in each section that can apply to the section (for example, you can't select Software distribution as an action for the Pre-installation section). You can add any available action to any section, but be aware that some actions will break the template or may render your system unusable if completed in the improper steps.

1. Double-click the template you just created.
2. In the left navigation pane, click **Action list**.
3. In the middle pane, select the section in which you want the action to occur.
    - **System migration:** Features and components that need to be saved before modifying the system (or migrating a device to other hardware or virtual machine). For example, this section can include an action to capture profile information when migrating to Windows Vista.
    - **Pre OS install:** Actions that are performed when the device boots into a pre-installation environment (Linux PE, Windows PE). For example, on a server you would add RAID configuration in this section.
    - **OS Install:** Actions that are performed in the pre-installation environment when the OS in installed (Linux PE, Windows PE).

- **Post OS Install:** Actions that are performed in the target operating system after it has been installed, such as running a patch management task.
- **System configuration:** Additional application installation/execution and system configuration in the installed OS. For example, add driver installation tasks in this section.

4. Click **Add**.
5. Type a specific name for the action in the **Name** field.
6. Type a detailed description of the action in the **Description** field.
7. In the **Type** list select an action type.
8. Under **Action variables**, click **Add** to add a variable that applies to this action only. Specify the values in the text boxes, select the variable type, and click **OK**.
9. Under **Selected action properties**, complete the data required for the action type. This data varies depending on the action type you selected.
10. When the action is defined, click **Apply** to save it and continue editing the template. When you have finished defining the template, click **OK**.

Step 3: Scheduling the template for deployment

A provisioning task contains templates and the device identifiers of the target devices. When a provisioning task begins, the job is associated with the device’s Computer record in the database so that the configuration history remains attached to the computer. Configuration tasks can't be reused with different target devices, but can be reused by specifying another device identifier.

The **Scheduled tasks** tool shows scheduled task status while the task is running and upon completion. The scheduler service has two ways of communicating with devices: Through the standard management agent (must already be installed on devices), or through a domain-level system account. The account you choose must have the login as a service privilege and you must have specified credentials in the Configure Services utility. For more information on configuring the scheduler account, see "Configuring the scheduler service."

To schedule a provisioning task

1. In the **Operating system deployment** tool, select a template from one of the **Provisioning templates** folders.
2. Click the **Schedule template** button on the toolbar.
   The Scheduled tasks tool opens with a task for the provisioning template.
3. In the network view, select the devices to which you will deploy the provisioning task. Drag the devices to the **Scheduled tasks** tool and drop them on the provisioning task.
4. Right-click the provisioning task and select **Properties**. Select a schedule option and click **Save**.

When you click **Schedule template**, a task is created (it has no targeted devices, and it is unscheduled). If you don't add target devices or schedule the task, be aware that the task remains in the task list until you schedule it or delete it.

In the **Scheduled tasks** tool, tasks are grouped in the following folders:

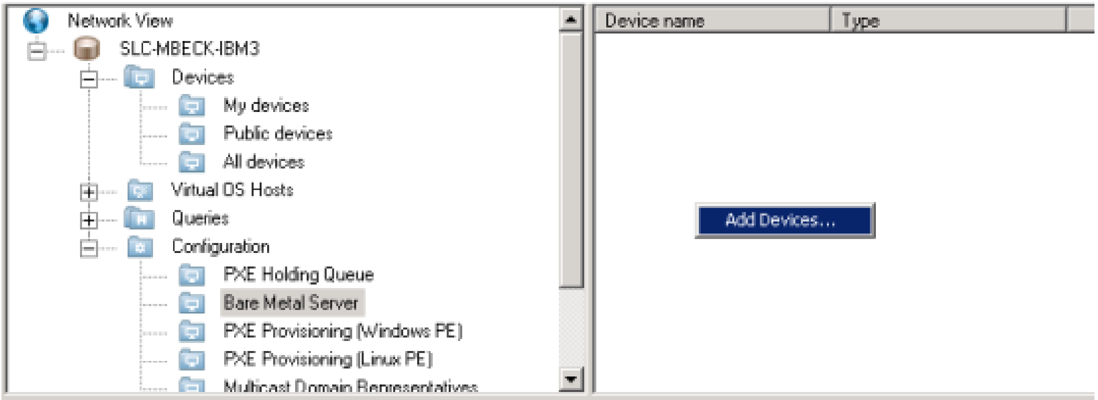
- **My tasks:** Tasks that you have scheduled. Only you and Management Suite administrative users can see these tasks.
- **Public tasks:** Tasks that users have marked public. Anyone who schedules a task from this category will become the owner of that task. The task remains in the **Public tasks** folder and will also be visible in the **User tasks** group for that user.
- **All tasks:** Both your tasks and tasks marked public.
- **User tasks** (Management Suite administrative users only): All tasks users have created.

Provisioning bare metal devices

Provisioning lets you provision bare metal devices. You can begin this process before device is physically present. To do so, you enter a hardware identifier (such as the GUID or MAC address) for each new device in the **Configuration > Bare Metal Server** folder in the network view. The information required by the automated provisioning agent (ldprovision) is recorded in the database.

To provision bare metal devices

1. In the network view, click **Configuration > Bare metal servers**.
2. Right-click in the device list and select **Add devices**.



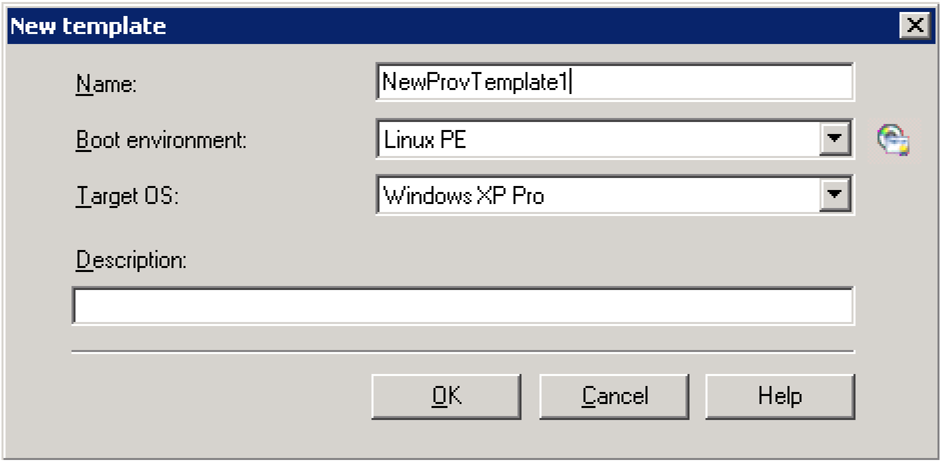
3. To enter data for individual devices, click **Add**. Type a name for the devices that you will add (you can type a name describing a group of devices or just one device).
4. Select a type from the **Identifier type** list.
5. Type the identifier for each device and click **Add** to add it to the list.
6. To import the device data, select a type from the **Identifier type** list. Type the drive, path, and filename of the import file or browse to select it. Click **Import**.
7. Associate each device with a provisioning template.
8. Plug in the devices and provide them an ldProvision boot CD, bootable USB drive, or configure BIOS to network/PXE boot.
9. Power up the devices.

Creating provisioning templates

Use the Template dialog to create a provisioning template. A template is a series of actions or building blocks to be applied to the server in a particular order. A template can have one or many actions. You can change the task order in a template. The action sequence can be changed where the action makes sense, but cannot be changed where it does not make sense (for example, one cannot place a post-OS-specific action before the installation of the OS). There are numerous pre-configured templates for various vendors (HP, Dell, and so forth). Templates are stored as XML in the database.

To create a template

1. Click **Tools > Distribution > OS Deployment**.
2. Under the **Provisioning templates** group, select either the **Public** or **My templates** folder.
3. Click **New provisioning template** on the toolbar.



New template

Name: NewProvTemplate1

Boot environment: Linux PE

Target OS: Windows XP Pro

Description:

4. Type a descriptive name in the **Name** box.
5. Type a description in the **Description** box. The Name and Description are displayed in columns in the list of templates.
6. If necessary, select the boot environment you want the template to preboot the server in (Windows PE or Linux PE).
7. If necessary, select a target operating system for the template. The boot environment and target OS should match (for example, Windows PE and Windows OS).
8. Click **OK**.

To change template properties, double-click the template or right-click the template and select **Properties**.

To delete a template

1. Select a template, and click **Delete**.
2. Click **Yes**.

You can delete only templates that have not been previously executed (locked) and that are not included in other templates. Locked templates can be deleted (removed) from the list view but remain in the database.

Creating boot media

Use the LANDesk Boot Media Creator dialog to create boot media that can be used to provision devices. Provisioning creates a physical media by which to boot the device into a preboot environment. This media can be delivered through a PXE server or a bootable USB device/CD/DVD. A preboot environment consists of an operating system complete with video, networking, a mini-inventory scanner, and an agent capable of receiving files and executing commands. In order for the boot media to work, you must configure the target device to boot from the proper media (in BIOS enable network IPXE or CD/DVD boot).

1. Click **Tools > Distribution > OS Deployment**.
2. On the toolbar, click the **Create provisioning boot media** button.
3. Select the **Preboot environment type** (Windows or Linux).
4. Select the **Boot media type** (USB drive, bootable CD, or bootable ISO). If you selected USB Drive, insert the USB drive and select the drive letter. If you selected Bootable CD, select the CD burning drive. If you selected Bootable ISO, select the destination path the ISO will be saved to.
5. Click **Create boot media.**

The creation of boot media may fail if the system is low on memory.

When creating a USB boot media, you must have administrator rights. In the case of Microsoft Vista, you have to download the program and run the program as administrator.

To create CD or ISO media, the device where you run the boot media creation tool must have IMAP2, which is available from Microsoft at http://support.microsoft.com/kb/kb932716.

Deploying PXE representatives

PXE support software is installed on your core server as part of the normal installation. However, to enable PXE support, you must first deploy a PXE representative on each subnet of your network where you want PXE support available. PXE representatives provide scalability on your network by deploying OS images to devices in their respective subnets..

Devices on each subnet use normal PXE query and file transfer methods to communicate with their resident PXE representative, which communicates with the core server using Web services (HTTP).

Disable other PXE servers
If there is *any* other PXE server currently running on your network, you must first disable it in order to use LANDesk PXE support.

Deploying PXE representatives

You need to deploy one PXE representative on each subnet where you want to provide PXE boot support. You set up a PXE representative by running the PXE Representative Deployment script on the selected device. This predefined script is available in the **Manage scripts** tool (click **Tools > Distribution > Manage scripts**, then click the **Public scripts** folder).

You can have multiple PXE representatives on a subnet to help with load-balancing. When this is the case, the first PXE representative to respond to a device's request is the one that will be used to communicate with the core server.

We recommend that you do *not* deploy a PXE representative on your core server.

There are no special hardware requirements for the device you select to be a PXE representative, but it must meet the following software requirements:

- **Operating system:** Windows NT 4, Windows 2000, or Windows XP.

  For Windows NT and 2000, ensure that the Microsoft MSI service is running (XP includes MSI by default). If you have installed the latest service pack for either OS, MSI service should be running. Otherwise, you can deploy it to the target PXE representative from the console by following these steps: Click **Tools > Distribution > Manage scripts**, select the **MSI service deployment** task under **All scripts**, and click the **Schedule** button. In the **Scheduled tasks** windows, drag the target devices into the window, right-click the **MSI service deployment** task and select **Properties**, click **Schedule task** and specify a start time to schedule the MSI service deployment.

- **Installed agents:** Enhanced Software Distribution agent and Inventory Scanner agent. For more information, see "Configuring device agents" on page 75.

To deploy a PXE representative

1. In the console, click **Tools > Distribution > OS Deployment**.
2. In the **Operating system deployment** window, click the **All other scripts** tree item. Click the **PXE representative deployment** script, and then click the **Schedule** toolbar button.
3. In the console's network view, select the target device on which you want to install PXE services.

4. Drag and drop the selected device to the **PXE Representative deployment** task in the **Scheduled tasks** window.
5. Right-click **PXE representative deployment**, click **Properties**, and finish configuring the task.

Sharing templates

Use the Import templates toolbar button to import templates in XML format. You can edit the XML in the XML contents section of the Template view. The template displays in the following general XML format.

```
 <template name= >
        <description></description>
        <section name= >
              <description></description>
              <action></action>
       </section>
        <section name= >
              <description></description>
              <action></action>
       </section>
</template>
```

To import a template

1. Click **Tools > Distribution > OS Deployment**.
2. On the toolbar, click the **Import templates** button.
3. Type the path and file name of the XML file in the **Import file** text box, or click **Brows e** and select the file. Click **Import**. This imports the template into the **My templates** folder.

The file is saved as a .XTP file (XML Template Pages)

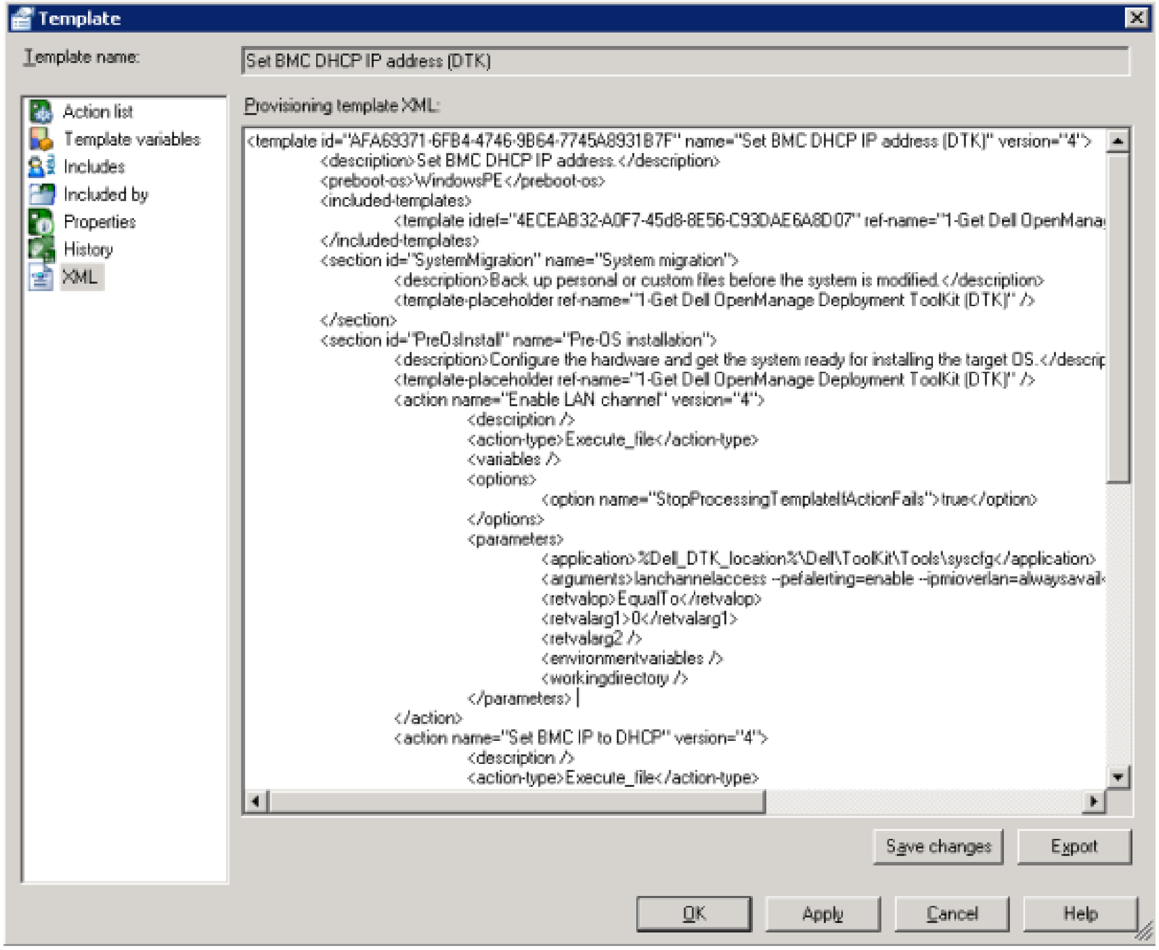
To export a template

1. Click **Tools > Distribution > OS Deployment**.
2. Select **Public** or **My templates** or one of their subgroups.
3. Double-click a template. In the Template view, click **XML**.
4. Click **Export**. Select the location you want to save the template to, and click **Save**.

The file is saved as a .XTP file (XML Template Pages). If you are exporting a template containing UTF- only characters, the title will not display correctly in Internet Explorer. The non-displayable characters in the template title will appear as underscores. You can change the template title through the **Save As** dialog box.

To view a template's XML code

1. Click **Tools > Distribution > OS Deployment**.
2. Select **Public** or **My templates** or one of their subgroups.
3. Double-click a template. In the Template view, click **XML**.
4. You can view or edit the XML code for the template. To save changes, click **Save changes**. Click **OK** to close the Template view.



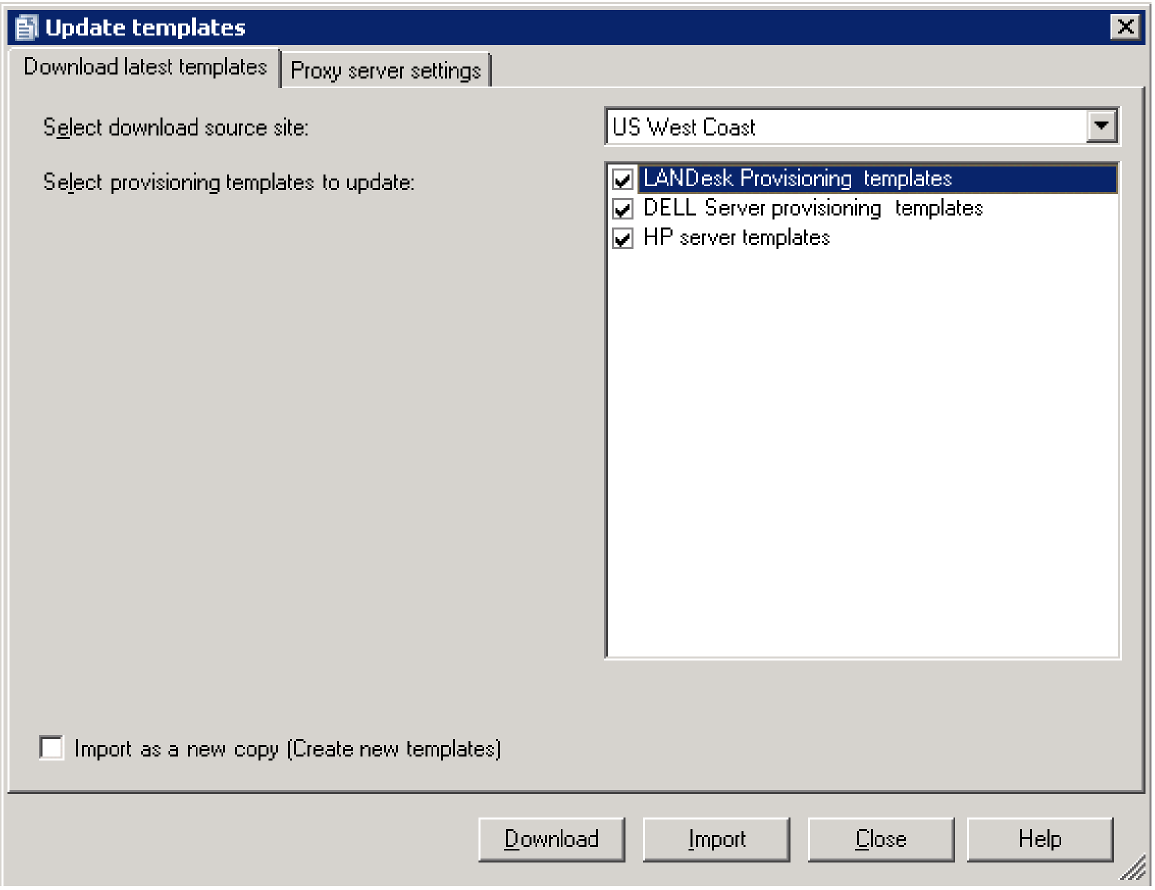
Template name: Set BMC DHCP IP address (DTK)

```
<template id="AFA69371-6FB4-4746-9B64-7745A89318 7F" name="Set BMC DHCP IP address (DTK)" version="4">
        <description>Set BMC DHCP IP address.</description>
        <preboot-os>WindowsPE</preboot-os>
        <included-templates>
                <template idref="4ECEAB32-A0F7-45d8-8E56-C93DAE6A8D07" ref-name="1-Get Dell OpenMana
        </included-templates>
        <section id="SystemMigration" name="System migration">
                <description>Back up personal or custom files before the system is modified.</description>
                <template-placeholder ref-name="1-Get Dell OpenManage Deployment ToolKit (DTK)" />
        </section>
        <section id="PreOsInstall" name="Pre-OS installation">
                <description>Configure the hardware and get the system ready for installing the target OS.</descrip
                <template-placeholder ref-name="1-Get Dell OpenManage Deployment ToolKit (DTK)" />
                <action name="Enable LAN channel" version="4">
                        <description />
                        <action-type>Execute_file</action-type>
                        <variables />
                        <options>
                                <option name="StopProcessingTemplateIfActionFails">true</option>
                        </options>
                        <parameters>
                                <application>%Dell_DTK_location%\Dell\ToolKit\Tools\syscfg</application>
                                <arguments>lanchannelaccess --pefalerting=enable --ipmioverlan=alwaysavail
                                <retvalop>EqualTo</retvalop>
                                <retvalarg1>0</retvalarg1>
                                <retvalarg2 />
                                <environmentvariables />
                                <workingdirectory />
                        </parameters>
                </action>
                <action name="Set BMC IP to DHCP" version="4">
                        <description />
                        <action-type>Execute_file</action-type>
```

Updating provisioning templates

Use **Update templates** to download and update predefined templates optimized for specific system hardware and common provisioning tasks. You can also specify proxy server settings if you use a proxy server for external access.

When any scheduled template update task runs, it uses the settings on this dialog that are current at the time, not the settings when the scheduled task was created.



Select download source site: US West Coast

Select provisioning templates to update:

- ☑ LANDesk Provisioning templates
- ☑ DELL Server provisioning templates
- ☑ HP server templates

☐ Import as a new copy (Create new templates)

Download latest templates tab

- **Select download source site:** Specifies which provisioning template content server you will access to update your database with the latest provisioning templates. Select the server nearest your location.
- **Select provisioning templates to update**: Identifies which platforms' provisioning templates are updated. You can select one or more platforms. The more platforms you select, the longer the download will take.
- **Import as a new copy:** Import the templates as new templates, not overwriting any existing templates or groups.

Proxy server settings tab

If your network uses a proxy server for external transmissions (such as Internet access), use this tab to enable and configure the proxy server settings. Internet access is required for updating provisioning template information.

- **Use proxy server:** Enables the proxy server option (by default, this option is off). If you enable a proxy server, you must fill in the address and port fields below.
- **Address:** Identifies the IP address of your proxy server.
- **Port:** Identifies the port number of your proxy server.
- **HTTP-based Proxy:** Enables the proxy server, if it's an HTTP-based proxy (such as Squid), so that it will successfully connect to and download patches from FTP sites. (Patches hosted at some FTP sites cannot be downloaded through an HTTP-based proxy unless you first enable this option.)

- **Requires login:** Allows you to enter a username and password if the proxy server is credentialed instead of a transparent proxy server.
    - **Username:** Enter a valid username with authentication credentials to the proxy server.
    - **Password:** Enter the user's password.

To download the latest templates

1. Click **Tools > Distribution > OS Deployment**.
2. On the toolbar, click the **Update templates** button.
   The **Update templates** dialog box opens. To save your changes on either tab, at any time, click **Apply**.
3. Select a download source site.
4. Select the vendor-specific templates you want to download.
5. Select **Import as a new copy** to save downloaded templates separately, without overwriting any existing templates or groups with the same name.
6. Click **Download**. A success message displays at the top of the dialog box.
7. Click **Import** to move the templates to the **My templates** folder.

Importing installation scripts

Use **Install scripts** to create a template out of one or more scripts. Install scripts makes installation scripts available for use in creating scripted installation actions in templates. Provisioning supports batch file scripts, shell scripts, and many other scripts. The Deploy image, Scripted install, and Inject script actions use scripts like sysprep.inf or unattend.txt. Install scripts can also insert variables into your scripts; for example, a device name can be inserted into a sysprep.inf file.

To import installation scripts

1. Click **Tools > Distribution > OS Deployment**.
2. On the toolbar, click the **Install scripts** button.
3. Type the path and file name of the script in the **File name** text box, or click **Browse**, navigate to the script, select it, and click **OK**.
4. Type a name for the script in the **Script name** text box. This name will display in the **Install scripts** list in this dialog box.
   It will also be displayed in the **Installation scripts** list when you add a Scripted install action to a provisioning template.
5. Type additional details about the script in the **Description** text box.
6. Select the target operating system in the **Target operating system** list.
7. Select the **Insert variables into script** check box if you want to swap out variables during the script import. When variables are replaced, the ones in the table below will be replaced automatically. Additional custom variables are supported, and the values will be replaced when the template is run.
8. Click **Import** to place the script in the **Install scripts** list.

To export an installation script

1. In the **Install scripts** dialog box, select the script in the **Install scripts** list.
2. Click **Export**. Specify a file name and location and click **Save**.

Using variables

Install scripts supports many key value pairs, such as:

Variable	Description
%ldHostname%	The host name
%ldDeviceID%	GUID of the device

If there is a key value pair in the WIN.INF file that already exists as a user-defined variable, Install scripts replaces it with the user-defined variable.

To pass variables through an installation script as a variable (not to be replaced by the provisioning process) encapsulate the variable in double percent signs, (for example, `%%variable%%`).

Notes on using scripts

- In Windows, a valid, active, formatted partition must exist before the Scripted install action can occur.
- The network installation source must have drivers for the target device injected correctly or put into the OEM's PnP driver path (for additional information, refer to the Microsoft installation documentation).
- Currently, only a command-line installation using winnt32 works.
- The file cmdlines.txt is used to append commands to the final OS boot.
- Currently, PXE/RIS is not supported.
- If the installation fails, you can troubleshoot the error by looking in the \ManagementSuite\ldlogon\provisioning\config folder to see the installation script with the variables replaced. This strategy also applies to any time you modify a script, or use a script in the Inject script or Deploy image actions.
- The temporary directory used for provisioning is %systemdrive%/ldprovisioning.

Linux installation issues

Linux scripted installation is only supported using PXE boot.

When running a scripted install action for Linux, be aware that each version of Linux checks that you are using the correct CD when you begin an installation. Therefore, you will need a different initrd and linux (vmlinuz) for every version of Linux.

The best way to do this is
to copy the boot images from each CD to the PXE and rename them. You should copy them to \LANDesk\PXE\System\images\x86pc\undi\provlinux . For example, for Red Hat 4, rename the files to initrd.rh4as and vmlinuz.rh4as, and for Sles10, rename the files to initrd.sles10 and linux.sles10. Then, when you create a scripted install action, use the correct initrd.xxx and xxxlinux.xxx in the Scripted install template.

Linux install scripts support many key value pairs, such as:

Variable	Description
ldDNSDomain	The DNS domain
ldInstallServer	The install source server
ldInstallDir	The installation directory. For example, /storage/OS/linux/redhat/enterprise_4as/u3/i386/
ldNameserver1	DNS server 1

Variable	Description
ldNameserver2	DNS server 2

Provisioning template variables

Template variables allow for greater portability and customizability in templates. For example, a template may contain very specific file names to copy, paths to install to, or an IP address to export files from, but with user variables in place of these specific items, the template can address more situations or locales because you can simply swap out the variables in the XML code to replace those specific items.

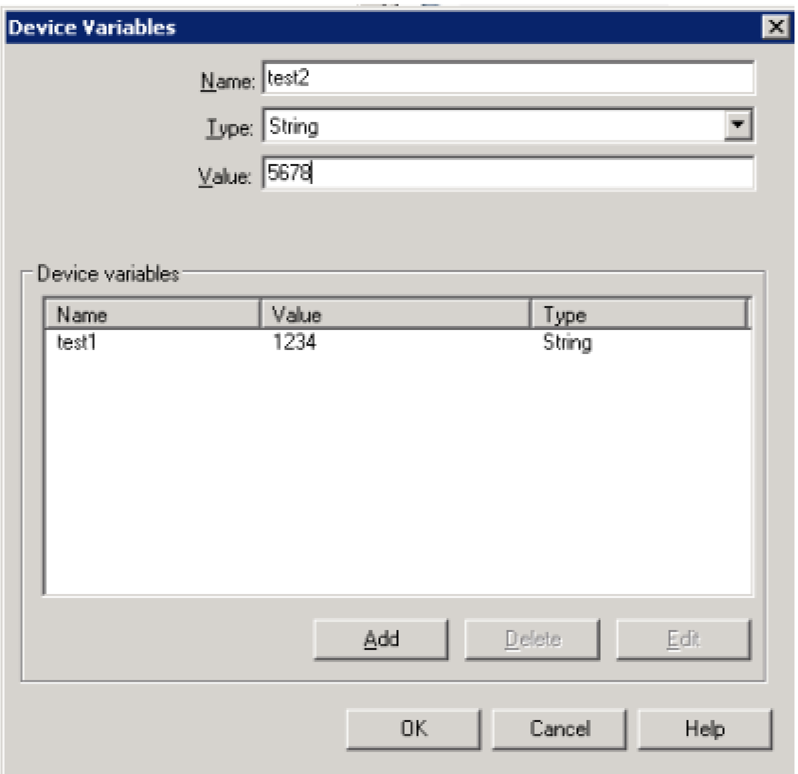
There are four types of variables. They are (in order of precedence)

- **Device:** Variables assigned to a specific device
- **Global:** Variables that are public (available) to all templates
- **Template:** Variables applying only to the assigned template
- **Action:** Variables applying only to a specific action

Variables are case-sensitive.

To define a device variable

1. In the **All devices** list, right-click a device and select **Manage variables**.



Name: test2
Type: String
Value: 5678

Device variables

Name	Value	Type
test1	1234	String

2. Type the name of the item (such as IP address) in the **Name** text box.
3. Type the value to be replaced in the **Value** text box.
4. Select the type.
    - **String:** Enter a string value

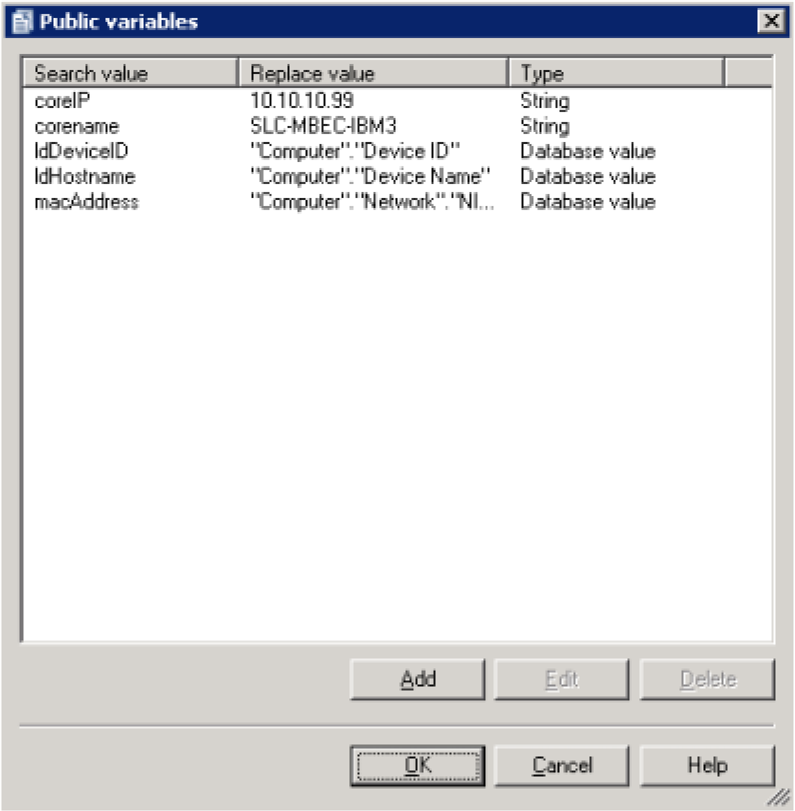
- **Database value:** Enter a database ID string, such as Computer.Network."NIC Address"
- **Sensitive data:** Enter the value to be encrypted in the database.

Use quotation marks around names with spaces. Most values from the Inventory database can be used.

5. Click **Save**.

To define a public (global) variable

1. Click **Tools > Distribution > OS Deployment**.
2. On the toolbar, click the **Public variables** button.



Search value	Replace value	Type
coreIP	10.10.10.99	String
corename	SLC-MBEC-IBM3	String
ldDeviceID	"Computer"."Device ID"	Database value
ldHostname	"Computer"."Device Name"	Database value
macAddress	"Computer"."Network"."NI...	Database value

3. To add a variable, click **Add**.
4. Type the variable you want to add in the **Search value** text box (for example, CoreIP).
5. Type the value you want to replace in the **Replacement value** text box (for example, if the search value is CoreIP, type the IP address you want to replace CoreIP with).
6. Select the type.
   - **String:** Enter a string value
   - **Database value:** Enter a database ID string, such as Computer.Network."NIC Address"
   - **Sensitive data:** Enter the value to be encrypted in the database.

Use quotation marks around names with spaces. Most values from the Inventory database can be used.

7. Click **OK**.

Creating unique identifiers for new devices

To create unique identifiers for new devices, use a Public variable that is based on the MAC address of the target device as shown below:

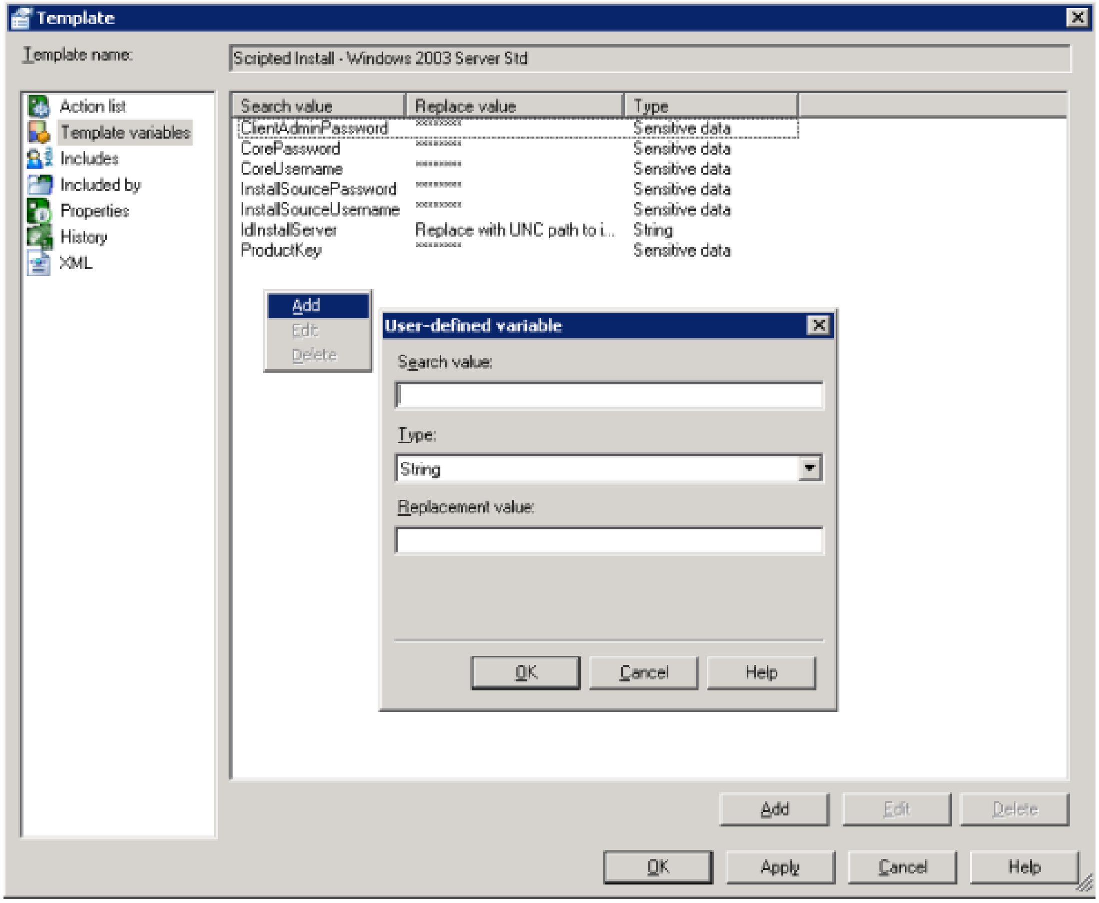
Variable (Database) =macAddress	Value = Computer.Network."NIC Address"
Variable (String) = Prefix	Value = UT (User value like location - Optional)
Variable (String) = Suffix	Value = XP (User value like OS - Optional)
Variable (String) = ComputerName	Value = %Prefix%%MACaddr%%Suffix%

Next, use the ComputerName variable in your sysprep.inf or unattend.txt files to uniquely identify the new device, as shown in the following code sample.

```
[UserData]
ProductKey=%ProductKey%
FullName="Engineering"
OrgName="LANDesk"
ComputerName=%ComputerName%
```

To define a template variable

1. Click **Tools > Distribution > OS Deployment**.
2. Under **Provisioning templates**, click **Public** or **My templates** to display a list of templates.
3. Double-click a template to open the Template view.
4. Click **Template variables**.



Template name: Scripted Install - Windows 2003 Server Std

Search value	Replace value	Type
ClientAdminPassword	********	Sensitive data
CorePassword	********	Sensitive data
CoreUsername	********	Sensitive data
InstallSourcePassword	********	Sensitive data
InstallSourceUsername	********	Sensitive data
IdInstallServer	Replace with UNC path to i...	String
ProductKey	********	Sensitive data

Search value:

Type: String

Replacement value:

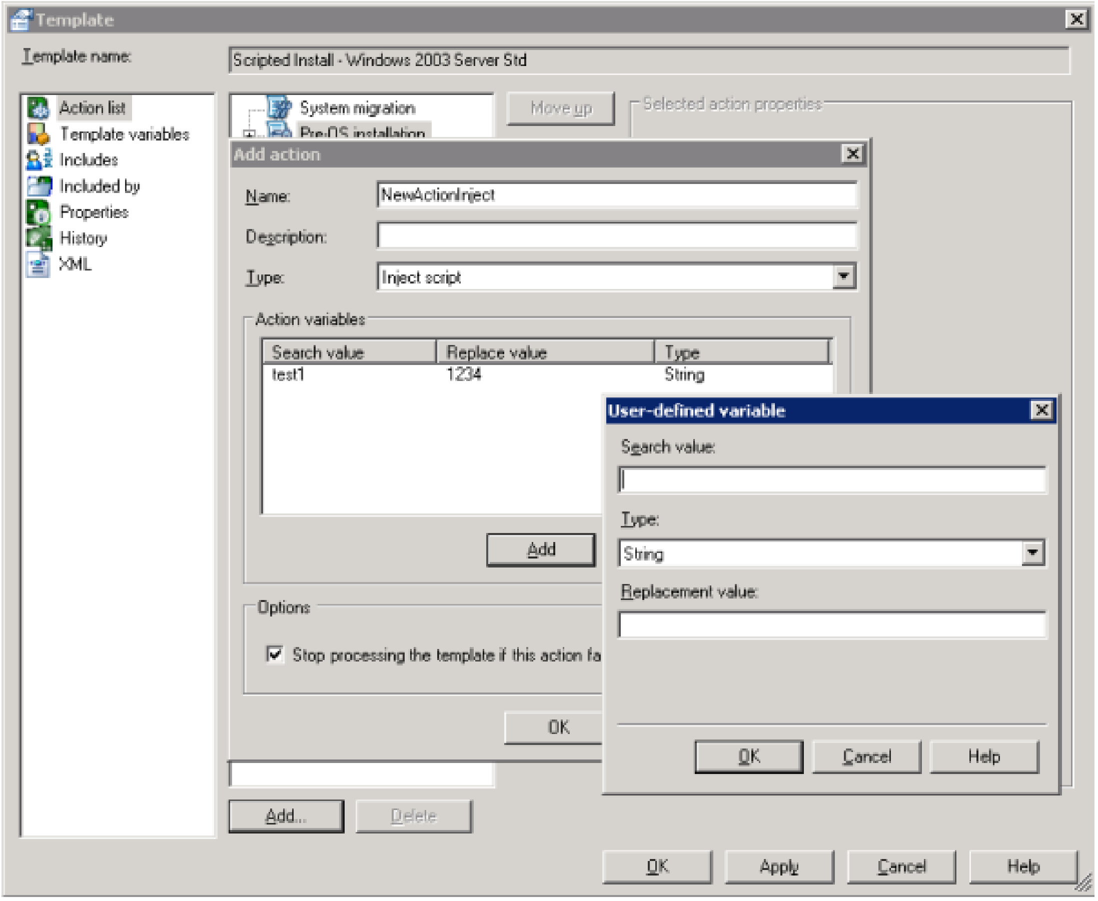
5. Click **Add**.
6. Type the variable you want to add in the **Search value** text box.
7. Type the value you want to replace in the **Replacement value** text box.
8. Select the type.
   - **String:** Enter a string value
   - **Database value:** Enter a database ID string, such as Computer.Network."NIC Address"
   - **Sensitive data:** Enter the value to be encrypted in the database.

Use quotation marks around names with spaces. Most values from the Inventory database can be used.

9. Click **OK**.

To define an action variable

1. Click **Tools > Distribution > OS Deployment**.
2. Right-click a template and click **Edit**.
3. Click **Action list**.
4. Click **Add** to create a new action. (If you want to modify an existing action, right-click the action and select **Properties**.)
5. To add an action variable, click **Add**.



Template name: Scripted Install - Windows 2003 Server Std

Name: NewActionInject

Description:

Type: Inject script

Action variables

Search value	Replace value	Type
test1	1234	String

☑ Stop processing the template if this action fa

Type: String

6. Type the variable you want to add in the **Search value** text box.
7. Type the value you want to replace in the **Replacement value** text box
8. Select the type.
   - **String:** Enter a string value
   - **Database value:** Enter a database ID string, such as Computer.Network."NIC address"
   - **Sensitive data:** Enter the value to be encrypted in the database.

   Use quotation marks around names with spaces. Most values from the Inventory database can be used.
9. Click **OK**.

Setting variables for all templates

Use the **Public variables** toolbar button to view and set global variables that apply to all provisioning templates. Such variables are used to customize template file names to copy, paths to install to, or IP addresses to export files from. User variables (variables that apply to only one template) take precedence over public variables.

To set public user-defined variables

1. Click **Tools > Distribution > OS Deployment**.
2. On the toolbar, click the **Public variables** button.
3. Click **Add**.

4. Type the value to be replaced in the **Search value** box (for example, CoreIP).
5. Type the new value in the **Replacement value** box. For example, if the Search value is CoreIP, type the IP address you want to replace CoreIP with.
6. Select the type.
   - **String:** Enter a string value
   - **Database value:** Enter a database ID string, such as Computer.Network."NIC Address"
   - **Sensitive data:** Enter the value to be encrypted in the database.

   Use quotation marks around names with spaces. Most values from the Inventory database can be used.
7. Click **OK**.

Database lookups are handled by adding a ldbnf: prefix to the Replace value. The database table and key pair can then be used to lookup a specific entry in the database. The ldDeviceID public variable that is configured by default is an example of how to add a database lookup variable.

Creating unique identifiers for new devices

To create unique identifiers for new devices, use a Public variable that is based on the MAC address of the target device as shown below:

Variable (Database) =macAddress	Value = Computer.Network."NIC Address"
Variable (String) = Prefix	Value = UT (User value like location - Optional)
Variable (String) = Suffix	Value = XP (User value like OS - Optional)
Variable (String) = ComputerName	Value = %Prefix%%MACaddr%%Suffix%

Next, use the ComputerName variable in your sysprep.inf or unattend.txt files to uniquely identify the new device, as shown in the following code sample:

```
[UserData]
ProductKey=%ProductKey%
FullName="Engineering"
OrgName="LANDesk"
ComputerName=%ComputerName%
```

Adding actions to a provisioning template

The following actions are described in this section:

- Capture image
- Configure agent
- Configure target OS
- Control service
- Copy file
- Create directory
- Delete file
- Deploy image
- Distribute software
- Download file
- Execute file
- Hardware-independent imaging
- Inject script
- Install service
- Join domain
- Map/unmap drive
- Partition
- Patch system
- Reboot/Shutdown
- Replace text
- Scripted install
- Uninstall service
- Unzip file
- Update registry
- Wait

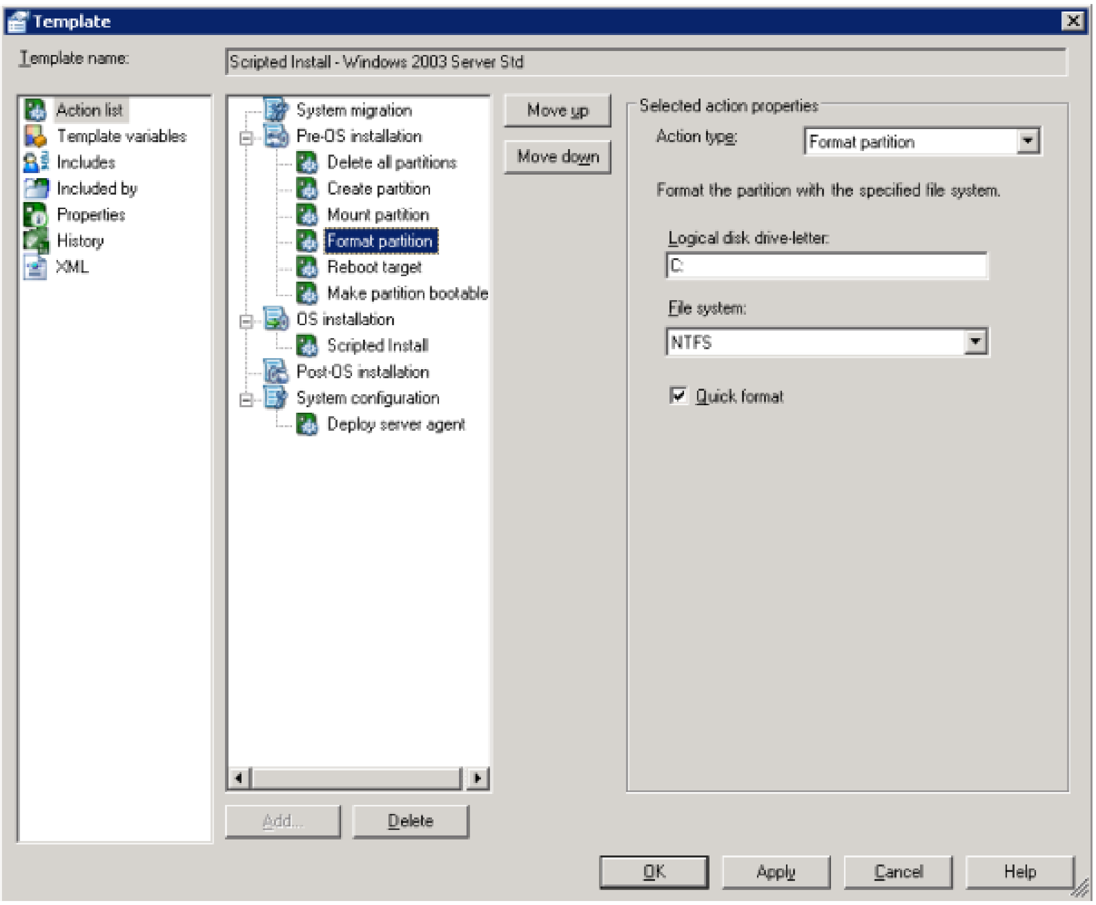
Use the **Add action** dialog to create new actions for provisioning templates, or to edit the actions of existing templates. Public templates are visible to all users. Templates in the My templates group are not visible to all users, and can
only be modified by the template creator or by users with administrative rights.

Actions are ordered in five sections. You can only select actions in each section that can apply to the section (for example, you can't select Software distribution as an action for the Pre-installation section). You can add any available action to any section, but be aware that some actions will break the template or may render your system unusable if completed in the improper steps.

The **Condense** toolbar button rewrites the current parent template to incorporate all included templates, so that all actions from the included templates become part of the parent template. This means that the parent template has no more dependencies. This is useful for exporting templates or making templates public. Once a template is condensed, it is a new template. You can't expand a condensed template.

To add actions to a template

1. Click **Tools > Distribution > OS Deployment**.
2. Under **Provisioning templates**, click **Public** or **My templates** to display templates.
3. Double-click a template.



Template name: Scripted Install - Windows 2003 Server Std

Action type: Format partition

Format the partition with the specified file system.

Logical disk drive-letter: C:

File system: NTFS

☑ Quick format

4. In the Template view, click **Action list**.
5. Click the section you want to add an action to. You can choose from these sections:
   - **System migration:** Features and components that need to be saved before modifying the system (or migrating a device to other hardware or virtual

machine). For example, this section can include an action to capture profile information when migrating to Windows Vista.

- **Pre OS install:** Actions that are performed when the device boots into a pre-installation environment (Linux PE, Windows PE). For example, on a server you would add RAID configuration in this section.
- **OS Install:** Actions that are performed in the pre-installation environment when the OS in installed (Linux PE, Windows PE).
- **Post OS Install:** Actions that are performed in the target operating system after it has been installed, such as running a patch management task.
- **System configuration:** Additional application installation/execution and system configuration in the installed OS. For example, add driver installation tasks in this section.

6. Click **Add**.
7. Type a specific name for the action in the **Name** text box.
8. Type a detailed description of the action in the **Description** text box.
9. Select an action type from the **Type** list. The type you select will determine what options you'll need to specify for the action. See below for more information on the specific action types.
10. If you want to add a variable that applies to this action only, click **Add** under **Action variables**. Type the name and value of the variable in the text boxes, and click **Save**.
11. Select **Stop processing the template if this action fails** if you want to define this action as essential to the provisioning task. If the action can be ignored, clear this check box.
12. When finished, click **OK**.

Action types

The table below displays the action types and where they fit into sections by default. You can add any action type to any section, but note that some actions inherently fit in certain sequences in provisioning, and if an action is executed outside its intended sequence, unintended consequences may occur.

Action name	System migration	Pre-OS installation	OS installation	Post-OS Installation	System configuration
Capture image			X		
Configure agent					X
Configure target OS				X	
Control service					X
Copy file	X	X	X	X	X
Create directory	X	X	X	X	X
Delete file	X	X	X	X	X
Deploy image			X		
Distribute software					X
Download file	X	X	X	X	X
Execute file	X	X	X	X	X
Inject script	X	X	X	X	X

Action name	System migration	Pre-OS installation	OS installation	Post-OS Installation	System configuration
Install service					X
Join domain					X
Map/Unmap drive	X	X	X	X	X
Partition		X	X	X	
Patch system					X
Reboot/Shutdown	X	X	X	X	X
Replace text	X	X	X	X	X
Scripted install			X		
Uninstall service					X
Unzip file	X	X	X	X	X
Update registry					X
Wait	X	X	X	X	X

Capture image (OS installation section only)

The Capture image action lets you capture an image at the time of OS installation, through the use of the imaging tool you specify. If the tool or the contents to be captured in an image are located on a share, you must place the Map drive action prior to the Capture image action in order to authenticate to the share.

- **Imaging tool:** The path to the location of the imaging tool.
- **Command-line parameters:** Enter any command-line parameters that will customize the way the image is captured.
- **Launch wizard:** Launches the imaging tool's wizard, which takes you through the process of capturing an image.

Note: To avoid the problem of the file system being locked open in WinPE, you must first Sysprep your image. In Windows Vista, follow the steps below.

1. Boot into Vista.
2. Change to the %SystemRoot%\System32\sysprep directory.
3. Run "sysprep /generalize /shutdown".
4. Boot to the PE and run ImageX.

The Windows XP/2003 steps don't require the /generalize and /shutdown switches for sysprep. The /factory switch should work on those operating systems.

Configure agent (System configuration section only)

The Configure agent action lets you select an agent configuration to install on the provisioned server. This action should be the first thing done after the reboot that follows the OS install actions. Configurations are added to the drop-down list as you create them in Agent configuration. This action can only be completed as part of a template that includes either the Scripted install or Deploy image actions, or if the client machine has already been configured with an agent.

- **Configuration name:** The name of the configuration. Select a configuration from the list.

- **Domain and user name:** Enter a domain and user name to log on to the core server on which the agent configuration resides.
- **Use variable for the password:** Select this check box to use a variable for the password. This variable is set in **Template variables** under **Sensitive data type**. (For details about variables, see Provisioning template variables.)
- **Password:** Enter the password to log on to the core server. Confirm the password in the **Confirm password** box.

When you install a new service pack, the agent configuration database IDs change. This means that the templates referencing those configurations become outdated. As a result, any provisioning history referencing those configurations will be unable to display the name of the configuration it once referenced, and any template referencing the old configurations will need to be updated before it will run correctly. The configuration name is not displayed in the History page, and if you try to re-schedule this template, it will fail on the Agent Configuration action because of this problem. To fix it, you must clone the template, open the cloned template, open the **Agent Configuration** action, and assign the configuration you want to use. Then the task will run successfully.

Configure target OS (post-OS installation section only)

This action inserts the provisioning agent (ldprovision) into an image so that the agent can be installed after reboot. It is required for continued provisioning after the new OS starts. For this action to work, the following conditions must be met:

1. The Windows system drive must be mounted.
2. The Windows file system must be either sysprepped or have an agent on the machine
3. Linux can't have any uncommon file systems (xfs, jfs, bobfs). The reiserfs and ext2/3 OSes are the only current valid supported OSes.
4. The Linux root system can't be on a software RAID controller, or be on a software RAID (md's). Real hardware RAID configurations are allowed, as long as the controller driver is recognized by the PE.

- **Insert unique ID:** To use the existing device ID, select this check box and enter the device ID in the text box.

This action should be performed as the last action in the post-OS installation section because this action includes a reboot operation.

Control service (System configuration section only)

The Control service action starts, stops, or restarts a specified service. The target OS must be Windows for this action.

- **Display name:** The name of the service.
- **Service control action:** The action to execute on the service. Can be Stop, Start, or Restart.

Copy file (all sections)

The Copy file action copies files to specific locations on the target server. Both the source and destination can be located on a share. If this is so, you must include a Map drive action prior to the Copy file action. The Copy file action can be recursive, meaning that all files/folders below the source path can be copied, maintaining their original structure. Wildcard characters are supported (such as *.exe or ld*.*).

- **Source path and file name:** The server/share path and file name location of the file to be copied. If you want to copy all files and folders below the source path, no file name is necessary.

- **Destination path and file name:** The server/share path and file name location to copy the file to.
- **Copy subdirectories:** Copies all subfolders and files below the source.

Create directory (all sections)

The Create directory action creates a directory in the specified location and can create the parent directory, if needed.

- **Path of the directory:** Type the path to the directory to be created.
- **Create parent directory if needed:** Select this check box to create the parent directory.

Delete file (all sections)

The Delete file action removes files in specific locations on the target server. The path can be located on a share. If this is so, you must include a Map drive action prior to the Delete file action. The Delete file action can be recursive, meaning that all files/folders below the source path can be deleted. Wildcard characters are supported (such as *.exe or ld*.*).

- **Path and file name:** Enter the full path and name of the file to be deleted.
- **Delete subdirectories:** Deletes all subfolders and files below the source.

Deploy image (OS installation section only)

This action deploys the selected image to the target server through the use of the imaging tool you specify. If the tool or the image to be deployed are located on a share, you must place the Map drive action prior to the Deploy image action in order to authenticate to the share.

You must manually reboot after deploying an image.

- **Imaging tool:** The path to the location of the imaging tool. If you select "Other" as imaging tool, then the entry for the path and filename of the image needs to contain the complete command line string for the imaging tool.
- **Command-line parameters:** Enter any command-line parameters that will customize the way the image is deployed.
- **Launch wizard:** Click this button to open a dialog box that lets you specify the type of image as well as the imaging application and command-line parameters.

Distribute software (System configuration section only)

This action distributes a software distribution package to the target. You can choose from any distribution package that you have saved in the Distribution packages tool. This action can only be completed after the agent configuration action, or after agents have been installed on the server.

- **Software distribution package:** Select the package you want to distribute.

Download file (all sections)

The Download file action downloads the selected file using anonymous user (anonymous HTTP login) to a destination you specify. If the files to be downloaded or the destination are located on a share, you must place the Map drive action prior to the Download file action in order to authenticate to the share.

- **Source path and file name:** The current server/share path and name of the file to be downloaded. Downloading files from a UNC path is not supported. If you want to download a file from a UNC path, you should use the Map drive action to map to the UNC path, then use the Copy file action.
- **Destination path and file name:** The location the file is to be downloaded to.

- **Use proxy server:** Enables the proxy server option to download a file. By default, this option is off. If you enable a proxy server, you must fill in the address and port fields below.
- **Address:** Identifies the IP address of your proxy server.
- **Port:** Identifies the port number of your proxy server.
- **Requires login:** Allows you to enter a username and password if the proxy server is credentialed instead of a transparent proxy server.
    - **Username:** Enter a valid username with authentication credentials to the proxy server.
    - **Use variable for the password:** Click this checkbox to use a variable for the password. This variable is set in **Template variables** under Sensitive data type. (For details about variables, see Provisioning template variables.)
    - **Password:** Enter the user's password.

Execute file (all sections)

The Execute file action executes the selected file on the targeted server, along with any command-line parameters or return codes you specify.

- **Target path and file name:** The location of the file you want to execute.
- **Command-line parameters:** Enter any command-line parameters that customize the way the file is executed.
- **Working directory:** The program will be executed with reference to this directory. Any supporting files of the program should reside in this directory. Command-line parameters start from this reference point.
- **Expected return value:** The value expected to be returned by the application upon execution. Can be Any, equals (=), less than (<), greater than (>), or Between. If the value is to be anything other than Any, enter the values to be expected in the boxes provided.
- **Insert:** Opens the **Environment variable** dialog box, where you can add an environment variable and its value.
    - **Name:** Type the name of the environment variable of the file. Use double percent signs to specify environment variables (for example, %%windir%%\system32\calc.exe).
    - **Value:**Enter the value of the variable.
- **Modify:** Modify the selected variable.
- **Remove:** Delete the selected variable.

Hardware-independent imaging (Post-OS installation only)

The Hardware-independent imaging action includes the hardware-independent imaging tool (hiiclient.exe) in the provisioning process. Hardware-independent imaging (HII) lets you create a single provisioning template or deployment script that can be deployed to multiple device models. A base image is installed on the device, and the HII tool then injects drivers that are specific to the device model.

This action is only included in the Post-OS installation section for templates based on the Windows preboot environment. After the OS is installed, but before the device reboots, the HII tool detects the device model and retrieves drivers for that model. The drivers are installed onto the device and their information is included in the registry. After a reboot, when the OS starts it configures the drivers.

- **Auto detect:** select this option to have the HII tool automatically select the manufacturer and model of the device you are provisioning, based on the strings in the device's BIOS. You should select this option if you want to use the provisioning template for devices from multiple manufacturers.

- **Select manufacturer and model:** select this option *only* if you will use the template on the same device model every time. Select a manufacturer from the list, then select a model from the list. The device drivers associated with this model are listed for your reference.

If you use this action, include a Reboot action after it in the Post-OS installation section.

For more information about hardware-independent imaging, see Hardware-independent imaging

Inject script (all sections)

This action injects a script into the target OS file system. You can inject sysprep.inf into the Deploy image action or unattend.txt into a Scripted install action. The Inject script action can only be done after the OS install action and before the first reboot that follows the OS install. The scripts that you can select are those in the **Install scripts** list that can be applied to the current template.

- **Script name:** The name of the script.
- **Target file name:** The location of the script you want to inject.

Install service (System configuration section only)

The target OS must be Windows for this action.

- **Display name:** The name you want to display to represent the service.
- **Service name:** The name of the service.
- **Service description**: A description of the service
- **Target path and file name:** The location of the service you want to install.
- **Command-line parameters:** Enter any command-line parameters that will customize the way the service is installed.
- **Service startup type:** Can be Manual, Automatic, or Disabled.
- **Interactive service:** Select this option to display on the desktop any user interface that can be used by the logged-in user when the service is started. This includes any message boxes the service may invoke during the installation process. If this check box is not selected, the template runs without user interaction, assuming the default selections of any service messages. If the service displays any messages during startup, it may cause the template to pause until the message dialog box is closed.

Join domain (System configuration section only)

Joins target device to a domain or workgroup.

- **Select operation type:** Can be Join domain or Join workgroup.
- **Domain name:** Enter the domain you want to join.
- **Workgroup name:** Enter the workgroup you want to join.
- **Username:** Type the username required to authenticate to the domain.
- **Use a variable for the password:** Click this checkbox to use a variable for the password. This variable is set in **Template variables** under Sensitive data type. (For details about variables, see Provisioning template variables.)
- **Password:** Enter the corresponding password to the username above. Confirm the password in the **Confirm password** text box.

Map/Unmap drive (all sections)

Map a drive or connect to a resource to access vital files to complete actions in a section or disconnect a drive or resource. Please note that some systems do not accept drive mappings below H:.

- **Map/Unmap a drive:** Select whether this action is to map a drive or disconnect a drive.
- **UNC path:** Enter the server and share you want to map to.
- **Drive letter/Mount point:** Enter the drive letter you to map the path above to. If you chose to unmap a drive, type the name of the drive you want to disconnect.
- **User name:** Enter the name of the user credential to log into the drive.
- **Use variable for the password:** Click this checkbox to use a variable for the password. This variable is set in **Template variables** under Sensitive data type. (For details about variables, see Provisioning template variables.)
- **Password:** Enter the corresponding password to the username above. Confirm the password in the **Confirm password** text box.

Partition (Pre-OS installation, OS installation, Post-OS installation sections only)

The Partition action lets you complete a variety of actions relating to partitions on the target server. Select partition actions from the **Action type** list. The actions are listed below.

The boot environment and target OS must be set prior to executing this action.

Create partition: Create a partition on the specified disk.

- **Disk:** Type the disk ID. On Windows, it is the disk number. On Linux, it is the name of the disk.
- **Partition type:** Select the partition type. This can be Primary, Extended, or Logical.
- **Size:** The size of the partition to be created, in MB.
- **Offset:** A number (in 8-bit byte format) indicating how far into the disk you want to create the partition.
- **Start:** The start position of the partition (cylinder number).
- **End:** The end position of the partition (cylinder number).

Remove partition: Delete a partition on the specified disk.

- **Remove from disk:** Type the disk ID. On Windows, it is the disk number. On Linux, it is the name of the disk.
- **Partition ID:** The partition number to be removed.

Remove all partitions: Delete all partitions on the disk.

- **Remove from disk:** Type the disk ID. On Windows, it is the disk number. On Linux, it is the name of the disk.

Format partition: Create a file system structure on a partition.

- **Logical disk drive letter:** The drive letter of the partition to be formatted (Windows).
- **Partition:** The device name of the partition to be formatted (Linux).
- **File system:** For Windows , the file systems are FAT, FAT32, and NTFS. For Linux, the file systems are ext2, ext3, reiserfs, and linux-swap.
- **Quick format:** Select this check box to perform a quick format on the partition.

Mount partition: Mount a partition.

- **Disk:** The disk number to be mounted (Windows).
- **Partition:** The device name of the partition (Linux).
- **Partition ID:** The partition number to be mounted (Windows).
- **File system:** For Linux, the file systems are ext2, ext3, and reiserfs.
- **File path to mount:** The name of the partition to be mounted. The mount point must exist (Linux).

- **Logical disk drive letter to create:** The drive letter of the partition to be mounted (Windows).

Unmount partition: Unmount a partition.

- **Disk:** The disk number to be unmounted.
- **Partition ID:** For Windows, the partition number to be unmounted. For Linux, the device name of the partition.
- **Logical disk drive letter to remove:** The drive letter of the partition to be unmounted (Windows).
- **Mount point to unmount:** The name of the partition to be unmounted (Linux). The mount point must exist.

Make bootable: Make a partition bootable.

- **Disk:** The disk number to be made bootable. For Windows, this is the disk number. For Linux, this is the name of the disk.
- **Partition ID:** The partition number to be made bootable.
- **Bootable:** Select the check box to make the partition bootable.
- **Windows 7 / Windows 2008 R2 with a separate system partition:** Select this check box to create separate OS partition.
- **OS partition ID:** The partition number for the separate OS partition.

Expand partition: Expands the last partition on the drive. Free space must be available.

- **Disk:** The disk number to be mounted.
- **Partition ID:** For Windows, the partition number to be mounted. For Linux, the device name of the partition.
- **Size:** The new size of the partition in MB (Windows). If you leave this blank, the partition will be expanded to fill the disk.
- **Start:** The start position of the partition (cylinder number).
- **End:** The end position of the partition (cylinder number).

Patch system (System configuration section only)

The Patch system action scans the target device for vulnerabilities and remediates them. This action can only run after a Configuration action that installs the Software updates agent is run.

- **Scan only:** Scans the machine for vulnerabilities.
- **Scan and remediate vulnerability:** Scans the machine for vulnerabilities, and fixes (where possible) the vulnerability.
- **Scan and remediate group:** Scans the machine for vulnerabilities and fixes the vulnerabilities included in the group.
- **Vulnerability ID:** A valid vulnerability ID from Patch Manager. If the ID is not valid, the action will fail.
- **Group ID:** A valid group ID from Patch Manager. If the ID is not valid, the action will fail. You can click the Group ID list button to select a vulnerability group that you have created.

The core vulnerability definitions should be updated prior to executing this action. All patches to be remediated must be downloaded on the core before executing either remediation option in this action.

Reboot/Shutdown (all sections)

Reboot or shut down the server. A reboot must immediately follow the OS install action. Upon reboot, the provisioning agent restarts the template to continue the progression of provisioning tasks. Use the Reboot action to move from System migration section to OS sections or OS sections to System configuration section. Multiple reboots are supported.

- **Reboot:** Shut down the server and restart it.
- **Shut down:** Shut down the server at the end of the provisioning task and leave it powered down (off). You must make sure that this action is the last action in the template, or additional actions will not be completed.

Replace text (all sections)

Replace text in an existing file.

- **Source path and filename:** The path and filename of the file to have text replaced.
- **Find what:** The existing text that is to be replaced.
- **Replace with:** The text that is to take the place of the existing text.
- **Replace first occurrence, Replace all occurrences:** Replace the new text either the first time it is encountered or every time it is encountered.

Scripted install (OS installation section only)

Install an operating system through the use of custom scripts. There can only be one action that installs an OS.

Windows

- **UNC path to installation source:** This is a path where the executable file is found within the installation source. This must have been mounted within the Pre-OS Install section (Map drive action).
- **Domain and user name:** Enter a domain and user name to log on to the device on which the executable file resides.
- **Use variable for the password:** Select this check box to use a variable for the password. This variable is set in **Template variables** under **Sensitive data type**. (For details about variables, see Provisioning template variables.)
- **Password:** Enter the password to log on to the device. Confirm the password in the **Confirm password** box.
- **Additional parameters passed to setup:** Parameters to be passed to the install file when it is executed. For Winnt32, the Provisioning handler automatically fills in the unattend (/unattend) and the source arguments (/s). These are generated from the path that was given in the Winnt32 path, and from the script that has been selected.
- **Installation script:** The unattend file used when installing the operating system.

Linux

- **Location of the initrd:** The location of the Initial RAMdisk file. The default is /x86pc/undi/provlinux/initrd.img.
- **Kernel location:** The location of the Linux kernel.
- **Additional parameters passed on boot:** Parameters to be passed to initrd when it is executed.
- **Installation script:** The unattend file used when installing the operating system.

Uninstall service (System configuration section only)

Uninstall a service on the target device.

- **Service name:** The name of the service to be uninstalled.

Unzip file (all sections)

Unzip the contents of a package to a predetermined location. This action can restore original structure.

- **Source path and file name:** The path and file name of the package to be unzipped.
- **Target path:** The location where the package is to be unzipped. If this is an existing directory/folder, any duplicate filenames will be overwritten.
- **Create target directory if it doesn't already exist:** If the target does not exist, select this check box to create it automatically.

Update registry (System configuration section only)

This action adds or removes keys or values to the registry, or imports a registry (.REG) file. Editing the registry incorrectly may damage your system, potentially rendering it inoperable. Before making changes to the registry, you should back up any valued data on your computer.

Select an operation from the **Registry operation** drop-down list.

- **Delete key:** Remove a registry key's expected folder and path.
- **Delete value:** Remove the expected value of the key.
- **Create key:** Create a folder on the left side of the Registry Editor.
- **Import value:** Import a registry file.
- **Set value:** Create a value. The data entered is interpreted as a value determined by the **Type** list.
- **Key:** Enter the key to create or delete.
- **Value:** Enter the value to create or delete.
- **Datum:** Enter data to be saved in a value.
- **Type:** Select a data type. This can be String Value, Expanded string value, Binary Value, DWord Value, or Multi-String Value.
- **Import file contents:** Type a description of the registry file to be imported.
- **Import data from registry file:** Type the full path to the registry file, or click **Browse** to find it, then click **Import file**.

Wait (all sections)

Pause the template execution for a specified time or until a required file has been created.

- **Number of seconds to wait:** Pause the template for a specified number of seconds.
- **Wait for file to exist:** Pause the action until the specified path and file exists. This is useful when an action requires an application to install a file. When the file is created, you can trigger execution of the next action based on the existence of the file.
- **Maximum number of seconds to wait:** Waits for the specified time (in seconds). If the time passes and the file never appears, the template continues with the next action.

Included templates

The Template view displays the templates that are included in the current template (included templates are also known as child templates). You can view included templates and add templates to the current template. Once a template is included with another template, it is part of the parent template. If you change the included template in its original stand-alone form, it is changed in the parent template package, too.

To add a template to the current template

1. Click **Tools > Distribution > OS Deployment**.
2. Under **Provisioning templates**, click **Public** or **My templates** to display templates.
3. Double-click a template.
4. In the Template view, click **Includes**.
5. Click the **Include** button.
6. Using the tree structure, navigate to the template you want to include, select it, and click **OK**.
   The **Template information** section displays details about the template that may be useful in deciding whether to include the template.

To delete a template from the list of included templates, click **Remove** to remove the selected template.

To include a template, its boot environment and target OS must match the template setting of the parent template. Not Applicable is treated as a wildcard.

To view other templates that include the current template, see "Parent templates" on page 252.

Parent templates

The **Included by** view displays a list of other templates that include the current template (templates including the current template are also known as parent templates).

To view the list of templates that include the current template

1. Click **Tools > Distribution > OS Deployment**.
2. Under **Provisioning templates**, click **Public** or **My templates** to display templates.
3. Double-click a template.
4. Click **Included by**.

To include other templates in the current templates, see "Included templates" on page 251.

Template properties

Use the template **Properties** view to display the template information current to the time the template was created.

To view template properties

1. Click **Tools > Distribution > OS Deployment**.
2. Under Provisioning templates, click **Public** or **My templates** or one of their subgroups.
3. Double-click a template, and click **Properties**. The following information is displayed:
   - **Template name:** The name of the template.
   - **Description:** The description of the template.
   - **Owner name:** The core server and login name of the person who has rights to run the template. If the template is in a Public folder, this name is Public User.
   - **Boot environment:** The preboot environment the template boots into (Windows PE or Linux PE).
   - **Target OS:** The target operating system of the template (for example: Windows, Windows XP, Windows 2000, Linux, SuSE, or Red Hat).

This view of a template's properties is not editable. You can also view and change some properties for a template by right-clicking it in a list of templates and selecting **Properties**.

Templates in the My templates folder are visible to others but can only be edited by the template's creator or users with Administrator rights.

Provisioning history

The provisioning history option lets you view the history of a provisioning template. You can check on the status of a particular task, determine how a particular server was provisioned, or find out which servers were provisioned with a particular template. When a system is provisioned, all the actions are recorded in the provisioning history.

If you want to put a system back into a known state, you can replay the template that lets you return to that known state. If you want to replay a template, keep in mind that some actions are external to provisioning. Save any software distribution packages, agent configurations, and programs that you download and execute in conjunction with a template. Otherwise you won’t be able to replay them.

To view a template's provisioning history

1. Click **Tools > Distribution > OS Deployment**.
2. Under **Provisioning templates**, click the **Public** or **My templates** folders to display templates.
3. Double-click a template.
4. Click **History**.
5. Click a name in the **Task name** column and click **Select** to view details about that task.

If the template has never been executed, there will be no history.

To view the provisioning history by task

1. Click **Tools > Distribution > Scheduled tasks**.
2. Under **My tasks** or **Public tasks**, click the task name.
3. Click a category under the task (All devices, Active, Pending, Successful, or Failed). Targeted devices are listed in these categories depending on the status of the provisioning task on the device.
4. Right-click a targeted device and select **Provisioning history**.
5. Click **Properties** to view the provisioning template properties.
6. Expand a template section and click an action to view details of the action's deployment.

To view the provisioning history by device

1. In the network view, click **My devices** or **Public devices** and find the device.
2. Right-click the device and select **Provisioning history**.
3. Click a task name and click **Select** to view details of the provisioning task.
4. Click **Properties** to view the provisioning template properties.
5. Expand a template section and click an action to view details of the action's deployment.

To get the current status of a template that is in the process of executing, click the **Refresh** button to update the history status.

Creating provisioning groups

You can create groups of provisioning templates for use in provisioning tasks. You can use provisioning groups to organize your templates in ways to suit your needs. For example, you could create groups based on specific vendors, and additional subgroups based on server models. Later, if you want to modify one of the templates in the group, you only need to remove the template from the group and re-add it to the group in its modified state. You can create subgroups up to six layers deep.

To create a group of templates

1. Click **Tools > Distribution > OS Deployment**.
2. Select **Public** or **My templates**.
3. Click the **Create a template group** button on the toolbar.
4. Type a name for the group in the **Group name** text box.
5. Type a description in the **Group description** text box.
6. Click **OK**.

To delete a group

1. Select a group, and click the **Delete** button on the toolbar.
2. Click **Yes**, and then confirm that you want to delete the group.

A group can be deleted even if it is not empty. Make sure than any subgroups or templates in the group can be deleted before you confirm the deletion.

Provisioning troubleshooting

Problems booting into WinPE

In Windows Vista, if the machine is configured to go into hibernation, it will have difficulty in booting into WinPE. If HIBERFIL.SYS exists, WinPE will not boot.

To work around this, make sure that hibernation is turned off.

The location on the core the provisioning templates are downloaded to

The provisioning templates on the Content server are downloaded to the \Program Files\LANDesk\ManagementSuite\cache folder. Within that folder, additional folders are used to organize the templates.

Setting the level of logged provisioning status messages

The file LogLevel.ini controls the logging level used for various components in provisioning. It can be modified to fit the needs of your environment. You can set the level of logging to compile messages of a certain level and below. These levels are (in order from lowest to highest) ERROR, WARNING, INFO, VERBOSE, and DEBUG. The levels are additive, so a logging level of INFO will also display all ERROR and WARNING message. DEBUG displays all messages. Additional information can be found in the commented text of LogLevel.ini, which is located in the \Program Files\LANDesk\ManagementSuite\log\provisioning folder.

How do I lock and unlock templates?

Any time you use a template not marked Public, an instance of that template is locked. The instance can't be deleted, but it can be hidden. You can't unlock an instance of a template. You must open the original template.

Troubleshooting – core

Template execution messages are stored in “provisioning.log” located in the \Program Files\LANDesk\ManagementSuite\ldlogon\provisioning folder. You can view PXE representative deployment and prov_schedule log files in \Program Files\LANDesk\ManagementSuite\log folder

Troubleshooting – target

The tables below describes some useful files for troubleshooting.

WinPE

Folder\File	Description of file content
\ldprovision\launch.log	Provisioning loading status
\provision folder\ldprovision.log	Error messages and XML content
\ldprovision\output.txt	Application error messages only if the application hangs

LinuxPE

Use Alt+F2 to toggle to a terminal window.

Directory/File	Description of file content
var/log/messages	Errors loading LinuxPE
var/log/taskmaster.log	Errors load provisioning
var/log/provisioning.log	Template errors and XML content

Windows target device

Folder/File	Description of file content
WinDir\Temp\ldProvision.log	Error messages and XML content
WinDir\Temp\run##.tmp	Template execution messages

Linux target device

Directory\File	Description of file content
/tmp/ldProvision.log	Error messages and XML content

Troubleshooting – PE manual execution

Load new console into PE and change to ldprovision folder x:\ldprovision – PXE, z:\ldprovision – Boot Media

Launch provisioning by executing ldprovision.exe

ldProvision command-line options:

Option	Explanation
-c	core name or IP

Option	Explanation
-d	debug
-f	task XML file name
-h	help
-m	mode 1-3 (1=default)
-s	run as daemon (Linux only)
-t	download directory
-v	version V # (1-255) Verbose logging

Example: `ldprovision –c mycore –t x:\ldclient –V 255`

OS manual execution

Windows

Using target that has ld agent installed, map a drive to or copy contents of \Program Files\LANDesk\ManagementSuite\ldlogon\provisioning\windows from core to local folder. Execute ldprovision as shown in PE manual execution above. Note that the log files are placed in windir/temp.

Linux

Using target that has ld agent installed, mount point to or copy contents of \Program Files\LANDesk\ManagementSuite\ldlogon\provisioning\linux from core to local folder. Execute ldprovision as shown in PE manual execution above. Note that the log files are placed in var/log.

Tips on provisioning large numbers of devices

If you need to provision or re-provision a large (100+) number of devices, you may encounter slowdowns or timeouts in the downloading of the PE image from the PXE Representative, particularly the WinPE image. The actual OS imaging is not affected by provisioning, but is limited by the network capacity or ability to get the image file from depository server to client. For example, downloading a WinPE image to 14 clients from a single PXE Representative may require approximately 45 seconds. Using 14 clients, 0 to 3 clients would time out before they received an acknowledgement from the PXE Representative. These clients would then precede to the local boot. If the device was bare metal (No OS) they would reboot and PXE boot to the PXE Rep. Multicast clients would not remove the PXE Rep booting/downloading bottleneck.

If this occurs, try the following:

- PXE boot groups of up to 10 devices at a time. If you want to PXE boot more than 10 clients at a time, you should increase the PXE boot retries/timeout.
- Stagger the device groups at three-plus minute intervals. This will allow the PE image to be downloaded and the majority of the OS imaging to take place.
- If you need to provision/image devices at a faster rate, add additional PXE Representatives as needed.

Even though the LinuxPE image is a third the size of WinPE, the PXE Representative still can't handle more than 10 simultaneous boot requests. If you stagger them by a couple of seconds they should all book as expected, but if you start them all at once, some clients will not PXE boot. Generally the LinuxPE image will download twice as fast as WinPE.

Profile migration

The Management Suite profile migration feature adds device profile migration capabilities to your network. Profile migration is used with other OS deployment and provisioning features to streamline new device provisioning and existing device migration, without requiring additional end-user or IT interaction once the process starts.

For information on installing the OS deployment and profile migration component on your core server, and configuring your OS deployment and profile migration environment, refer to "OS deployment" on page 201

Read this chapter to learn about:

- "Profile migration overview" on page 257
- "Creating migration scripts with the OS deployment wizard " on page 259
- "Defining profile content" on page 263
- "Creating a command file" on page 263
- "Migrating user profiles" on page 264
- "Migrating desktop settings " on page 264
- "Migrating application settings and associated files" on page 266
- "Migrating printer settings" on page 267
- "Migrating network settings" on page 267
- "Migrating files and folders" on page 268

Profile migration overview

Profile migration complements OS deployment by offering a complete user migration solution. With profile migration, you can preserve customized user profiles, desktops, settings for applications, network connections, printers, files, and folders, as you implement upgrade or migration projects. Profile migration supports in-place migrations of individual devices as well as remote, large-scale migrations of multiple devices across your network.

The User Migration Assistant (UMA) tool is used for migration tasks: it runs on each managed device to capture profiles and restore them on a new OS. When you schedule an OS deployment script, the UMA is installed on the managed device after the first time the "Capture profile" or "Restore profile" task is run on the device. You can also run the UMA as a standalone tool on managed devices after it has been installed (see "Profile migration" on page).

Profile migration is a two-part process:

1. *Capturing* a source device's unique profile, consisting of user accounts, desktop (PC) and application settings, network settings, printers, and data files and folders.
2. *Restoring* the profile to a target device.

For step-by-step descriptions of the profile capture and restore procedures, see "Creating migration scripts with the OS deployment wizard " on page 259.

For page-by-page descriptions of the wizard's interface, see "OS deployment and Profile migration wizard help" on page 638.

How profile migration works

Using profile migration, you can create separate capture and restore scripts with the OS Deployment/Migration Tasks wizard. The script can then be scheduled to run remotely on one or multiple target devices on your network. The actual process of capturing and restoring profiles is done by the User Migration Assistant (UMA), an executable that is silently installed on the managed device as the script is running.

What can be captured depends on the User Migration Assistant command file source, an XML file with specific settings related to profile migration. Each item in the file can be turned on or off by setting it to True or False. For example, the setting `<mouse>true</mouse>` means that the user's mouse setting will be captured. A sample command file is provided for your reference, located in the <core server>\ldlogon\uma\commandxml folder.

For more information about the types of data that can be migrated, see "Defining profile content" on page 263.

Prerequisites

To do a profile migration, devices must meet the following prerequisites:

- Devices must be scanned in the core database.
- Devices must have the standard LANDesk agent, which includes the inventory scanner, local scheduler, and software distribution agents. (Profile migration uses the software distribution agent to distribute files.)

Migration paths

Profile migration supports migrating across the following Windows operating system versions:

- Windows 2000 Professional
- Windows XP Home
- Windows XP Tablet PC Edition 2005
- Windows XP Professional
- Windows Vista(R) Home Basic 32-bit
- Windows Vista Home Premium 32-bit
- Windows Vista Business 32-bit
- Windows Vista Ultimate 32-bit
- Windows Vista Home Basic 64-bit
- Windows Vista Home Premium 64-bit
- Windows Vista Business 64-bit
- Windows Vista Ultimate 64-bit
- Windows 7 Home Premium 32-bit
- Windows 7 Professional 32-bit
- Windows 7 Ultimate 32-bit
- Windows 7 Home Premium 64-bit
- Windows 7 Professional 64-bit
- Windows 7 Ultimate 64-bit

Work environments from a 32-bit OS can be migrated to a 64-bit OS, but you can't migrate from a 64-bit OS to a 32-bit OS.

The source and target devices must run the same language version of Windows.

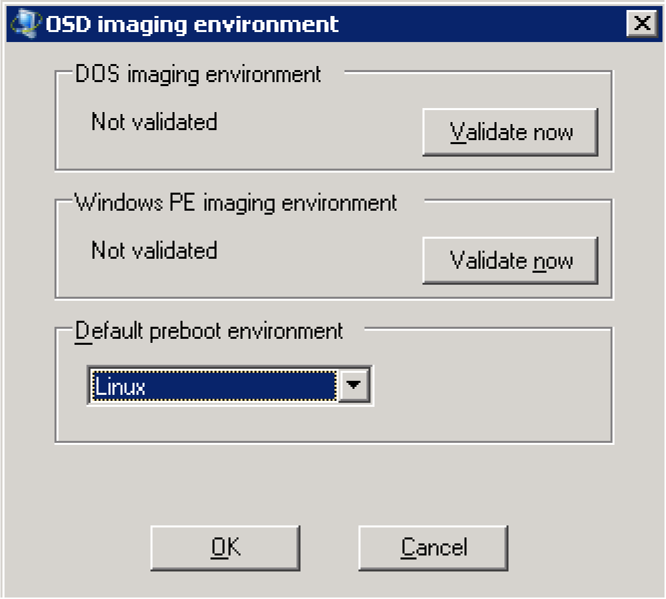
For a detailed list of allowable migration scenarios, see "Using profile migration in LANDesk Management Suite 9," which can be downloaded from the LANDesk support community at community.landesk.com.

Creating migration scripts with the OS deployment wizard

The steps below outline the basic procedures for capturing and restoring a device's profile using the OS deployment wizard. For more information about each of these steps, click the **Help** button located on each page of the script wizard.

To create a profile capture script

1. Click **Tools > Distribution > OS Deployment**.
2. If you have not yet done so, validate your operating system preboot environment license. Click the **Validate licenses** button on the toolbar and click **Validate now** for DOS or Windows environments. (For more information about validating licenses, see "OS image guidelines" on page 203


OSD imaging environment

DOS imaging environment
Not validated

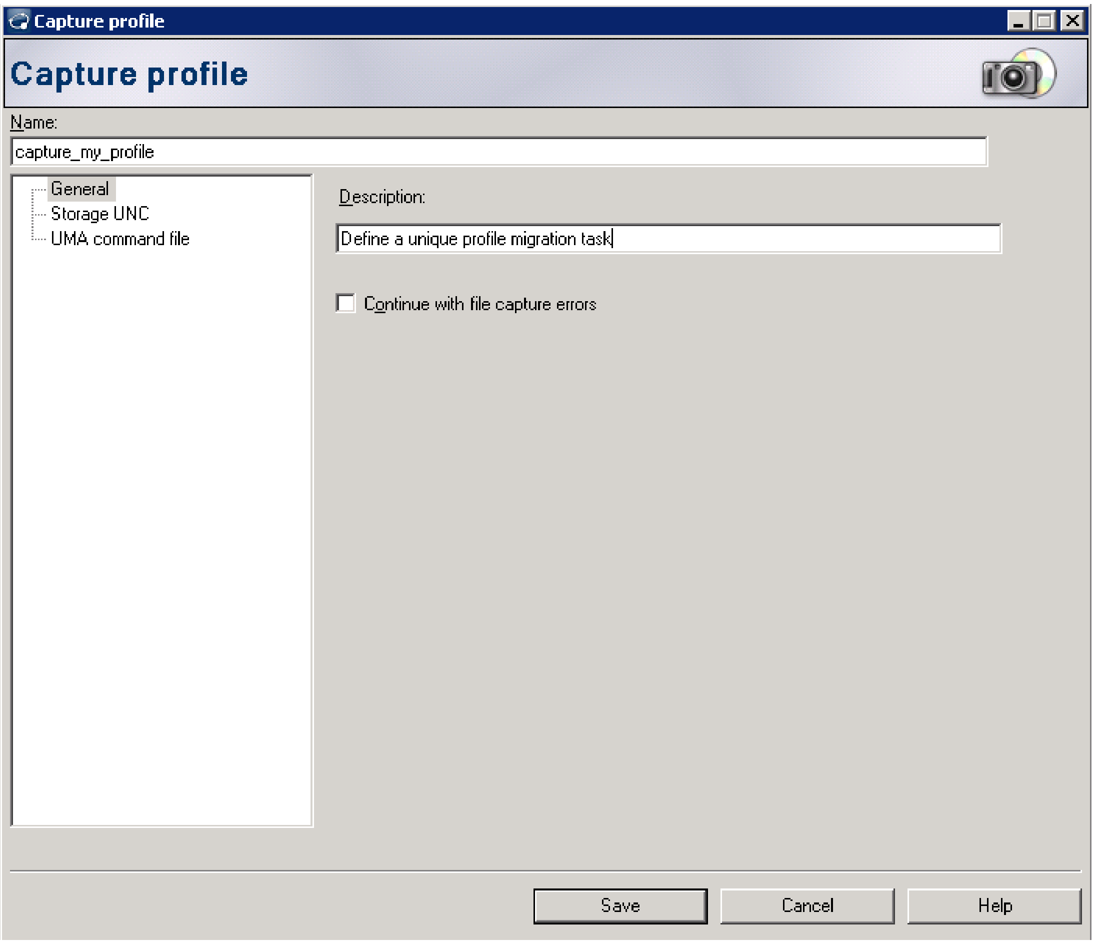
Windows PE imaging environment
Not validated

Default preboot environment: Linux

3. In the **Operating system deployment** window, right-click **My OSD Group members** or **All OSD Scripts** and then select the PE configuration type you want to create. (Only Windows and DOS PE configurations can capture profiles.)

   Use **My OSD Group members** to create a private profile migration script; use **All OSD Scripts** to create a public profile migration script.

4. Select **Capture profile**, and then click **OK**.
5. On the **General** page, enter a description for the script. If you want the profile capture to continue even when there are errors, select the **Continue with file capture errors** check box. (If you select this, the file errors are recorded in the log file.)

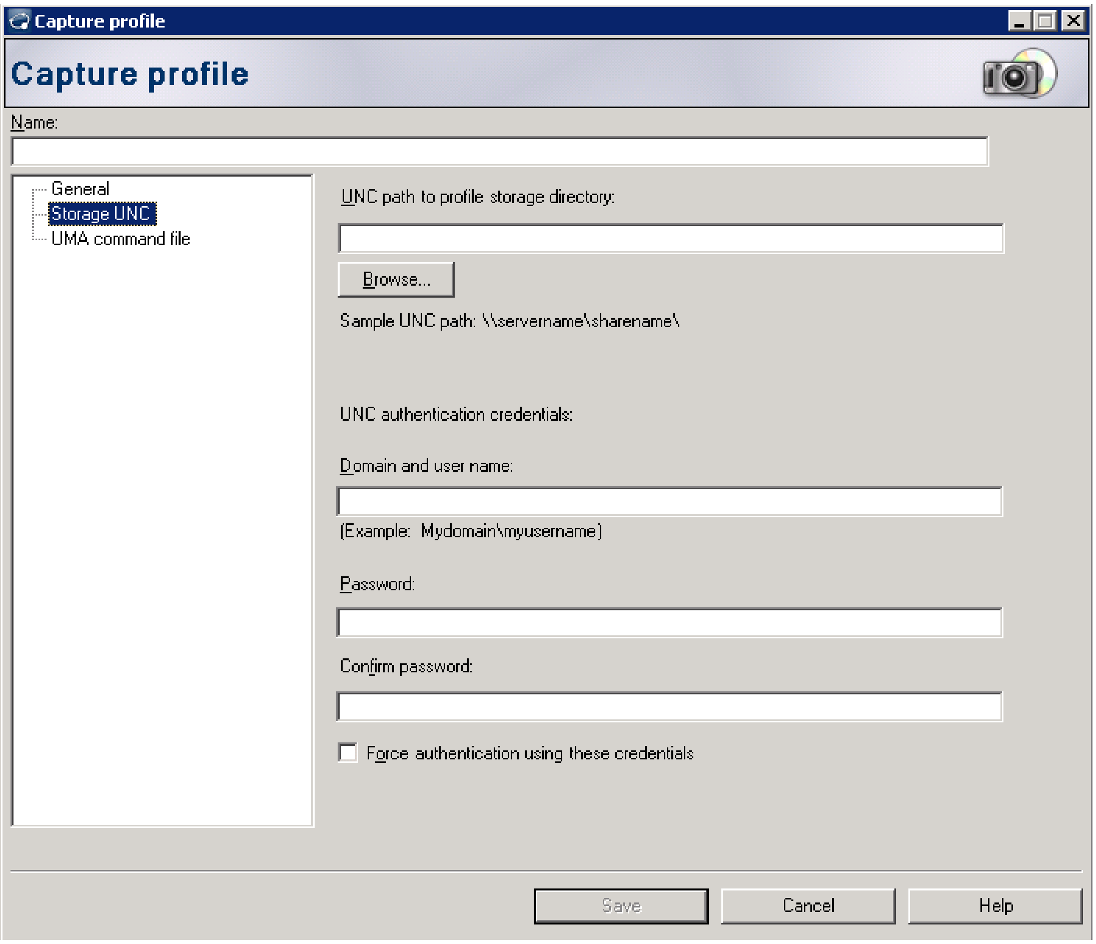


Name: capture_my_profile

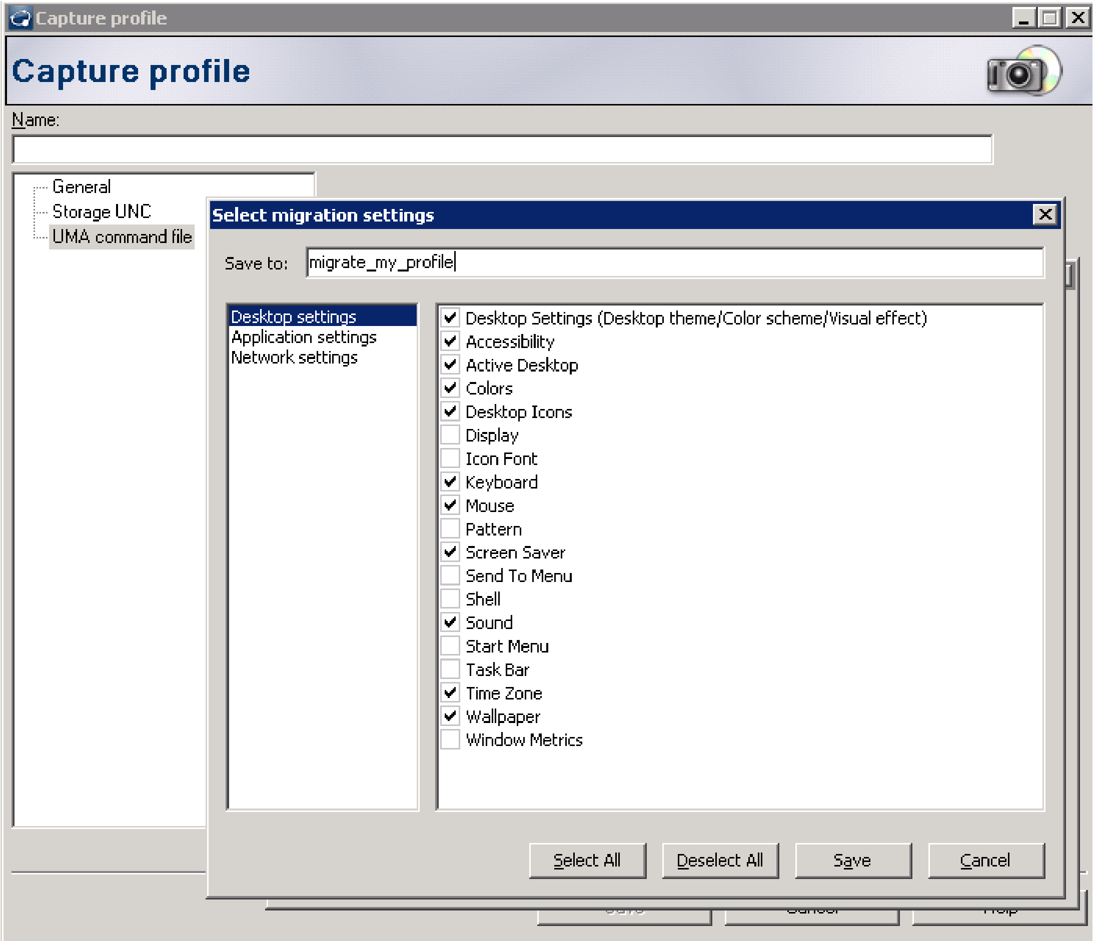
Description: Define a unique profile migration task

□ Continue with file capture errors

6. On the **Storage UNC** page, enter a UNC path and authentication credentials for the location where you want to store the profile data. Specify a filename to use for storing the profile data.


Capture profile
Capture profile
Name:
General
Storage UNC
UMA command file
UNC path to profile storage directory:
Browse...
Sample UNC path: \\servername\sharename\
UNC authentication credentials:
Domain and user name:
(Example: Mydomain\myusername)
Password:
Confirm password:
□ Force authentication using these credentials
Save
Cancel
Help

7. On the **UMA command file** page, specify the name and location of the command file to be used for profile migration. Click **Edit** to create a new command file or edit an existing command file.
   - In the **Migration settings** dialog box, select an existing command file and click **Edit**, or click **New** to create a new command file.
   - Click **Desktop settings** and select the check box for each item you want to capture in the migration.
   - Click **Application settings** and select the check box for each application that you want to capture in the migration.
   - Click **Network settings** and select the check box for each network, drive, and computer setting you want to capture in the migration.
   - Click **Save** to save the settings to the command file you have specified.



Save to: migrate_my_profile

- ☑ Desktop Settings (Desktop theme/Color scheme/Visual effect)
- ☑ Accessibility
- ☑ Active Desktop
- ☑ Colors
- ☑ Desktop Icons
- ☐ Display
- ☐ Icon Font
- ☑ Keyboard
- ☑ Mouse
- ☐ Pattern
- ☑ Screen Saver
- ☐ Send To Menu
- ☐ Shell
- ☑ Sound
- ☐ Start Menu
- ☐ Task Bar
- ☑ Time Zone
- ☑ Wallpaper
- ☐ Window Metrics

8. Click **Save** to create the profile capture script.

To run a profile capture script

1. Click **Tools > Distribution > OS Deployment**.
2. In the **All OSD scripts** folder, select the capture script.
3. Click the **Schedule** button on the toolbar.
4. Using the **Scheduled tasks** tool, schedule the script to run on one or more target devices on your network.

Storing profile data for multiple devices (and multiple users)

Profile data is stored in System Migration Assistant (.sma) files in a directory structure located under the UNC path you specify. If you run a profile capture script on multiple devices, each device's profile data is stored in a separate directory named after its unique Windows computer name.

Likewise, if multiple users are discovered and captured on the same source device, each user's profile data is stored in a separate subdirectory of the device's directory, and is named with the user login name. In other words, every migrated device has its own profile storage directory and contains a subdirectory for every captured user account on that device.

To create a profile restore script

1. Click **Tools > Distribution > OS Deployment**..

2. In the **Operating system deployment** window, right-click **All OSD Scripts** and then select the PE configuration type you want to create. Only Windows and DOS PE configurations can restore profiles.
3. Select **Restore profile**, and then click **OK**.
4. On the **General** page, enter a name and a description for the script.
5. On the **Profile storage** page, enter a UNC path and authentication credentials for the location where the profile data is stored.
6. Click **Save** to create the profile restore script.

To run a profile restore script

1. Click **Tools > Distribution > OS Deployment**.
2. In the **All OSD scripts** folder, select the restore script.
3. Click the **Schedule** button on the toolbar.
4. Using the **Scheduled tasks** tool, schedule the script to run on one or more target devices on your network.

Profile migration log file

Profile migration creates a log file for every script you run. Log files are saved on the core server in the <core server>\ldlog folder. Log files are named `CJ-OSD-`*scriptname*`-`*date*`-`*time*`.log`

Defining profile content

Profile migration allows you to migrate the following content:

- User profiles
- Desktop settings
- Application settings and associated files
- Printer settings
- Network settings
- Files and folders

User accounts are migrated by default. Settings and files are migrated according to a user-defined rules in the UMA command file, described in the following sections.

You don't need to edit the UMA command file directly; the OS deployment Capture Profile wizard gives you the option to select settings as you are creating a profile capture script. The wizard lets you change settings for the desktop, applications, and network. However, if you want to change other settings that are not in the wizard, the following sections will help you modify the UMA command file.

Creating a command file

The User Migration Assistant (UMA) stores information about the profile content you want to migrate in an XML file called a *command file*. To specify what options are stored when you capture a profile, you edit the command file.

The easiest way to create a new command file is to create or edit one when you create a profile capture script in the Operating system deployment tool (see "To create a profile capture script" on page 259). The command file you create here will have the default settings plus any changes you have made to the desktop, application, and network settings that are listed for you.

If you want to further customize the many settings in the command file, you can create a new XML file with the settings you want. A sample command file (sample_command_file.xml) is found on the core server in the <core server>\ldlogon\uma\commandxml folder. Copy this example file to create custom files for different profile migration tasks.

The following sections contain specific help for customizing a command file by editing the XML document.

If you delete a command file from the core server, any migration script referencing that command file will not run properly. You should also delete any scripts that reference the file, or edit them to reference another command file.

Migrating user profiles

In a scripted profile migration, all discovered local and domain user accounts on the source devices are captured by default, *except* for the All Users and Default User accounts.

All captured user accounts will be restored to the target devices. A user account that does not already exist on the target device will be created as a new local user account and its settings migrated. Before restoring user accounts, you can enter a default password for these new local user accounts. If a duplicate user account does already exist on the target device, the captured (source) user account's settings will be migrated to the existing user account, but the user's current password is preserved and should be used to log in.

To specify which user profiles to migrate

In the UMA command file, include user names to migrate in the `<IncUsers>` section. You can include all users with the variable `$(all)` or specify individual names enclosed in `<UserName></UserName>` tags. A code sample is shown below.

```
<IncUsers>
<UserName>$(all)</UserName>
</IncUsers>
```

To specify which user profiles to exclude from migration

In the UMA command file, exclude user names to migrate in the `<ExcUsers>` section. Specify individual names enclosed in `<UserName></UserName>` tags. A code sample is shown below.

```
<ExcUsers>
<UserName>ASPNET</UserName>
</ExcUsers>
```

Migrating desktop settings

Many of the customized and optimized settings on your device desktops can be migrated. These settings are defined in the `<Desktop>` section in the command file. For each item you want to include, specify `true` within the tags (for example, `<colors>true</colors>` will capture color settings). For items you do not want to include, specify `false` within the tags. You can select from the following settings:

- **Desktop settings:** Desktop theme, color scheme, visual effects
- **Accessibility:** Accessibility settings such as those for the keyboard, the sound, and the mouse (see Ease of Access Center in the Windows Vista or Windows 7 Control Panel)
- **Active Desktop:** The active state is only supported in the Windows 2000 operating system
- **Colors:** Desktop and window colors
- **Desktop icons:** All desktop contents, including folders, files, shortcuts, icons, and icon positions

- **Display:** Desktop width, height, and color depth
- **Icon Font:** The font used for the desktop icons
- **Keyboard:** Keyboard repeat rate, cursor blink rate, and delay
- **Mouse:** Left or right-handed mouse settings, speed, and double-click rate
- **Pattern:** The pattern used for the desktop is only supported in the Windows 2000 operating system
- **Screen Saver:** Current screen saver settings
- **Send To menu:** Send To menu settings
- **Shell:** View sort order, view type (large or UMAll icon), status bar, and toolbar show/hide status
- **Sound:** Sound settings
- **Start Menu:** Start menu commands
- **Taskbar:** Docking edge, size, always-on-top, auto hide, show clock, show UMAll icons in the Start menu
- **Time zone:** System time zone
- **Wallpaper:** Desktop wallpaper
- **Window metrics:** Spacing and arrangement of minimized windows, dialog message font, menu size, and scroll bar sizes

The following restrictions apply to desktop settings:

- **Active Desktop:** To migrate the Active Desktop including the wallpaper, you must select the wallpaper setting as well.
- **Icons:**1) The vertical and horizontal spacings between desktop icons do not migrate precisely. 2) Only the icons that are in the current user's desktop directory are migrated.
- **Shell:** To migrate the Windows Explorer shell settings, you must migrate both your shell desktop settings and your Microsoft Internet Explorer application settings. If the target computer uses Windows 2000 Professional, Windows XP, Windows Vista, or Windows 7, the folder view settings (such as large icons, tiles, and details) do not migrate.
- **Sound:** UMA migrates the active sound scheme from the source computer to the target computer. The sound scheme is set in the Sounds and Multimedia Properties window of the Windows control panel. If the sound scheme in the source computer is set to No Sounds, sounds will not be migrated to the target computer. If the source computer uses custom sounds, you must migrate the sound files along with the sound scheme.
- **Wallpaper:** If the wallpaper that you want to migrate is a JPEG file, you also must capture the Active desktop setting. It is not necessary to capture the Active desktop setting when you migrate wallpaper that is a BMP file.

A code sample of desktop settings is shown below.

```
<Desktop>
<desktop_settings>true</desktop_settings>
<accessibility>true</accessibility>
<active_desktop>true</active_desktop>
<colors>true</colors>
<desktop_icons>true</desktop_icons>
<display>false</display>
<icon_metrics>false</icon_metrics>
<keyboard>true</keyboard>
<mouse>true</mouse>
<pattern>false</pattern>
<screen_saver>true</screen_saver>
<sendto_menu>false</sendto_menu>
```

```
<shell>false</shell>
<sound>true</sound>
<start_menu>false</start_menu>
<taskbar>false</taskbar>
<time_zone>true</time_zone>
<wallpaper>true</wallpaper>
<window_metrics>false</window_metrics>
</Desktop>
```

Migrating application settings and associated files

Persistent application settings and associated files can be migrated as part of a device's profile. Application programs themselves are *not* migrated during profile migration (however, they can be part of an OS image deployment).

Individual applications are specified for migration in the `<Applications>` section of the command file. You can specify that all application settings are migrated by using the variable `$(all)`.

UMA can capture the user's settings and customizations. For Lotus Notes and Microsoft Outlook, the settings might be the address book and any locally stored e-mail. For Internet Explorer and Netscape Navigator, the customizations might include bookmarks, cookies, and preferences.

For more information about the restrictions that apply to migrating specific applications, see "Using profile migration in LANDesk Management Suite 9," which can be downloaded from the LANDesk support community at community.landesk.com.

A code sample of application settings is shown below.

```
<Applications>
<Application>$(all)</Application>
</Applications>
<Inclusions>
<IncDescription>
<Description>%Personal Directory%\ /s</Description>
<DateCompare>
<Operand />
<Date />
</DateCompare>
<SizeCompare>
<Operand />
<Size />
</SizeCompare>
<Dest />
<Operation />
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>%Personal Directory%\*.vol /s</Description>
<DateCompare>
<Operand />
<Date />
</DateCompare>
<SizeCompare>
<Operand />
<Size />
</SizeCompare>
</ExcDescription>
```

```
</Exclusions>
```

Migrating printer settings

Printer settings to migrate are specified in the <Printers> section of the command file. You can specify individual printer settings by enclosing the printer name within <Printer></Printer> tags, or you can migrate all settings by using the variable $(all).

You can only migrate printer settings for printers that have built-in printer definitions in the operating system you are using.

Virtual printers settings (for example, settings for an XPS printer) can't be migrated from a source computer to a target computer.

A code sample of printer settings is shown below.

```
<Printers>
<Printer>$(all)</Printer>
</Printers>
```

Migrating network settings

You can migrate settings for network connections and configurations, computer identification, and mapped drives. . These settings are defined in the <Network> section in the command file. For each item you want to include, specify `true` within the tags (for example, `<computer_name>true</computer_name>` will capture the computer name). For items you do not want to include, specify `false` within the tags. You can select from the following settings:

TCP / IP configuration

- IP / Subnet / Gateway
- DNS configuration
- WINS configuration

Network identification

- Computer name
- Computer description
- Domain / Workgroup name

Other

- Mapped drives
- Dial-up networking
- Shared folders / Drives
- ODBC data sources

The following restrictions apply to network settings:

- **Domain / Workgroup:** If the source computer is a member of a domain and you want the target computer to be a member of the same domain, create an account for the target computer on the domain controller. If the domain controller is running Microsoft Windows 2000 Server, select the **Allow pre-Windows 2000 computers to use this account** option.
- **DNS Configuration:** The DNS settings do not migrate when you perform a PC-to-PC migration.

A code sample of network settings is shown below.

```
<Network>
<ip_subnet_gateway_configuration>false</ip_subnet_gateway_configuration>
<dns_configuration>false</dns_configuration>
```

```
<wins_configuration>false</wins_configuration>
<computer_name>false</computer_name>
<computer_description>false</computer_description>
<domain_workgroup>false</domain_workgroup>
<shared_folders_drives>true</shared_folders_drives>
<mapped_drives>true</mapped_drives>
<dialup_networking>true</dialup_networking>
<microsoft_networking>false</microsoft_networking>
<odbc_datasources>false</odbc_datasources>
</Network>
```

Migrating files and folders

You can migrate individual or multiple files determined by directory location and filename. File and folder settings are enabled in the `<FilesAndFolders>` section of the command file. You can specify individual folders and files in the `<Inclusions>` and `<Exclusions>` sections of the document to specify which files you do and don't want to include.

Input the files that you want to migrate. The Files / Folders page lists the files on the source computer, sorted by location. You can select all the files in a location, or you can expand the tree and select individual files.

Consider where you want the selected files to be placed on the target computer. If the hard disks on the source and target computers are configured differently, you must select alternative destinations for files and directories.

Be careful when changing the locations of files. Batch and configuration files might contain fully qualified path names. If you change the locations of the files and directories to which the batch and configuration files refer, the programs or tasks will not run successfully.

A code sample of file and folder settings is shown below.

```
<FilesAndFolders>
<run>true</run>
</FilesAndFolders>
<ArchiveFile>
<filename></filename>
</ArchiveFile>

<Inclusions>
<IncDescription>
<Description>%Personal Directory% /s</Description>
<DateCompare>
<Operand></Operand>
<Date></Date>
</DateCompare>
<SizeCompare>
<Operand></Operand>
<Size></Size>
</SizeCompare>
<Dest></Dest>
<Operation></Operation>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>%Personal Directory%\*.vol /s</Description>
<DateCompare>
<Operand></Operand>
<Date></Date>
```

```
</DateCompare>
<SizeCompare>
<Operand></Operand>
<Size></Size>
</SizeCompare>
</ExcDescription>
</Exclusions>
```

Managing local accounts

LANDesk provides an administrative tool that enables you to manage a local machine's users and groups from the console.

Read this chapter to learn about:

Local accounts overview

Local accounts is an administrative tool used to manage the users and groups on local machines on your network. From the console, you can add and delete users and groups, add and remove users from groups, set and change passwords, edit user and group settings, and create tasks to reset passwords for multiple devices. For local accounts management to work, the Standard LANDesk Agent must be installed. If a device is turned off or not connected to the network, you won't be able to use local accounts to manage the device.

Note: When using local accounts, the core interacts with the other machines at near real-time.

Using the core server's local account

Since your core server is a node on your network and has local accounts, you can use the local accounts tool to perform administrative tasks on the server, as well as the console itself. You can add LANDesk users to the console by creating local users and adding them to the Windows LANDesk Management Suite, LANDesk Script Writers, or LANDesk Administrators group. This enables you to perform administrative tasks from the console, without having to use the native local accounts management system, such as Computer Management on Windows.

If you prefer, you can still use the native local accounts management system to manage local accounts. You can access the devices directly, remote control the machines from the console, or use a third-party tool to access the devices and perform the administrative tasks.

For more information on using the console to perform local accounts management, see "Adding Management Suite console users" on page 46.

Managing local users

You can add, delete, and edit users on a local machine from the console.

To add a user

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Users** and then click **Add**.
4. In the **New User** dialog, enter a user name, a full name, and a description.

5. Enter a password, confirm the password, and specify the password settings.
6. Click **Save**.

To delete a user

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to delete and then click **Delete**.
5. Click **Yes** to verify the procedure.

To edit a user

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to edit and then click **Edit**.
5. Make your desired changes and then click **OK**.

Managing local groups

You can add, delete, and edit groups on a local machine from the console.

To add a group

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Groups** and then click **Add**.
4. In the **New Group** dialog, enter a group name and a description.
5. (Optional) Add users to the group by clicking **Add**.
6. Click **Save**.

To delete a group

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to delete and then click **Delete**.
5. Click **Yes** to verify the procedure.

To edit a group

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to edit and then click **Edit**.
5. Make your desired changes and then click **OK**.

Assigning users to groups

There are two methods for adding and removing users to and from groups on a local machine from the console. The first method allows you to add or remove multiple users to or from a group at one time. The second method allows you to add or remove the selected user to or from one or more groups.

To add users to a group

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to add users to and then click **Edit**.
5. In the **Edit group** dialog, click **Add**.
6. Select the users you want to add to the group and then click **Add>>**.
7. Click **OK**.
8. Click **OK** in the **Edit group** dialog.

To add a user to one or more groups

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to add to one or more groups and then click **Edit**.
5. In the **Edit user** dialog, click the **Member of** tab.
6. Click **Add**.
7. Select the groups you want the user to belong to and then click **Add>>**.
8. Click **OK**.
9. From the **Edit user** dialog, click **OK** .

To remove users from a group

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to remove users from and then click **Edit**.
5. Select the users you want to remove and then click **Remove>>**.
6. Click **OK**.

To remove a user from one or more groups

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to remove from one or more groups and then click **Edit**.
5. In the **Edit user** dialog, click the **Member of** tab.
6. Select the groups you want the user to be removed from and then click **Remove>>**.

7. Click **OK**.

Changing passwords

You can change a user's password on a local machine from the console.

To change a user's password

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to change the password for and then click **Set password**.
5. Enter a new password, confirm the password, and then click **OK**.
6. Click **OK** to verify the password has been changed successfully.

Resetting passwords

You can create a scheduled task to reset the password for a specific user name. Once the task has been scheduled, you are taken to the **Scheduled tasks** tool where you can specify the target devices and the start time. For example, from a local account you could create a task to reset the password for the **Administrator** user name. You would then designate the target devices and schedule when the task will occur. Once the task is run, all administrators wanting to authenticate to the target devices would have to use the new password.

To reset the password

1. In the console, from the **Network View**, click **Devices > All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Click the **Schedule** icon.
5. In the **Schedule task** dialog, insert the user name that you want to reset the password for. You can select an existing user name from the drop-down list, or type a different one.
6. Enter a new password, confirm the password, and then click **Schedule**.
7. From the **Scheduled tasks** tool, right-click on the scheduled task and then click **Properties**.
8. From the **Scheduled tasks - properties** dialog, designate the target devices and enter the scheduling information.
9. Click **Save**.

Core synchronization

Core synchronization is a new feature introduced in LANDesk Management Suite 9.0. With core synchronization, you can copy configurations and tasks from core to core, either manually or automatically. You can use this feature to keep multiple cores synchronized with a master core.

You can synchronize these items:

- Agent configurations
- Alerts
- Column sets
- Delivery methods
- Distribution packages
- Power management settings
- Queries and query column settings
- Scripts
- Security and patch settings
- Tasks and policies

There are three ways to synchronize items:

- On demand
- Automatically
- Import/Export

When you export/sync tasks or software distribution package configurations, the export/sync data will contain associated queries and related items. Note that export/sync data only contains information from the Management Suite database. For example, software distribution export files won't contain the actual package being distributed.

Related to this, when working with export/sync scheduled tasks, make sure any package paths are the same for the source and target servers. Otherwise, when you import/sync the task and run it, the task will fail because the target server couldn't find the package.

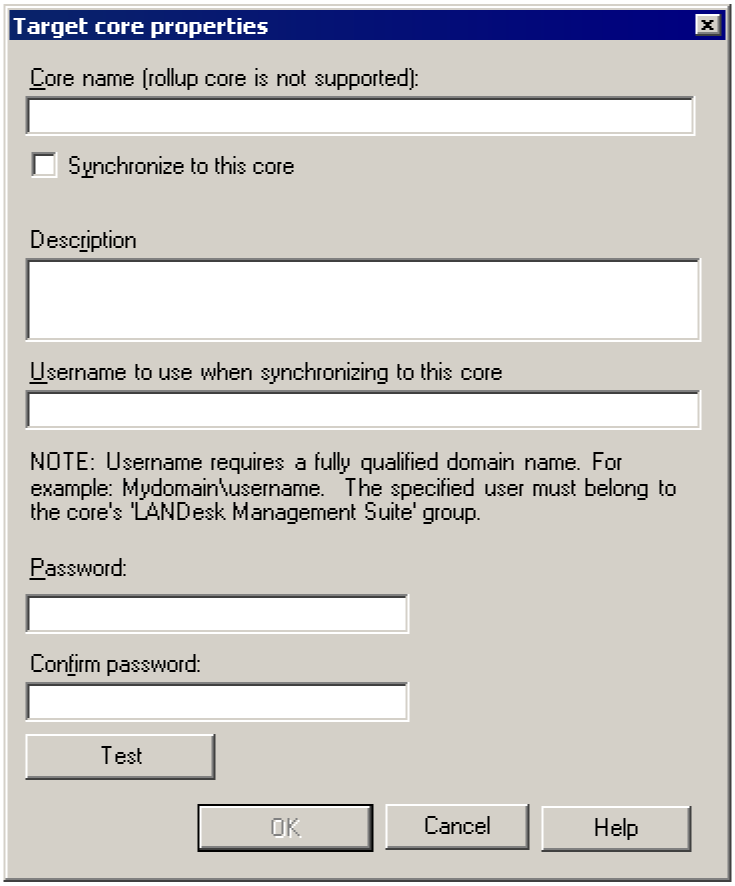
When you copy or autosync an item, the following happens:

1. The source core server creates an XML .ldms export file containing information necessary to recreate the source item and any items referenced by the source item.
2. The source core server connects via HTTPS to the target core server's secure Web service and transmits the .ldms file.
3. The target core's secure Web service copies the received .ldms file to its C:\Program Files\LANDesk\ManagementSuite\exportablequeue folder.
4. The core synchronization service regularly checks this folder for new files. It finds the exported file from the source core and imports it, removing the file from the folder.

Note: The OS deployment and software license monitoring tools don't support core synchronization.

Adding servers to the synchronization list

Before you can use synchronization, you need to configure the list of servers you want to synchronize with. Cores communicate via HTTPS and authenticate with a username and password you provide for each core.


Target core properties
Core name (rollup core is not supported):
Synchronize to this core
Description
Username to use when synchronizing to this core
NOTE: Username requires a fully qualified domain name. For example: Mydomain\username. The specified user must belong to the core's 'LANDesk Management Suite' group.
Password:
Confirm password:
Test
OK
Cancel
Help

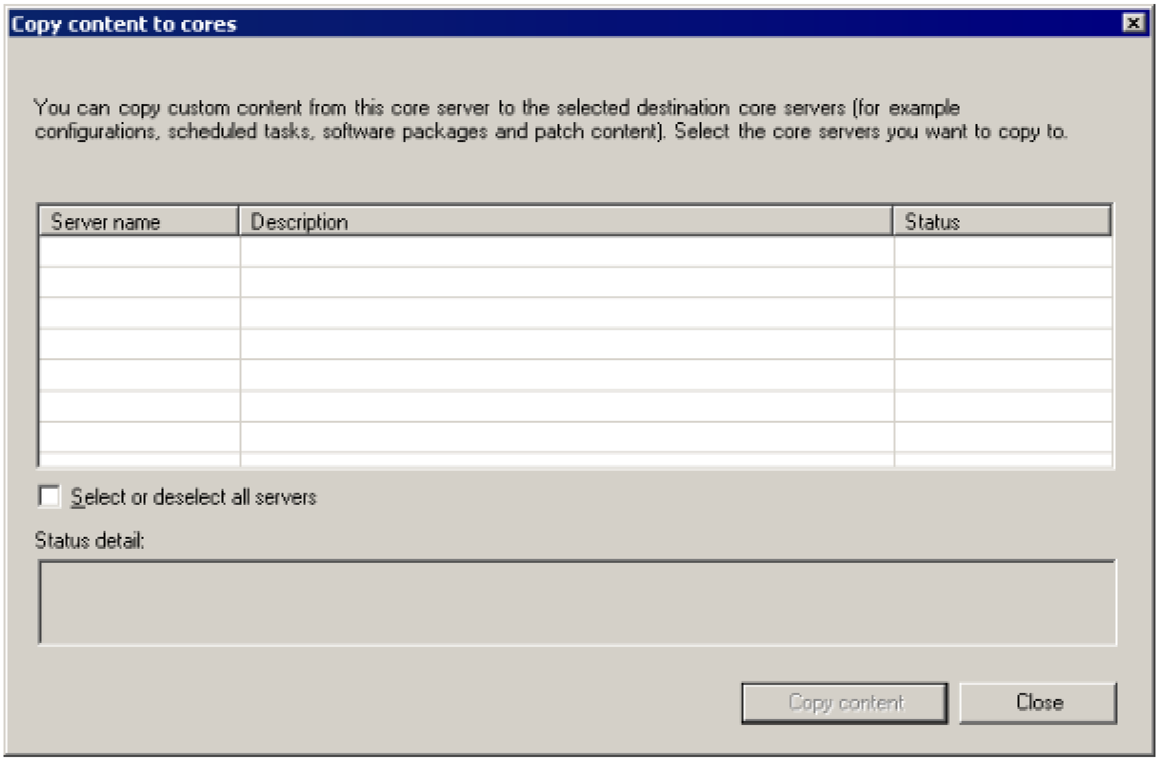
To add a core server to the synchronization list

1. Click **Tools > Administration > Core synchronization**.
2. Right-click the **Core servers** tree item and click **Add target core**.
3. Enter the **Core name**.
4. Select **Synchronize to this core** to enable core synchronization when you exit the dialog. You can select or clear this option later on to selectively enable or disable synchronization to that core.
5. Enter a **Description**.
6. Enter the fully-qualified domain name for the user account to use when synchronizing (domain\username). This account should have full console privileges and it must be a member of one of the local LANDesk user groups on the target core.
7. Enter and confirm the **Password** for the account you provided.
8. Click **Test** to confirm your configuration.
9. Click **OK**.

IMPORTANT: Rollup core servers use the scheduler service credentials to authenticate for synchronization. On rollup cores, these scheduler service credentials must be a member of a group with console administrator privileges on the source core servers. If the credentials don't have these privileges, you'll see task handler errors in the source core server's synchronization log. For information on how to change the scheduler service credentials, see "About the Configure LANDesk Software Services dialog: Change login dialog" on page 69.

Synchronizing items on demand

Synchronize an item on demand by right-clicking it and clicking **Copy to other core(s)**. When you do this, you can select the servers you want to receive the copy. Clicking **Copy content** immediately starts the copy operation. The copy only happens once, and the item you copied is available on the remote cores immediately. Note that you may have to manually refresh the remote core's console view by pressing F5 for the item to appear. The remote copies have the same name and location as the source copy and are editable. Any groups or subgroups containing the item will be created automatically.



You can copy custom content from this core server to the selected destination core servers (for example configurations, scheduled tasks, software packages and patch content). Select the core servers you want to copy to.

Server name	Description	Status

□ Select or deselect all servers

Status detail:

Automatically synchronizing items

Before using auto sync, configure which Management Suite components you want to synchronize.

Configuring auto sync

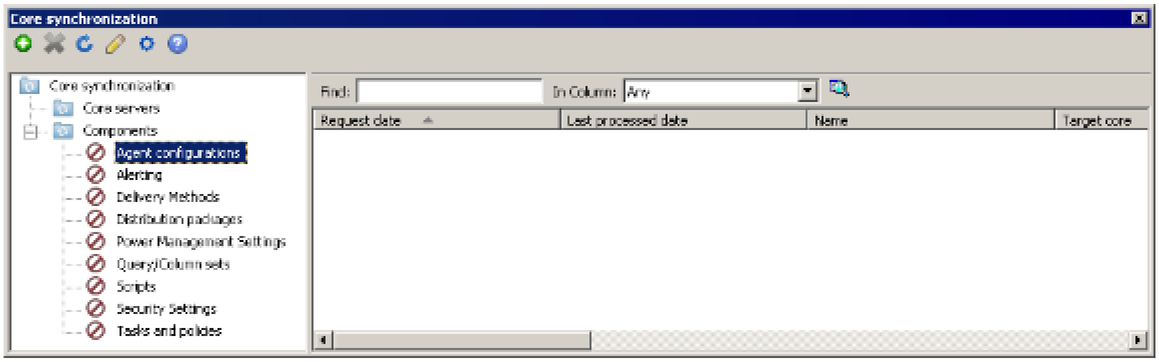
You can enable auto sync on individual items, but if an item's component doesn't have synchronization enabled, that item won't sync. Disabling synchronization on a component doesn't change the auto sync flag on flagged items, so if you disable and then later on enable synchronization, items you originally enabled auto sync for will resume synchronization.

To select the auto sync components you want enabled

1. Click **Tools > Administration > Core synchronization**.
2. Right-click the **Components** tree item and click **Edit auto sync components**.
3. Move the components you want to sync to the **Auto sync components** list.
4. Click **OK**.

You can also enable or disable auto sync by right-clicking a component and clicking **Auto sync**.

When you select a component in the **Components** tree, you can see synchronization activity for that component.



Enabling auto sync for an item

Synchronize an item automatically by right-clicking it in a component's tree view and clicking **Auto sync**. If the item's sync component isn't enabled, you'll be prompted to enable that component. The synchronization for this item will happen at the next synchronization interval. If you again right-click that item, you'll see a check mark next to **Auto sync** in the menu.

As with on-demand synchronization, auto sync items appear in the same location in the console. However, auto sync items are read-only on target cores and they can't be edited or deleted. Each time you change an auto sync item on the source core, the item gets synchronized to the target cores. If you want console users to be able to delete an auto synced item, just turn auto sync off. That won't remove the item from target cores, but those target items will become editable.

Synchronizing scheduled tasks

Synchronized scheduled task data doesn't include the task start time. If you synchronize a scheduled task, the only way to run it on the target server is to right-click it and click **Start now**. Since synchronized items are read only, you can't edit it on the target core and add a new start time. As a workaround, you can use the copy to core feature. The task still won't include a start time on the target core, but this way the task will be editable there.

Exporting and importing items

Items that you can sync can also be exported and imported. Exporting an item creates a .ldms file in XML format that contains the data necessary to recreate that item and any items that item referenced. You can then take this file to another core, for example, and re-import it.

When importing, you'll be prompted to do one of these three things:

- **Update:** Insert or update matching items, maintaining group hierarchy specified in the .ldms file. Preserves IDs from the file. This will overwrite any changes to the existing item.
- **Insert items into selected group or owner:** Insert all items and assign new IDs to each. Only add to group if the type matches. Update the owner of each imported item.
- **Insert items into group(s) specified in the .ldms file:** Insert the new items, maintaining group hierarchy specified in the .ldms file. New IDs are assigned to each item.

For more information on how conflict management works, see "Conflict management" on page 279.

To export an item

1. In the **Network view** or tool tree view, right-click the item you want to export and click **Export**. If an item is exportable it will have an **Export** command.
2. Enter a file name and navigate to the path you want.
3. Click **Save**.

To import an item

1. In the **Network view** or tool tree view, navigate to the location where you want the imported item to appear.
2. Right-click and click **Import**.
3. Click the import option you want.
4. Click **Import**.

Changing auto synchronization settings

You can configure the core server's auto synchronization interval. The default interval is two minutes. When your selected interval has passed, the core server checks auto sync items for changes. If any have changed, the core then sends those changes to the target cores you specified. Depending on the amount of data being synchronized, lowering this interval slightly increases the source core's processor load.

The Auto synchronization settings dialog has these options:

- **Synchronize every:** The synchronization interval you want. The default is two minutes.
- **Maximum number of retries:** The number of times this core will try to connect to target cores. The default is five. Once this limit is reached, the source core will no longer try to sync that item.
- **Compress data when sending:** Cores synchronize via HTTPS. When checked, this option also compresses the data stream. The default is checked.
- **Show read only warnings when user attempts to edit auto-synced items:** This option applies only to the server you make this change on, and it refers to auto-synced items that this server receives, not originates. You can disable this option if you don't want console users to see an extra warning if they try to make changes to an auto-synced item on this server. Disabling this only disables the extra warning. Console users still won't be able to change auto-synced items the server receives.

To change auto synchronization settings

1. Click **Tools > Administration > Core synchronization**.
2. On the **Core synchronization** tool's toolbar, click the **Edit sync service settings** button.
3. Enter the synchronization interval you want.
4. Change the other options if necessary.
5. Click **OK**.

To restart synchronization on an item that has exceeded the retry limit

1. Click **Tools > Administration > Core synchronization**.
2. Under **Core servers**, click the server you want to restart synchronization on.
3. In the log, right-click the failed item and click **Synchronize again**.

Monitoring synchronization status

When you select a **Core server** or **Component** in the tree view, you can see a log of syncs and real-time sync status. Scroll to the right to see the status columns that are available. When you select the root **Core servers** node, you can see a high-level sync status for target cores. This data includes the pending count, which if high or stuck may indicate there's a problem synchronizing to that core.

Sync items can have one of these states:

- **Pending:** The item is waiting to be sent.
- **Sent:** The item has been sent.
- **Working:** The target core is processing the item.
- **Succeeded:** The item was synchronized successfully.
- **Failed:** The item wasn't synchronized successfully.

Conflict management

Exportable items have a unique ID that helps Management Suite track whether items are the same or not. This helps synchronization manage sync item conflicts. If you copy or sync an item on one server and that same item exists on the target server, that item will only be overwritten if the items share the same unique ID. That unique ID consists of the core server name and the database row number containing that item. You can see an item's unique ID and revision number in an item's information dialog (right-click the item and click **Info**).

If two items with the same name have a different ID, synchronization will leave the original alone on the target and add a %1 to the sync item's filename. Synchronization will keep creating new entries on subsequent sync conflicts and increment this number for each one until the limit of 99 is reached.

Managing Macintosh devices

LANDesk Management Suite provides complete system management for Apple Macintosh computers and devices. This enables IT professionals to automate system management tasks throughout the enterprise. From the console, you can gather and analyze detailed hardware and software inventory data from each device. Use the data to select targets for software distributions and to establish policies for automated configuration management. Manage software licenses to save costs and monitor compliance with license agreements. Remote control devices to resolve problems or perform routine maintenance. Protect your devices from a variety of prevalent security risks and exposures. Keep track of your inventory and produce informative reports.

Read this chapter to learn more about:

- LANDesk Management Suite for Macintosh overview
- Agent Configuration for Macintosh devices
- Connecting through the LANDesk Management Gateway
- Inventory for Macintosh devices
- Remote control for Macintosh devices
- Software Distribution for Macintosh devices
- Managed scripts for Macintosh devices
- Scheduled tasks for Macintosh devices
- Reporting for Macintosh devices
- Software license monitoring for Macintosh devices
- Blocking applications for Macintosh devices
- Patch and compliance for Macintosh devices
- Operating system deployment for Macintosh devices
- Using the Mac remote control viewer

LANDesk Management Suite for Macintosh overview

This chapter describes how LANDesk Management Suite is used to manage Macintosh computers. It provides a central location for referencing specific information on Macintosh-related tasks, tools, features, and functionality. For more information about using tools and features to manage your network, refer to the section for each tool.

LANDesk Management Suite for Macintosh functionality works with the following operating systems:

Mac OS X: 10.4 (Tiger) and 10.5 (Leopard)

Mac OS X versions 10.4 (Tiger) and 10.5 (Leopard) support all of the Macintosh features available in LANDesk Management Suite.

Legacy support

You can find information on downloading legacy agents for Macintosh at http://community.landesk.com/support.

Mac OS X: 10.2 (Jaguar) and 10.3 (Panther)

The LANDesk Management Suite version 9.0 agent for Macintosh does not support Jaguar or Panther. However, you can still manage devices running these operating systems if they have the LANDesk Management Suite version 8.8 agent for Macintosh installed on them.

Note: Due to policy differences between version 8.8 and version 9.0, policy-based management will not work with Jaguar and Panther clients using the version 8.8 agent.

Mac OS 9

You can use inventory and remote control with Mac OS 9 devices. This OS is in the process of being phased out, so only limited support is available.

Agent Configuration for Macintosh devices

LANDesk uses agent configurations to gain control of devices and manage them. Management Suite version 9.0 introduces support for pushing Mac agent configurations to unmanaged Macintosh devices using the same process used to push agents to Windows devices.

Loading the default agent configuration for Macintosh devices

The Default Mac Configuration package contains the required agent for controlling Macintosh devices. In order to gain control of your Macintosh devices, you need to:

1. Obtain the necessary package (agents).
2. Deploy and install the agents to the devices.

After the default agents have been installed, your devices become managed devices. Then you can create custom configurations to have greater control of your Macintosh devices. Custom agents are easily implemented once your devices are managed.

Note: All devices must support TCP/IP.

Obtaining the package (agents) for Macintosh devices

You can obtain the default package **Default_Mac_Configuration.mpkg.zip** from the LDLogon/Mac shared folder on your core server. The LDLogon/Mac folder is automatically created during the installation of Management Suite. Since the LDLogon folder is a Web share, it is available from the Internet at http://<CoreServerName>/LDLogon/Mac.

Deploying agents to Macintosh devices that use Secure Shell (SSH)

To place agents on Macintosh devices that have Secure Shell (SSH) turned on, you must specify the SSH login credentials for the unmanaged Mac devices by selecting **Configure > Services > Scheduler > Change Login** from the Windows console. You can then use the same push-based agent deployment you would use for Windows devices.

Deploying and installing agents on Macintosh devices that do not use Secure Shell (SSH)

To place agents on Macintosh devices that do not have Secure Shell (SSH) turned on, you will need to decide on an alternate deployment method, such as:

- Accessing the agent using a Web browser from LDLogon/Mac (see Obtaining the package (agents) for Macintosh devices), and e-mailing the configuration package to users.
- Putting the configuration package on a CD or other removable media and taking it to each Macintosh device.

After you have deployed the agents to the target devices, you need to install them on the machines. A full hardware and software scan is run at the end of every install, which synchronizes the devices with the core server. You must have the Management Suite agents installed on your Macintosh devices and their inventory information sent to the core server before you can manage them. After you've installed the base agents, subsequent agent deployments and updates are easily handled through the existing agents.

To install agents

1. On the client machine, locate **Default Mac Configuration.mpkg.zip** or access the package from the Web share (see Obtaining the package (agents) for Macintosh devices).
2. Unzip the file or copy the files to the target device.
3. Double-click **LDMSClient.mpkg**.
4. Reboot the machine.

Creating agent configurations for Macintosh devices

Use the Agent configuration tool to create and update (replace) custom configurations for your Macintosh devices. You can create different configurations for your specific needs, such as changing inventory scanner settings, remote control permissions, or what network protocols the agents use.

In order to push a configuration to devices, you need to create or update an agent configuration and schedule the task to occur.

Creating or updating the agent configuration

Set up specific configurations for your devices. Don't use parentheses in your Macintosh agent configuration names. Parentheses in the name will cause the deployment task to fail.

To create an agent configuration for Macintosh devices

1. Click **Tools > Configuration > Agent configuration**.
2. Click the **New Mac** button to create a new Macintosh configuration.
3. Complete the Agent configuration dialog. For more information, see Using the Agent configuration dialog (for Macintosh), or click **Help** in the dialog.
4. Click **Save**.

To update an agent configuration

1. Click **Tools > Configuration > Agent configuration**.
2. Right-click the agent configuration to be updated and select **Properties**.
3. Make the updates to the agent configuration.
4. Click **Save**.

Scheduling the agent configuration

You can push agent configurations to devices that have the standard LANDesk agent installed. Use the **Scheduled tasks** tool to run your new or updated agent configuration.

To schedule an agent configuration for Macintosh devices

1. Click **Tools > Configuration > Agent configuration**.
2. Right-click the agent configuration to be scheduled and select **Schedule**.
3. Target devices for the task and start the task.

Manually running agent configuration for Macintosh devices

You can manually run agent configurations for Macintosh devices once they have been created or updated. When an agent configuration is created (**Tools > Configuration > Agent configuration**), the following file is created in the LDLogon/Mac folder on your core server:

- **<agent configuration name>.mpkg.zip**

The LDLogon/Mac folder is a Web share and should be accessible from any browser. Follow the instructions for Loading the default agent configuration for Macintosh devices. Insert your agent configuration files instead of the default files.

Uninstalling Macintosh agents

To uninstall Macintosh agents, run **uninstallmacagent.sh** from \\<core>\ldmain.

Using the Agent configuration dialog (for Macintosh)

This section describes the agent configuration dialog for Macintosh devices. The dialog consists of the following:

- Application policy management
- Inventory
- Remote control
- Standard LANDesk agent
- Patch and compliance scan

About the Application policy management page

Use this page to configure settings for the policy-based distribution agent.

- **TCP port number:** Specifies the port the policy-based distribution agent will use to communicate with the core server. The default port is 12175. You'll need to make sure this port is open on any firewalls between devices and the core server. If you change this port, you'll also need to change it on the core server. You can change the port the QIP server service uses by editing the following registry key: HKLM\Software\Intel\LANDesk\LDWM\QIPSrvr
- **Run when IP address changes:** If checked, a scan is triggered when the IP address changes.
- **Change settings:** Changes settings and configures a custom schedule based on time, day of week or month, whether a user is logged in, if an IP address changes, and the available network bandwidth.

About the Inventory page

Use this page to configure the inventory scanner.

- **Send scan to LDMS core server:** Sends the scan information to the core server database.
- **Save scan in directory:** The directory where the data from the scan is saved. If you select both the core server option and this option, the scan information will go to both locations.
- **Choose scan components:** Select the components you want to scan. Not selecting all components may slightly increase scanning speed.
- **Force software scan:** Forces the device to do a software scan with each inventory scan, regardless of whether the core server indicates one is due.
- **Run when IP address changes:** The IP address trigger sends only a mini scan to the core server, which makes the inventory much faster in IP address changes.

- **Change settings:** Changes settings and configures a custom schedule based on time, day of week or month, whether a user is logged in, if an IP address changes, and the available network bandwidth. The default schedule is to run a scan every day with a random delay of up to one hour.

About the Remote control page

Use this page to configure the remote control agent.

- **Local template:** This is the most basic security, using whatever remote control settings are specified on the device. This model doesn't require any other authentication or group membership.
- **Integrated security:** This is the most secure option. Integrated security follows this communication flow:
  1. The remote control viewer connects to the managed device's remote control agent, but the agent replies that integrated security authentication is required.
  2. The viewer requests remote control rights from the core server.
  3. The core server calculates remote control rights based on the viewer's scope, role-based administration rights, and Active Directory rights. The core server then creates a secure signed document and passes it back to the viewer.
  4. The viewer sends this document to the remote control agent on the managed device, which verifies the signed document. If everything is correct, the agent allows remote control to begin.
- **Permission required:** Prompts the user for permission to be remote-controlled whenever someone initiates a remote control session. If the user isn't at the keyboard or denies permission, the remote control session won't start.
- **Open applications and files:** Permits a remote user to open files on this device.
- **Copy items:** Permits a remote user to copy files to and from this device.
- **Delete and rename items:** Permits a remote user to delete or rename files that reside on this device.
- **Lock keyboard and mouse:** Permits a remote user to lock your keyboard and mouse during a remote control session. This option prevents you from interfering with remote actions.
- **Blank screen:** Permits a remote user to make your screen go blank during a remote control session. This option is useful if your device contains sensitive documents that an administrator may need to open remotely without letting others read if they happen to walk by your device monitor.
- **Restart and shut down:** Permits a remote user to restart or shut down your device.
- **Control and observe:** Permits a remote user to remote control and observe your actions on this device. The administrator can't do anything except watch your actions.
- **Alert when observing:** When a remote control session is active, display a visual cue in the menu bar.

About the Standard LANDesk agent page

Use this page to configure agent security and management scope. For more information on agent security, see Agent security and trusted certificates. For more information on scope, see Role-based administration.

- **Trusted certificates:** Lists the certificates on the core server. The client must have a certificate that matches the certificate on the core server for agent communication to be authorized. These certificates are used to authenticate agent communication. You can enter a domain name or IP address for the client to use when communicating with the LANDesk core server. The remote control agent for Macintosh doesn't use a certificate.

- **Path:** Defines the device's computer location inventory attribute. Scopes are used by role-based administration to control user access to devices, and can be based on this custom directory path. The path is optional.

About the Patch and compliance scan page

Use this page to configure scheduling for patch and compliance scans.

- **Change settings:** Changes settings and configures a custom schedule based on time, day of week or month, whether a user is logged in, if an IP address changes, and the available network bandwidth. The default schedule is to run a scan every day with a random delay of up to one hour.

Connecting through the LANDesk Management Gateway

There are two options for configuring managed Macintosh devices to connect to the core through the LANDesk Management Gateway:

- Push the configuration to mobile devices while they are attached to the local network. This is an easy way to configure mobile devices so they can connect through the LANDesk Management Gateway after they are disconnected from the local network. This type of configuration enables LANDesk Management Suite functionality through the appliance without the necessity of manually configuring individual managed devices.
- Manually configure each managed device to connect through the LANDesk Management Gateway. This type of configuration enables LANDesk Management Suite functionality through the appliance. Manual configuration can only be done by a user with Administrator rights on the client device.

To push the configuration to mobile devices while they are connected to the network

- After configuring the core for connection through the Management Gateway, rebuild any agents for Macintosh devices and push them to the devices. For more information, see Configuring the LANDesk Management Gateway .

To manually configure a managed device

1. From the **Utilities** folder on the managed device, launch the **LANDesk Management Gateway** application.
2. Specify the **Domain name** of the Management Gateway.
3. Choose the best connection method to the LANDesk core.
4. Request a certificate by typing a LANDesk console user name and password, then clicking **Request**.
5. Click **Test** to test the connection from the managed device to the LANDesk Management Gateway.
6. If the test fails, check the information you entered and correct any mistakes, then click **Test** to make sure the connection works.
7. If the managed device accesses the Internet through a proxy, specify the necessary proxy settings.

Inventory for Macintosh devices

The inventory scanning utility is used to add Macintosh devices to the core database and to collect device hardware and software data. When you configure a device, the inventory scanner is one of the components of the LANDesk agent that gets installed on the device. The inventory scanner runs automatically when the device is initially configured. A device is considered managed once it sends an inventory scan to the core database.

The scanner executable for Mac OS X is called **ldiscan** (UNIX; it is case sensitive). Inventory scan files are saved locally on the client and are compatible with the core. You can e-mail the file to the core administrator and then drag and drop it into the ldiscan directory. You need to change the extension of the file to .SCN.

Macintosh devices can be configured to scan at boot-up, at log in, at wake from sleep, and at network change. You can also use agent configuration to schedule the inventory scan to occur at a regular interval.

The Macintosh inventory scanner encrypts scans. The inventory scanner also uses delta scans so that after the initial full inventory scan, subsequent scans send only the changed data to the core server, reducing network bandwidth consumption.

The Macintosh inventory scanner looks in the "Custom Data" folder under the agent installation folder for XML files that contain additional information you want the inventory scanner to pass to the core server. This additional information appears in the inventory tree under the Custom Data node.

With the inventory scanner, you can view summary or full inventory data. You can print and export the inventory data. You can also use it to define queries, group devices together, and generate specialized reports. For more information about the Inventory tool, see Managing inventory.

Software scanning

A software scan compiles an inventory of software on managed devices. These scans take longer to run than hardware scans. Software scans can take a few minutes to complete, depending on the number of files on the managed device. You can configure the software scan interval in the **Configure > Services > Inventory** tab.

All applications installed in the Applications folder are placed into the **Software > Application Suites** node in the inventory tree.

Scanner command-line parameters

You can add command-line parameters to the inventory scanner's (ldiscan) shortcut properties to control how it functions. The option are case-sensitive.

Note: Unless the **--ignore** option is set, command line options don't override settings in the agent configuration scan preferences. For example, specifying **-F** for a full software scan won't perform software scan if the software scan is turned off in preferences.

Option	Name	Description
-c	--core <path>	Specifies which core the scan is sent to. Example: c spencercore2.landesk.com
-D	--Delta	Forces a delta scan
-e	--everything	Forces a full hardware and software scan
-F	--force	Forces a software scan even when none of the software scanning options have been selected in the agent configuration. Example: [MACHINES_MACX] REMEXEC0=/Library/Application\ Support/LANDesk/bin/ldiscan –F
-h	--help	Displays a list of command-line options
-i	--ignore	Ignores user and server preference settings

Option	Name	Description
-l	--ldappl <path>	Specifies path to alternate ldappl.ini path
-L	--Limit	Limits downloading of ldappl3.ini
-o	--output <path>	Specifies which directory you want the scan file to go to. Example: -o /Users/spencer
-P	--Print	Displays scan settings without scanning
-R	--reset	Resets scan database
-s	--sync	Performs a synchronization scan (and implies -R)
-T	--send <file>	Sends <file> to the core
-t	--mini	Performs a mini scan
--v	--version <n>	Reports formatted version information (1,2, or 3)
-V	--Verbostiy <n>	Sets verbosity level (debugging)

Editing the LDAPPL3.TEMPLATE file

The LDAPPL3.TEMPLATE file contains the scanner's inventory parameters. This template file works with the LDAPPL3 file to identify a device's software inventory.

You can edit the template file's [LANDesk Inventory] section to configure the parameters that determine how the scanner identifies software inventory. By default, LDAPPL3.TEMPLATE is located in this directory on the core server:

- \Program Files\LANDesk\ManagementSuite\LDLogon

Use this table as a guide to help you edit the [LANDesk Inventory] section in a text editor.

Option	Description
MacMode	Determines how the scanner scans for Macintosh software on devices. The default is All. Here are the settings: • **Listed:** Records the files listed in LDAPPL3. • **Unlisted:** Records the names and dates of all files that have the extensions listed on the MacScanExtensions line but that are not defined in the LDAPPL3. This mode helps discover unauthorized software on the network. • **All:** Discovers files with extensions listed on the MacScanExtensions line.

You need to click **Make available to the clients**, so they can download the MacModes. MacScanExtensions is turned on by default. This can create very large scan files (11 MB+), so you may want to change these defaults.

Note: The /Library or /System directories are not scanned in a MacScanExtensions scan by default. This reduces the size of the scan file. The directories can be placed in the Mac folder include section.

Scanning for custom data

For information on scanning for custom data, see Scanning for custom data on Macintosh devices

Remote control for Macintosh devices

You can remote control a Macintosh device from the console the same way you would a Windows device. Before you can perform any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see the connection messages and status in the **Connection messages** pane (**View > Connection messages**). The Management Suite integrated security checks to see if the user initiating the remote control session has the appropriate rights and that the machine is part of the user's scope. The data is obfuscated as it is passed over the network.

Note: Integrated security is turned on by default.

Macintosh keyboards have some keys that PC keyboards don't have. When remote controlling a Macintosh device, the following keys are used on the PC keyboard to emulate a Macintosh keyboard:

- The Alt key maps to the Command key.
- The Windows key maps to the Option key.

You need to have system key pass-through enabled in the remote control viewer window for the Alt and Windows keys to pass their Macintosh mappings.

Note: Clipboard sharing and draw features are not supported on Macintosh devices.

For more information, see Using remote control.

Connecting to a device

You can connect to a Macintosh device and remote control it.

To connect to a device

1. In the **Network view**, right-click the device you want to remote control, and then click **Remote control**, **Chat**, **File transfer**, or **Remote execute**.
2. Once the viewer window appears and connects to the remote device, you can use any of the remote control tools available from the **Tools** menu, such as chat, file transfer, reboot, inventory, or remote control.
3. To end a remote control session, click **File > Stop connection**.

Command line remote control

You can remote control a Mac machine from the command line on a machine that has the remote control container installed. Use the following command:

```
irccntr.exe /a[client name] /s[core name]
```

Remote control features

The inactivity timeout specifies a period of time (10 minutes by default), after which, if the client hasn't received mouse or key moves, the session is terminated. Similar to a screen saver, it prevents others from using the remote computer if it is left unattended.

Software Distribution for Macintosh devices

Software distribution lets you deploy software and file packages to Macintosh running OS X on your network.

You can distribute single-file executable packages to Mac OS X devices. Each distributed package consists of only one file, and the agent will try to install the file once the device receives it. Any file can be downloaded. Install packages (.PKG) can also contain directories, but they must be compressed. If the file downloaded has a suffix of .DMG, .PKG, .MPKG, .SIT, .SITX, .ZIP, .TAR, .GZ, .SEA, .APP, .SH, .HQX, or for Automator/workflow packages, LANDesk will decompress the file before returning (Automator packages will only work on versions 10.4.2 or later).

Note: Users should make sure that Stuffit Expander has its "check for new versions" option disabled; otherwise a dialog may interrupt the software distribution execution.

Software distribution also provides the ability to distribute shell scripts as jobs. This enables IT to take even greater control over the Mac operating environment and perform nearly any configuration or information gathering task on a Mac OS X device.

You can schedule Mac OS X distributions in the Scheduled tasks window and drag Mac OS X devices into the Scheduled tasks window as distribution targets (see Scheduled tasks for Macintosh devices).

Note: You must install the LANDesk Mac OS X agent on the target devices before you can distribute files to them.

A distribution package consists of the package files you want to send and distribution details, which describe the package components and behavior. You must create the package before it can be delivered and run. The following instructions explain how to perform software distribution. In order to execute it correctly, the software distribution package must exist on either a network or Web server and the recipient devices must have the software distribution agent installed.

There are three main steps required to distribute a package to devices:

1. Create a distribution package for the software you want to distribute
2. Create a delivery method
3. Schedule a software distribution task

To create a distribution package

1. Create the package you want to distribute.
2. Click **Tools > Distribution > Distribution Packages**.
3. Under **My distribution packages**, **Public distribution packages**, or **All distribution packages**, right-click **Macintosh** and select **New distribution package**.
4. In the **Distribution package** dialog, enter the package information and set the options. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your distribution appears under the tree item for the package type you selected.

To create a delivery method

1. If you've already configured a delivery method that you want to use, skip to the next procedure (To schedule a software distribution task).
2. Click **Tools > Distribution > Delivery Methods**.
3. Right-click the delivery method you want to use and then click **New delivery method**.
4. In the **Delivery method** dialog, enter the delivery information and change the options you want. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the delivery method you selected.

To schedule a software distribution task

1. Click **Tools > Distribution > Scheduled Tasks**.
2. Click the **Create software distribution task** toolbar button.
3. On the **Schedule task** page, enter the task name and the task schedule.
4. On the **Delivery Methods** page, select the delivery method you want to use.
5. On the **Distribution package** page, select the package script you created.
6. On the **Target machines** page, add the devices you want to receive the package.
7. On the **Summary** page, confirm the task is configured correctly.
8. Click **OK** when you're done.

View the task progress in the Scheduled tasks window.

You can use queries to create a list of devices to deploy a package to. For information on creating queries, see Database queries.

Macintosh software distribution commands

Macintosh software distribution commands are download commands, as opposed to a shell command (see Managed scripts for Macintosh devices). Download commands begin with either "http://" or "ftp://". If it's not a download command, it's a shell command by definition. The following is an example of a download command:

```
REMEXEC0=http://...
```

A download command won't autorun any files. After downloading the file to devices, you can follow up with a shell command to execute the file. Files are downloaded to /Library/Application Support/LANDesk/sdcache/, which you need to be aware of in your shell commands.

Note: If you're hosting files on a Windows 2003 server, you need to create MIME types for the Macintosh file extensions, such as .SIT, otherwise the 2003 server won't let you access the files. The MIME type doesn't have to be valid, it just needs to exist.

Configuring policies for Macintosh devices

You can also create Macintosh device policies. Creating a Macintosh device policy is similar to creating a policy for a Windows-based device. Macintosh devices also have the same required, recommended, and optional policy types. Macintosh application packages must be a single-file format. Policy-based management will check for policy updates at an interval of four hours. For optional or recommended policies, the client user needs to launch the LANDesk preference pane and click **Check now** for policy-based distribution. When targeting policies, Macintosh devices don't support policy-based management by user name, only by device name.

Policy-based management does the following with Macintosh application policy packages:

1. Downloads files to /Library/Applications/LANDesk/sdcache (just like software distribution downloads).
2. If the download is compressed, policy-based management will decompress it in place.
3. If the download is a disk image, policy-based management will mount it, look for the first Apple Package Installer file found on the mounted volume, run it silently, and then un-mount it.
4. If the download is an Apple Package Installer file, policy-based management will run it silently.

Also, policy-based management does support .DMG files with EULAs.

Note: Some package types don't work well with software distribution. (Installer Vise and Installer Maker installers don't work well with policy-based management. They almost always require user interaction and can be canceled.)

To add a Macintosh client policy

1. Click **Tools > Distribution > Delivery methods**.
2. Configure a policy-supported push or policy delivery method for the package you want to distribute.
3. Click **Tools > Distribution > Scheduled tasks**.
4. Click the **Create software distribution task** button.
5. Configure the task. Click **Help** on each page if you need more information.

To refresh the local client policies

1. In the LANDesk agent application on the Macintosh device, click the **Delivery** icon.
2. Click **Check now** for application policy management.

To view installed policies

- In the Management Suite Preference Pane on the Macintosh device, click the **APM** tab.

Exposing the UI to the client

You have the option of showing or hiding the UI to the client when distributing a software package. If the LANDesk administrator is pushing out a package that requires the user to select a license agreement, the package needs to be installed using a user-controlled type delivery method because the package will not install if the license agreement is not accepted by the end user. You can expose the UI for either a push- or policy-based delivery method.

To show the UI to the client during software distribution

1. Create a new software distribution delivery method or select an existing method to edit.
2. Select **Feedback** from the tree.
3. Select **Display progress to user** and then select **Display full package interface**.

Managed scripts for Macintosh devices

Management Suite uses scripts to execute custom tasks on devices. You can create scripts from the **Manage scripts** window (**Tools > Distribution > Manage scripts**). Macintosh scripts use shell commands to execute files. Shell commands run as root. The scripts are saved as text files, and you can edit them manually if you need to once they're created. The following is an example of a command:

```
REMEXEC0=/Library/Application\ Support/LANDesk/bin/ldscan
```

The user can use the shell command "open" to launch files and applications, or "installer" to install .PKG files. It's also possible for the download file to be a shell script written in Perl, Ruby, Python, and so on.

When files are downloaded, they are saved to /Library/Application Support/LANDesk/sdcache/, which you need to be aware of in order to execute some of your shell commands.

You can schedule Mac OS X managed scripts in the Scheduled tasks window and drag Mac OS X devices into the Scheduled tasks window as script targets (see Scheduled tasks for Macintosh devices).

Scheduled tasks for Macintosh devices

The scheduled tasks tool activates or starts many of the tasks you set up or configure in the application. These tasks can be run immediately, scheduled to occur at a later time, or configured to run on a regular basis. For more information, see Scripts and tasks.

Note: Before you can schedule tasks for a device, it must have the standard LANDesk agent installed and be in the inventory database.

The following procedures require the use of the scheduled tasks tool:

- Agent configuration deployment
- Software distribution
- Managed scripts
- Operating system deployment
- Security and patch manager

Reporting for Macintosh devices

The reporting tool lets you generate a wide variety of specialized reports that provide critical information about the Macintosh devices on your network. The reporting tool operates the same way for all operating systems. For more information, see Reports.

Software license monitoring for Macintosh devices

Macintosh devices running Mac OS X support software license monitoring. With each inventory scan, the Macintosh software monitoring agent sends information to the core server about the applications that devices run. The Software license monitoring window shows Macintosh applications along with Windows applications.

You can scan for files based on their extensions. The LDAPPL3.INI file contains the list of extensions to scan for. By default, .DMG and . PKG file types are scanned for. You can insert additional extensions into the LDAPPL3.INI file, which is located in the **/Library/Applications/System/User** folders by default. The file location can be changed as well. You can also use the LDAPPL3.INI file to scan for multimedia files.

The LANDesk agent application can be used to show applications that have been launched and how often they have been used.

Blocking applications for Macintosh devices

You can use the Management Suite Patch and compliance tool to block applications on managed Macintosh devices. This functionality works the same way as it does for Windows devices, except that no pre-defined blocked content is available for Macintosh devices. In order to block specific applications, you will need to create a custom definition for each blocked application using the procedure outlined in Creating custom definitions and detection rules. When creating the custom definition, be sure to check **Apply to Mac**.

Note: You can block only .APP files on managed Macintosh devices.

Patch and compliance for Macintosh devices

Patch and compliance is a complete, integrated security solution that helps you protect your Macintosh devices from a wide range of prevalent security risks. The tool allows you to manage security and patch content, scan devices, use patches, and remediate devices.

Configuring Macintosh devices for security scanning and remediation

Security functionality is included as part of the standard LANDesk agent for Macintosh devices. It allows you to scan managed Macintosh devices for vulnerabilities, and perform remediation by deploying patches or software updates.

Launching the scanner for Macintosh devices

You can launch the scanner from the console or manually on the client machine.

To launch the security scanner

1. Open the Mac OS X **System Preferences** on the target device and select the **LANDesk Client** panel.
2. On the **Overview** tab, click **Check Now** in the Security and Patch Manager section.

Operating system deployment for Macintosh devices

You can use operating system deployment with the LANDesk agent for Macintosh by utilizing NetBoot/NetInstall as part of Mac OS X Server. For information, download the operating system deployment for Macintosh white paper from http://community.landesk.com/support/docs/DOC-1192.

Using the Mac remote control viewer

Use the remote control viewer to remotely access a device. You can only remote control Windows and Mac devices that have the LANDesk agent installed. During a remote control session, you will have the same rights and privileges as the logged-in user on the remote device. You can do anything at the remote device that the user sitting at it can do.

Once you've taken control of a remote device, its screen appears in the viewer window. Because the viewer window often isn't as big as the remote device’s screen, you’ll either need to use the scroll bars to scroll up, down, and side to side, or use the **Scale** feature to rescale the remote screen representation so it fits in the viewer window. Scaling reduces the image quality, and if the scaler has to reduce the screen size too much you may have a hard time reading text.

You can also increase the viewer window displayable area by disabling items in the **Session** menu, such as the chat and log panes or the toolbar. Use the **Session** menu's **Full screen** option to completely remove the viewer window's controls. If the remote screen's resolution exceeds yours, it will be scaled to fit your monitor.

If you want to speed up the viewing rate or change the viewer window settings, use the **LANDesk Remote Control** menu's **Preferences** option to display the **Options** dialog.

Read the following sections for more information:

- Connecting to devices
- Chatting with remote devices
- Sending special key sequences
- Using remote control without viewing the remote screen
- Customizing remote control

Connecting to devices

Before you can do any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see connection messages and status in the log pane, if that is visible. If it isn't, you can display it by clicking **Session > Show log**.

If you want to start a new session, click **File > New**. To stop a session, click **File > Close**. If the **Session** menu options are dimmed, you aren't connected to a device.

Chatting with remote devices

You can use the remote control viewer to remotely chat with a user at a remote device. This feature is useful if you need to give instructions to a remote user whose dial-up connection is using the only available phone line. Users can respond back using the chat window that appears on their screen. You can only use chat on devices that have the LANDesk Agent for Mac installed. This feature works even if you’re not viewing a remote device's screen.

If you want to save the messages from a chat session, you can. Any text appearing in the gray area of the chat session will be saved to a text file.

To chat with a user at a remote device

1. Once you're connected to a remote device, click **Session > Show chat**.
2. A chat frame appears on the right side of the viewing window. The top section shows sent and received messages. The bottom section is where you can type your message. Press enter to send a message you've typed.

Your message will appear on the remote device's screen. A user can respond by typing a message and clicking **Send**. The user also can click **Close** to exit out of a chat session.

To save messages from a chat session

1. In the chat area of the viewer window, click **Save messages**.
2. In the **Save as** dialog, type in a filename and click **Save**.

Sending special key sequences

You can send special key sequences such as Alt-Tab to remote devices. You need to use a menu item to send these key sequences to prevent your local OS from intercepting them.

Once you're connected to a remote device, click Session and click the special key sequence you want. The available special key sequences vary, depending on the operating system you're remote controlling.

- Send Alt-Tab
- Send Ctrl-Esc
- Send Ctrl-Alt-Del
- Send Command-Tab

Using remote control without viewing the remote screen

If you don't want to see the remote device's screen but you still want to be able to chat with a user at the remote device, you can stop observation.

To stop observing a remote device but still maintain a remote control connection

1. Once you've connected to a remote device, click **Session > Don't observe**. You can still use the chat feature with the device.
2. Click **Session > Observe** to restore the remote view.

Customizing remote control

You can customize these remote control options:

- Change remote control settings
- Optimize remote control performance
- Customize the toolbar

Changing remote control settings

Use the **Options** dialog's **Change settings** tab (**LANDesk Remote Control > Preferences**) to adjust the remote control settings.

- **Lock out the remote keyboard and mouse:** Locks the remote device's keyboard and mouse so that only the user running the viewer can control the remote device. Note that special key combinations in Windows such as "Ctrl-Alt-Del" or the "Windows Key+L" aren't locked out.
- **Blank the remote computer screen:** Blanks the remote device's screen so only the user running the viewer can see the user interface display on the remote device.
- **Write log entries to Remote.log:** If you want to save a log of remote control actions in a log file on the remote device, check this option. You can choose from three logging levels, with level 1 being the least detailed and level 3 being the most detailed. Level 1 is the default level.

Optimizing remote control performance

Use the **Options** dialog's **Optimize performance** tab **(LANDesk Remote Control > Preferences)** to optimize remote control performance.

Changing the optimization setting dynamically adjusts color reduction, wallpaper visibility, and remote windows appearance effects (the ones you can adjust in Windows **Display Properties > Appearance > Effects**), such as transition effects for menus and tool tips.

Remote control always uses a highly efficient compression algorithm for remote control data. However, even with compression, it requires a lot of data to send high color depth information. You can substantially reduce the amount of remote control data required by reducing the color depth displayed in the remote control viewer. When the viewer reduces the color depth, the viewer has to map the full color palette from the remote desktop to a reduced color palette in the viewer. As a result, you may notice colors in the remote control window that don't accurately reflect the remote desktop. If that's a problem, select a higher-quality compression setting.

Another way you can optimize performance is to **Suppress remote wallpaper**. When you do this, remote control doesn't have to send wallpaper updates as parts of the remote desktop are uncovered. Wallpaper often includes bandwidth-intensive images, such as photographs. These don't compress well and take time to transfer over slower connections.

Customizing the remote control toolbar

You can customize which buttons appear on the remote control toolbar.

To customize toolbar buttons

1. Click **Session > Customize toolbar**.
2. Drag buttons you want from the palette onto the viewer window.
3. Drag buttons you don't want from the viewer window to the palette.
4. To restore the default button layout, drag the default set at the bottom of the palette onto the viewer window.

You can change the button size by clicking **Use small size**. You can also use the **Show** option to show icons only, text only, or both icons and text.

Patch and Compliance

Patch and Compliance is a complete, integrated security management solution that helps you protect your LANDesk managed devices from a variety of prevalent security risks and exposures.

Patch and Compliance provides all the tools you need in order to download the most common types of security content updates (such as vulnerabilities, spyware, configuration security threats, virus definition (pattern) files, and unauthorized applications) from LANDesk security services. You can download associated patch files, and configure and run security assessment and remediation scans on your managed devices. You can also create your own custom definitions to scan for and remediate specific, potentially harmful conditions on devices. If any security risks are detected, Patch and Compliance provides a variety of methods to remediate affected devices. Additionally, at any time you can view detailed security information for scanned devices, and generate specialized patch and compliance reports.

All of these enterprise security management tasks can be performed from the convenience of a single console.

Additionally, Patch and Compliance lets you scan managed devices, and core servers and console machines, for versions of installed LANDesk software and deploy the appropriate LANDesk software updates.

About LANDesk Security Suite
The Patch and Compliance tool is the main security management component of LANDesk Security Suite. Security Suite is based on much of the primary LANDesk Management Suite functionality, supplemented with specialized security management tools such as the Patch and Compliance, Antivirus, Endpoint Security (HIPS, Firewall, Device Control), and more. The Patch and Compliance tool offers the same features in Management Suite and Security Suite and is described in detail in this section. For more information on which basic LANDesk functionality is supported in Security Suite, see the LANDesk Security Suite *Users Guide*.

Read this section to learn about:

Looking ahead: What to do after configuring devices for security scanning and remediation

Once you understand Patch and Compliance concepts, how to navigate the user interface, and the general task workflow; and after you've configured devices to work with Patch and Compliance, you can perform the following patch and compliance management tasks:

- Download security content updates and patches
- View security content definition and detection rule properties
- Create custom vulnerability definitions

- Scan managed devices for security risks
- Remediate affected devices
- Enable security alerts
- Generate security reports

For detailed information on performing these tasks, see "Managing security content and patches" on page 315, and "Scanning and remediating devices" on page 332.

Patch and Compliance overview

Patch and Compliance provides all of the tools you need to establish system-wide security across your network. With Patch and Compliance, you can automate the repetitive processes of maintaining security content, and organizing and viewing that content.

Use security scan tasks and policies to assess managed devices for known platform-specific vulnerabilities. You can download and manage patch executable files. Finally, you can remediate detected vulnerabilities by deploying and installing the necessary patch files, and verify successful remediation.

Additionally, you can create your own custom vulnerability definitions in order to scan managed devices for specific OS and application conditions that might threaten the operation and security of your system. Custom definitions can be configured for detection only or to do both detection and remediation. For more information, see "Creating custom definitions and detection rules" on page 324.

New features

Patch and Compliance offers several new capabilities, such as:

- Use the change settings task to change/update only the device agent configuration settings you want to, including : 802.1X support settings, compliance security settings, configure Windows firewall settings, custom variable override settings, HIPS settings, LANDesk Antivirus settings, and security scan and repair settings. With the change settings task you can change desired settings without a full device agent configuration deployment.
- Configure global alert settings.
- Scan for the presence of spyware on your managed devices. If spyware is detected, you can schedule a repair job that removes the spyware from affected devices.
- Deny launch of unauthorized or prohibited applications on end user devices with blocked application definitions.
- Enable real-time spyware monitoring (detection and removal), and real-time application blocking.
- Scan managed devices for security threats (Windows system configuration errors and exposures) on the local hard drive. Once a security threat is identified, you can perform the necessary fix manually at the affected device.
- Use specific security threat definitions that detect the Windows firewall, turn it on or off, and configure the firewall settings.
- Use custom variables that are included with other security threat definitions in order to customize and change specific local system configurations, and to enforce enterprise-wide system configuration policies.
- Receive alerts when specified vulnerabilities are detected on managed devices by a security scan. You can configure alerting by definition severity.
- Implement frequent security scans for critical, time-sensitive security risks such as virus scanning.
- Use vulnerability dependency relationships to identify which patches need to be installed before other vulnerabilities can adversely affect managed devices or before

they can be remediated. Supercedence information describes patches that have been replaced by more recent versions and that don't need to be applied.

- Verify the latest LANDesk software is installed on your managed devices, as well as core servers and console machines, by scanning for LANDesk software updates. If an outdated version is detected on a device, you can schedule a repair job the deploys and installs the latest LANDesk software update.

Features

With Patch and Compliance, you can:

- Provide patch security for international versions of the operating systems on your network, including current support for the following languages: Czech, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Simplified Chinese, Spanish, Swedish, and Traditional Chinese.
- Organize and group security definitions to perform customized security assessment scans and remediation (see "Tree view" on page 304).
- Assess vulnerabilities and other security risks on a variety of supported device platforms, including Windows, Sun Solaris, and Linux (see "Scanning devices for security risks" on page 332).
- View patch and compliance information for scanned devices (see "Viewing security content" on page 319).
- Schedule automatic patch management tasks, including content updates, device scans, and patch downloads.
- Perform remediation as a scheduled task, a policy, or automatically with the Auto Fix feature (see "Remediating devices that detected security risks" on page 342).
- Download, deploy, and install patches that have been researched and verified (see "Downloading patches" on page 322).
- Track the status of patch deployments and installation on scanned devices.
- Use LANDesk's Targeted Multicast, peer download, and checkpoint restart features for fast and efficient patch deployment.
- Generate and view detected an extensive variety of patch and compliance management-specific reports (see "Using patch and compliance reports" on page 354).

Security content types and subscriptions

When you install LANDesk Management Suite, the Patch and Compliance tool is now included by default (previously, it was a separate add-on). However, without a Security Suite content subscription, you can only scan for LANDesk software updates and custom definitions. A Security Suite content subscription enables you to take full advantage of the Patch and Compliance tool by providing access to additional security content (definition types).

LANDesk Security Suite content types include:

- Antivirus updates (for third-party scanners, includes antivirus scanner detection content only; for LANDesk Antivirus, includes both scanner detection content AND virus definition files)
- Blocked applications (see the "Legal disclaimer for the blocked applications type" on page 314)
- Custom vulnerability definitions
- Driver updates
- LANDesk software updates
- Security threats (system configuration exposures; includes firewall detection and configuration)
- Software updates

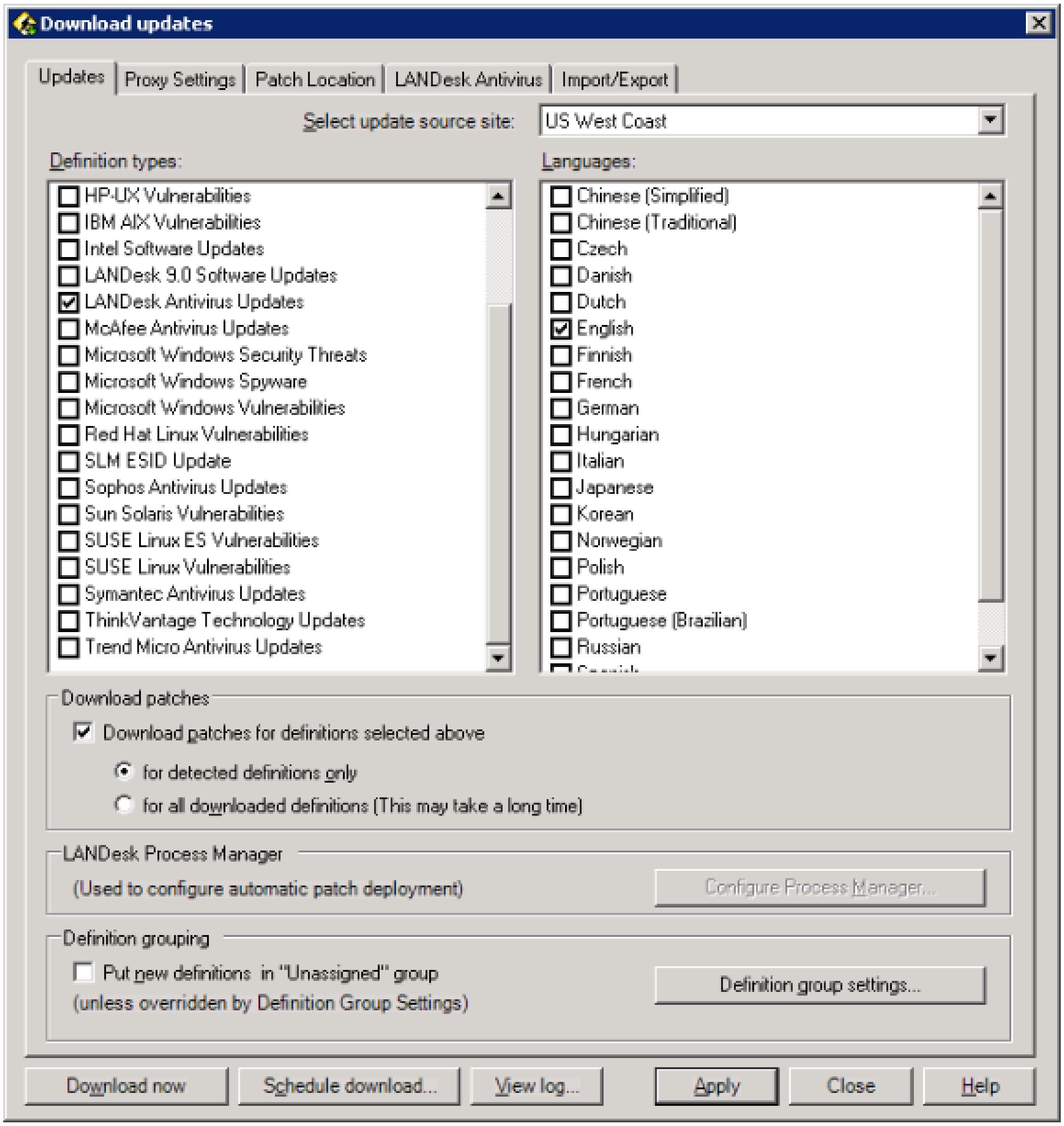
- Spyware
- Vulnerabilities (known platform- and application-specific vulnerabilities)

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

The LANDesk User Community has user forums and best known methods for many LANDesk products and technologies. To access this valuable resource, go to: http://community.landesk.com

Using Download Updates

Note that the **Updates** page of the **Download updates** dialog includes several security content types in the definition types list.



Select update source site: US West Coast

Definition types:

- ☐ HP-UX Vulnerabilities
- ☐ IBM AIX Vulnerabilities
- ☐ Intel Software Updates
- ☐ LANDesk 9.0 Software Updates
- ☑ LANDesk Antivirus Updates
- ☐ McAfee Antivirus Updates
- ☐ Microsoft Windows Security Threats
- ☐ Microsoft Windows Spyware
- ☐ Microsoft Windows Vulnerabilities
- ☐ Red Hat Linux Vulnerabilities
- ☐ SLM ESID Update
- ☐ Sophos Antivirus Updates
- ☐ Sun Solaris Vulnerabilities
- ☐ SUSE Linux ES Vulnerabilities
- ☐ SUSE Linux Vulnerabilities
- ☐ Symantec Antivirus Updates
- ☐ ThinkVantage Technology Updates
- ☐ Trend Micro Antivirus Updates

Languages:

- ☐ Chinese (Simplified)
- ☐ Chinese (Traditional)
- ☐ Czech
- ☐ Danish
- ☐ Dutch
- ☑ English
- ☐ Finnish
- ☐ French
- ☐ German
- ☐ Hungarian
- ☐ Italian
- ☐ Japanese
- ☐ Korean
- ☐ Norwegian
- ☐ Polish
- ☐ Portuguese
- ☐ Portuguese (Brazilian)
- ☐ Russian
- ☐ Spanish

Download patches

☑ Download patches for definitions selected above

● for detected definitions only

○ for all downloaded definitions (This may take a long time)

LANDesk Process Manager

(Used to configure automatic patch deployment) [Configure Process Manager...]

Definition grouping

☐ Put new definitions in "Unassigned" group
(unless overridden by Definition Group Settings) [Definition group settings...]

Scanning and remediation functions are not the same for these various content types. For more information on how Patch and Compliance scans for and remediates detected security risks on managed devices, see the appropriate sections in "Scanning and remediating devices" on page 332.

Supported device platforms

Patch and Compliance supports most of the standard LANDesk-managed device platforms, including the following operating systems:

- Windows NT 4.0 (SP6a and higher)
- Windows 2000 Professional (SP4)
- Windows 2003 Servers
- Windows XP Professional (SP1/SP2)
- Windows Vista
- Mac OS X (10.2.x, 10.3.x, and 10.4.x)
- Red Hat Linux 9 (scanning from the console; manual remediation)
- SUSE Linux (scanning from the console; manual remediation)
- Sun Solaris (scanning from the console; manual remediation)

For information on configuring managed devices for security scanning, see "Configuring devices for security scanning and remediation" on page 309 later in this section.

Scanning core servers and consoles for LANDesk software updates is supported
You can also scan LANDesk core servers and consoles for LANDesk software updates, but those machines must first have the standard LANDesk agent deployed, which includes the security scanner agent required for security scanning tasks.

Role-based administration with Patch and Compliance

Patch and Compliance uses role-based administration to allow users access to features. Role-based administration is the access and security framework that lets LANDesk Administrators restrict user access to tools and devices. Each user is assigned specific roles and scope that determine which features they can use and which devices they can manage.

Administrators assign these roles to other users with the Users tool in the console. Patch and Compliance is a specific right that appears under the Security rights group in the Roles dialog. In order to see and use the Patch and Compliance tool, a user must be assigned the necessary Patch and Compliance right.

IMPORTANT: LANDesk Script Writers group permission required
In order to create scheduled tasks and policies in the Patch and Compliance tool and the Security Configurations tool (for security and compliance scan tasks, repair tasks, and change settings tasks), a user must have the LANDesk Script Writers group permission. In other words, they must belong to a group that has the LANDesk Script Writers permission assigned. For more information about role-based administration, see "Role-based administration" on page 44.

With the Patch and Compliance right, you can provide users the ability to:

- See and access the Patch and Compliance tool in the Tools menu and Toolbox
- Configure managed devices for security assessment, compliance, and remediation scanning
- Configure devices for real-time spyware and blocked application scanning
- Configure devices for high frequency scanning for critical security risks
- Download security updates and associated patches for the security types for which you have a Security Suite content subscription
- Create scheduled tasks that automatically download definitions and/or patch updates
- Create custom vulnerability definitions and custom detection rules

- Import, export, and delete custom definitions
- View downloaded security content by type (including: all types, blocked applications, custom definitions, LANDesk updates, security threats, spyware, vulnerabilities, driver updates, and software updates)
- Customize selected security threats with custom variables
- Edit custom variable values (for security content types with custom variables, such as security threats)
- Add and remove security definitions from the Compliance group
- Change the status of definitions contained in the Compliance group
- Configure and run security and compliance scans on managed devices as a scheduled task or as a policy
- Divide a scheduled task scan into a staging phase and a deployment phase
- Create and configure scan and repair settings that determine the scan options, such as: content type to be scanned for, scanner information and progress display, device reboot behavior, and the amount of end user interaction. Then, apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks
- View detailed scan results by: detected group, specific definition, individual device, or a group of selected devices
- Perform remediation as a scheduled task or as a policy
- Use Auto Fix to automatically remediate the following security types if they are detected: vulnerabilities, spyware, LANDesk software updates, and custom definitions (must also be a LANDesk Administrator)
- Track and verify the status of patch deployment and installation (repair history on scanned devices)
- Purge unused security type definitions (must be a LANDesk Administrator)
- Uninstall patches from scanned devices
- Remove patches from the core database
- Configure vulnerability alerts
- Generate a variety of security specific reports (also requires Reporting roles)

Patch and compliance task workflow

The following steps provide a quick summary outline of the typical processes involved in implementing patch and compliance management on your LANDesk network. Each of these procedures are described in detail in subsequent sections.

Basic steps in implementing and using patch and compliance management:

1. Configure managed devices for security and compliance scans and remediation.
2. Download security content (vulnerability and other security risk definitions) from a security content server (updated from industry/vendor data sources). Also, create custom definitions.
3. Organize and view security content.
4. Create security and compliance scan tasks.
5. Configure scan and repair settings to determine scan operation and define security compliance policies.
6. Scan for vulnerabilities, spyware, security threats, blocked applications, etc.
7. View scan results for scanned devices.
8. Download patches that will remediate detected vulnerabilities.
9. Repair detected vulnerabilities by deploying and installing patches to affected devices
10. Repair other detected security risks and exposures.

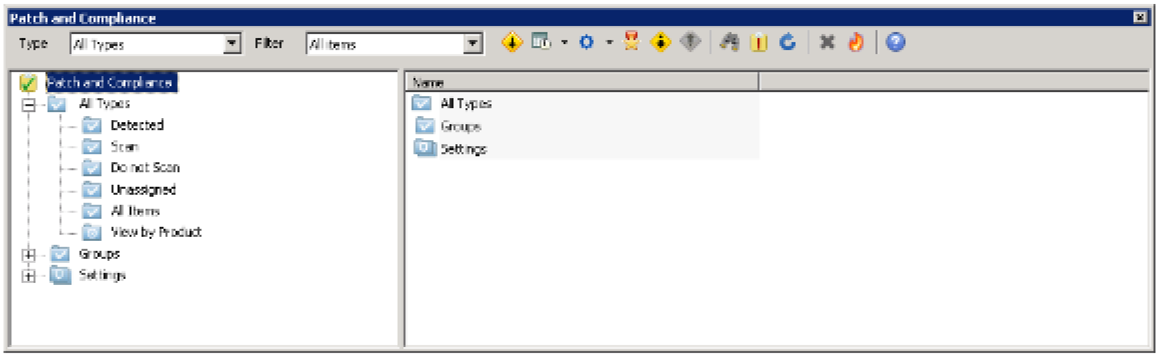
11. View patch installation status and repair history information.

Understanding and using the Patch and Compliance tool

The Patch and Compliance tool window, like all other LANDesk tools, is opened from either the **Tools** menu or the **Toolbox** and can be docked, floated, and tabbed with other open tool windows (see "Dockable tool windows" on page 23).

Patch and Compliance right
In order to see and access the Patch and Compliance tool, users must have either the LANDesk Administrator right (implying full rights), or the specific Patch and Compliance right. For more information about user roles and rights, see "Role-based administration" on page 44.

To open the Patch and Compliance tool, click **Tools > Security > Patch and Compliance**.



The Patch and Compliance window contains a toolbar and two panes. The left-hand pane shows a hierarchical tree view of security type definition and detection rule groups. You can expand or collapse the objects as needed.

The right-hand pane displays a column list of the selected group's definition details or detection rule details, depending upon which group you've selected in the left-hand pane, plus a **Find** feature for searching in long item lists.

Characters not allowed when searching a list
In the **Find** box, the following extended characters are not supported: <, >, ', ", !

The Patch and Compliance tool window contains a toolbar with the following buttons:

Toolbar buttons

- **Download updates:** Opens a dialog where you can specify the platforms and languages for the security content types you want to update, as well as which security content server to access. You can also configure whether to place definitions in the Unassigned group, whether to download associated patches concurrently, the location where patches are downloaded, and proxy server settings.
- **Create a task:** Includes a drop-down list where you can select which type of task you want to create:
  - **Security scan:** Lets you create a security scan task, specify whether the scan is a scheduled task or a policy, and select a scan and repair settings that determines whether the security scanner displays, reboot and interaction behavior, and the content types scanned for.
  - **Compliance scan:** Lets you create a security scan task that specifically checks target devices for compliance with your current security policy as defined in LANDesk Network Access Control settings and by the contents of the Compliance group. You can also specify whether the compliance security scan runs as a scheduled task (including which devices to scan and whether to scan immediately) or as a policy.

  - **Change settings:** Lets you create a task that changes the default settings on a managed device by writing the specified settings ID to the local registry. With a change settings task you can change one or more of these settings: 802.1X support settings, compliance security settings, configure Windows firewall settings, custom variable override settings, HIPS settings, LANDesk Antivirus settings, and security scan and repair settings. You can use this task as a quick and convenient way to change only the settings you want to without having to redeploy a full device agent configuration.
  - **Reboot:** Lets you create a device reboot task, specify whether the reboot is a scheduled task or a policy, and select a scan and repair settings that determines display and interaction behavior. Note that only the options on the reboot page of the dialog apply to this task.
  - **Repair:** Lets you create a security repair task that remediates detected security exposures on scanned devices. You can configure the repair as a scheduled task or as a policy or both, divide the repair task into separate staging and repairing phases, select a scan and repair settings, and download patches. Note that one or more repairable security definitions must first be selected in order to create a repair task.
  - **Gather historical information:** Lets you create a task that gathers the current scanned and detected counts (for a specified number of days) that can be used for reporting. You can also create and configure a scheduled task that performs the same action.
- **Configure settings:** Includes a drop-down list where you can select which type of settings you want to configure, change, or update:
  - **Scan and repair settings:** Lets you create, edit, copy, and delete scan and repair settings. Scan and repair settings determine whether the security scanner displays on devices while running, reboot options, user interaction, and the content types scanned.
  - **Compliance settings:** Lets you create, edit, copy, and delete compliance settings. Compliance settings determine when and how a compliance security scan takes places, whether remediation occurs automatically, and what to do when LANDesk Antivirus detects a virus infection on target devices.
  - **Custom variable override settings:** Lets you create, edit, apply, and delete scan and repair settings. Custom variables overrides allow you to configure exceptions to custom variable values. In other words, with custom variable override settings you can ignore or bypass a specific custom variable condition so that a scanned device is not determined to be vulnerable.
  - **Definition group settings:** Lets you create, edit, copy, and delete Definition group settings to automate security content downloads.
  - **Alert settings:** Lets you configure global security alerts.
  - **Rollup core settings:** Lets you create and manage rollup core settings. Rollup core settings determine automatic forwarding of the latest security scan results to a rollup core server on your network. Security scan data forwarding allows you to view real-time vulnerability status for all of your managed devices in a large, distributed enterprise network without having to manually retrieve that data directly from the primary core server.
- **Create custom definition:** Opens a blank Definition properties dialog with editable fields where you can specify whether the custom definition is detection only or also allows remediation, enter specific vulnerability information, create detection rules, and identify the appropriate patch file for remediation.
- **Import custom definitions:** Allows you to import an XML file containing custom definitions.
- **Export selected custom definitions:** Allows you to export a custom definition as an XML file.

- **Scan information:** Lets you view detailed patch and compliance activity and status information, by categories such as recently scanned and definition severity, for all of your managed devices.
- **Computers out of compliance:** Lists devices that have been scanned to check for compliance with the predefined compliance security policy (based on the content of the Compliance group), and are determined to be unhealthy or out of compliance.
- **Refresh:** Updates the contents of the selected group.
- **Delete selected custom definitions:** Removes the selected custom definitions from the core database.
- **Purge patch and compliance definitions:** Lets you specify the platforms and languages whose definitions you want to remove from the core database. Note that only a LANDesk Administrator user can perform this operation.
- **Help:** Opens the online help to the Patch and Compliance section.

Type drop-down list

Use the **Type** drop-down list to determine which downloaded definitions display in the tree view. Definition types are designated by the publisher of the content. Filtering the display can be helpful if you want to see only one specific type of security content, or if you want to narrow down an extremely long comprehensive list.

The **Type** drop-down list includes the following options:

- All types (comprehensive list of all downloaded security definitions)
- Antivirus (lists downloaded scanner detection definitions only; does not list specific LANDesk Antivirus virus definition files)
- Blocked applications (lists downloaded blocked application definitions only)
- Custom definitions (lists user-defined vulnerability definitions only)
- Driver updates (lists downloaded driver update definitions only)
- LANDesk updates (lists downloaded LANDesk software updates only)
- Security threats (lists downloaded security threat definitions only)
- Software updates (lists downloaded software updates only)
- Spyware (lists downloaded spyware definitions only)
- Vulnerabilities (lists all downloaded vulnerability definitions for any of the available platforms)

The left pane of the Patch and Compliance window shows the following items:

Tree view

The root object of the tree view contains all of the security types such as vulnerabilities, spyware, security threats, blocked applications, and custom definitions groups (and associated detection rule groups, if applicable). The root object can be expanded and collapsed as needed.

All Types (or the currently selected type name)

Contains the following subgroups:

- **Detected:** Lists all of the definitions detected by security scans, for all of the devices included in the scans. The contents of this group are cumulative based on all the security scans run on your network. Definitions are removed from this group only by: being successfully remediated, being removed from the Scan group and running the scan again, or by actually removing the affected device from the database.

The Detected list is a composite of all detected security definitions found by the most recent scan. The Scanned and Detected columns are useful in showing how many devices were scanned, and on how many of those devices the definition was detected. To see specifically which devices have a detected definition, right-click the item and click **Affected computers**.

Note that you can also view device-specific information by right-clicking a device in the network view, and then clicking **Security and Patch Information**.

You can only move definitions from the Detected group into either the Unassigned or Don't Scan groups.

- **Scan:** (For the Blocked Applications type, this group is called **Block**.) Lists all of the security definitions that are searched for when the security scanner runs on managed devices. In other words, if a definition is included in this group, it will be part of the next scan operation; otherwise, it won't be part of the scan.

  By default, collected definitions are added to the Scan group during a content update. (**Important:** Except for blocked applications, which are added to the Unassigned group by default.)

  Scan can be considered one of three possible states for a security definition, along with Don't Scan and Unassigned. As such, a definition can reside in only one of these three groups at a time. A definition is either a Scan, Don't Scan, or Unassigned and is identified by a unique icon for each state (question mark (?) icon for Unassigned, red X icon for Don't Scan, and the regular vulnerability icon for Scan). Moving a definition from one group to another automatically changes its state.

  By moving definitions into the Scan group (click-and-drag one or more definitions from another group, except the Detected group), you can control the specific nature and size of the next security scan on target devices.

  Caution about moving definitions from the Scan group
  When you move definitions from the Scan to the Don't Scan group, the current information in the core database about which scanned devices detected those definitions is removed from the core database and is no longer available in either an item's Properties dialog or in a device's Security and Patch Information dialog. To restore that security assessment information, you would have to move the definitions back into the Scan group and run the same security scan again.

- **Don't scan:** (For Blocked Applications, this group is called **Don't Block**.) Lists all of the definitions that aren't searched for the next time the security scanner runs on devices. As mentioned above, if a definition is in this group, it can't be in the Scan or Unassigned group. You can move definitions into this group in order to temporarily remove them from a security scan.
- **Unassigned:** Lists all of the definitions that do not belong to either the Scan or Don't Scan groups. The Unassigned group is essentially a holding area for collected definitions until you decide whether you want to scan for them or not.

  To move definitions, click-and-drag one or more from the Unassigned group into either the Scan or Don't Scan groups.

  New definitions can also be automatically added to the Unassigned group during a content update by checking the **Put new definitions in the Unassigned group** option on the **Download updates** dialog.

- **All Items:** Lists all of the selected type's definitions in a flat list, even if you've moved a definition into either the Unassigned, Scan, or Don't Scan group.
- **View by Product:** Lists all of the definitions organized into specific product subgroups. These subgroups help you identify definitions by their relevant product category.

You can use these product subgroups to copy definitions into the Scan group for product-specific scanning, or copy them into a custom group (see below in order to perform remediation for groups of products at once).

Definitions can be copied from a product group into the Scan, Don't Scan, or Unassigned group, or any of the user-defined custom groups. They can reside in platform, product, and multiple custom groups simultaneously.

Groups

Contains the following subgroups:

- **Custom Groups:** Lists all of the subgroups you've created and the definitions they contain. My Groups provide a way for you to organize security definitions however you want. Use a group's contents to copy several definitions into the Scan group for customized scanning, or to create a repair job for several definitions at once.

  You can also use a custom group to define the contents of a security scan. Copy the definitions you want to scan for into a custom group and select that group in the Scan for option of the Scan and repair settings dialog

  To create a custom group, right-click **Custom Groups** (or a subgroup) and then click **New Group**.

  To add definitions to a custom group, click-and-drag one or more of them from any of the other definition groups. Or, you can right-click a custom group, and then click **Add Definition**.

- **Predefined:** Lists any predefined vulnerability definition groups as determined by the LANDesk security content subscription. For example, this group might contain industry published definitions such as the SANS Top 20, which are the top 20 vulnerability definitions identified and published by Microsoft. (These definitions are typically a subset of the Microsoft Windows Vulnerabilities that are downloaded with the **Download updates** dialog.)
- **Alert:** Lists all of the definitions that will generate an alert message the next time the security scanner run and devices.
- **Compliance:** Lists all of the definitions that are used to determine whether a managed (or mobile/guest device) is Healthy or Unhealthy. This group is used by LANDesk Network Access Control (NAC) to deny or allow access to the main network. The definitions and associated patch files contained in the Compliance group are copied to a special remediation server that scans devices, determines compliance or non-compliance, and can remediate non-compliant devices so that they can be granted full access to the corporate network.

Detection Rules

The Detection Rules group displays only for certain security content types.

Detection rules
These rules define the specific conditions (of the operating system, application, file, or registry) that a definition checks for in order to detect the associated security risk. Definitions (i.e., content types) that use detection rules include: vulnerabilities, security threats, and custom definitions. Spyware and blocked applications do not use detection rules.

The Detection Rules group contains the following subgroups:

- **Scan:** Lists all of the detection rules that are enabled for security scanning on devices.

  By default, detection rules associated with a definition of any security content type are added to the Detection Rules Scan group during a content update. Likewise, custom detection rules associated with a custom definitions are added to the Scan group when you create the custom definition.

Note that in addition to having a definition's detection rules enabled, its corresponding patch executable file must also be downloaded to a local patch repository on your network (typically the core server) before remediation can take place. The Downloaded attribute (one of the detail columns in the tool window's right-hand pane) indicates whether the patch associated with that rule has been downloaded.

- **Don't Scan:** Lists all of the detection rules that are disabled for security scanning on devices. Some definitions have more than one detection rule. By disabling a detection rule, you can ensure that it won't be used to scan for the conditions indicating that definition is present on devices. This can allow you to simplify a security scan without redefining the definition.
- **View by Product:** Lists all of the detection rules for collected definitions, organized into specific product subgroups. These subgroups help you identify detection rules by their relevant product category.

You can use these product subgroups to perform group operations.

Settings

The Settings group lets you view the various settings you've created for security scanning tasks. You can right-click any of the Settings groups to create a new settings and view the settings information in a report format.

Contains the following subgroups:

- **Scan and Repair:** Lists all of the scan and repair settings you've created that are used to determine the operation of the security scanner. Each scan and repair settings has a unique ID number. The right-hand pane shows useful information for the listed scan and repair settings.
- **Compliance:** Lists all of the compliance settings you've created that are used to determine the operation of the security scanner when performing a specific compliance scan. Each settings has a unique ID number. The right-hand pane shows useful information for the listed scan and repair settings.
- **Custom variables to override:** Lists all of the custom variable override settings you've created that are used to determine which modified custom variable values to ignore when the security scanner runs. Each settings has a unique ID number. The right-hand pane shows useful information for the listed settings.

Definition details

The right pane of the Patch and Compliance window displays detailed information listed in sortable columns for definition and detection rule items, as described below:

- **ID:** Identifies the definition with a unique, vendor-defined alphanumeric code.
- **Severity:** Indicates the severity level of the definition. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown.
- **Title:** Describes the nature or target of the definition in a brief text string.
- **Language:** Indicates the language of the OS or application affected by the definition.
- **Date Published:** Indicates the date the definition was published by the vendor.
- **Repairable:** Indicates whether the definition can be repaired through patch file deployment and installation. Possible values are: Yes, No, Some (for a definition that includes multiple detection rules and not all detected definitions can be fixed), and No rules (for a custom definition that doesn't include any detection rules).
- **Silent Install:** Indicates whether the definition's associated patch (or patches) installs silently, meaning without user interaction. Some definitions may have more than one patch. If any of a definition's patches don't install silently, the Silent Install attribute says No. To see how individual patches install, right-click the definition and click **Properties | Patches**.

- **Detected:** Displays the number of scanned devices that detected the definition.
- **Scanned:** Displays the number of devices scanned for the definition.
- **Auto Fix:** Indicates whether Auto Fix is enabled or disabled for the definition.
- **CVE ID:** (Applies only to vulnerabilities) Identifies a vulnerability by its unique CVE (Common Vulnerabilities and Exposures) name. For more information, see "Using CVE names" on page 330.

Using a definition shortcut menu

You can right-click an item to view more details with the **Properties** option.

A definition's shortcut menu also lets you do the following tasks (depending on the security type):

- Affected computers
- Computers that did not scan
- Download associated patches
- Autofix when scanning
- Add to Compliance group
- Add to Alert group
- Clear scan/repair status
- Repair
- Copy
- Properties
- Info
- Export
- Copy to other core(s)
- Auto sync

Detection Rule details

- **Name:** Displays the name of the detection rule (can be the file name of the patch executable).
- **ID:** Displays the ID of the definition associated with the rule.
- **Repairable:** Indicates whether the associated definition can be repaired through patch file deployment and installation.
- **Silent Install:** Indicates whether the rule's associated patch installs silently on devices without user interaction.
- **Reboot:** Indicates whether the associated patch file requires a system reboot in order to complete a successful remediation.
- **Auto Fix:** Indicates whether Auto Fix is enabled or disabled for the associated definition.
- **Downloaded:** Indicates whether the rule's associated patch executable file has been downloaded to the local repository.

Right-click a detection rule to view more details with the **Properties** option. The shortcut menu also lets you enable/disable the rule, download the associated patch, open the patch repository folder, and uninstall the patch.

Configuring devices for security scanning and remediation

Before managed devices can be scanned for vulnerabilities, spyware, security threats, and other security types, and receive patch deployments or software updates, they must have the security scanner agent installed (this agent is installed by default with the standard LANDesk agent).

This section includes information about configuring Windows devices for security scanning via an agent configuration, and information about configuring Linux, UNIX and Mac devices.

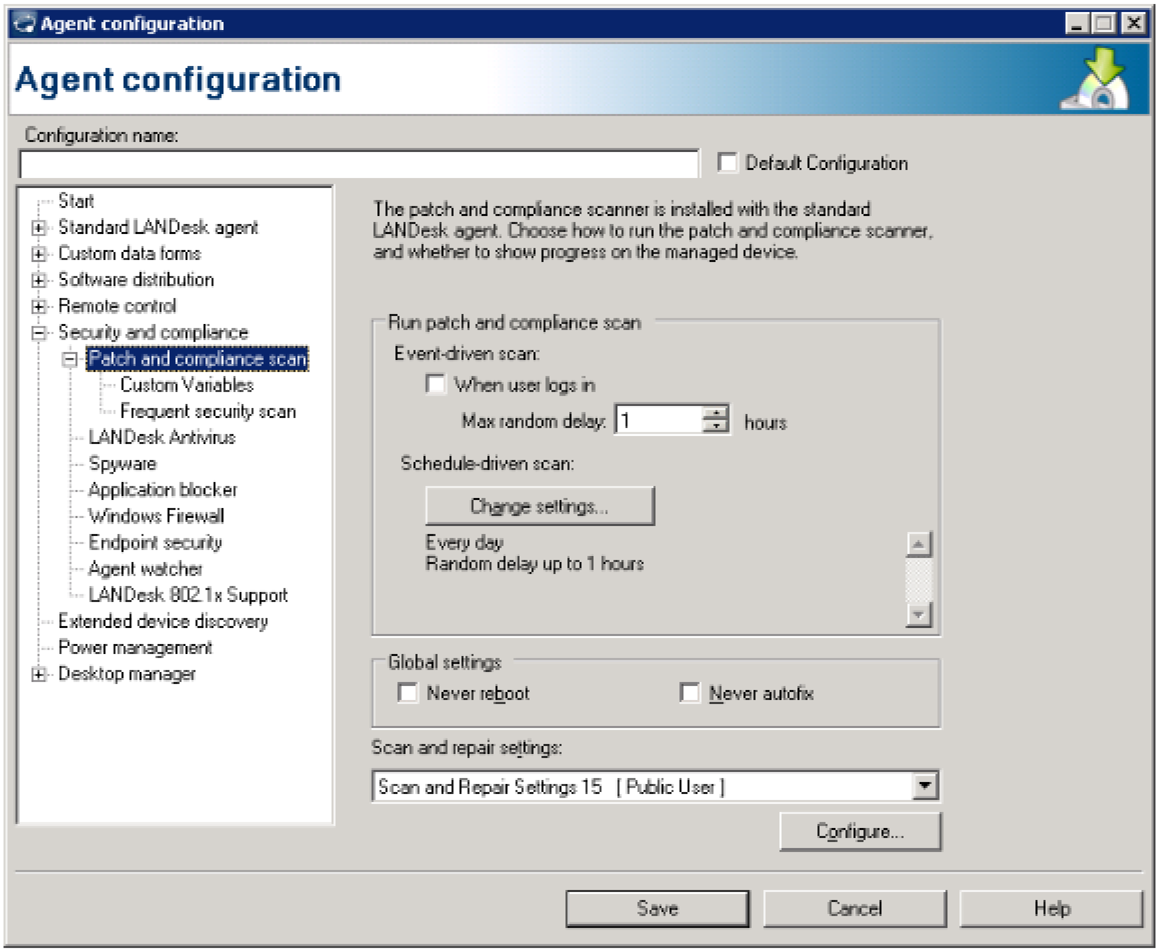
Scanning core servers and consoles for LANDesk software updates is supported
You can also scan LANDesk core servers and consoles for LANDesk software updates, but they must first have the standard LANDesk agent deployed, which includes the security scanner agent required for security scanning tasks.

Configuring Windows devices for security scanning

The security scanner agent is included by default with the standard LANDesk agent and is installed on devices with even the most basic agent configuration. In other words, any Windows device configured with the Agent configuration tool will be ready for patch and compliance scanning and remediation.

Using the Agent Configuration tool

Use the Agent Configuration tool (**Tools > Configuration > Agent Configuration > New Windows configuration**) to create agent configurations with specified Patch and Compliance scanning settings , and other security settings, that can be deployed to target devices.



Configuration name:

□ Default Configuration

The patch and compliance scanner is installed with the standard LANDesk agent. Choose how to run the patch and compliance scanner, and whether to show progress on the managed device.

Run patch and compliance scan

Event-driven scan:

□ When user logs in

Max random delay: 1 hours

Schedule-driven scan:

Every day
Random delay up to 1 hours

Global settings

□ Never reboot □ Never autofix

Scan and repair settings:

Scan and Repair Settings 15 [Public User]

To configure devices for security scanning and remediation via an agent configuration

1. In the console, click **Tools > Configuration > Agent Configuration**.
2. Click the **New Windows** toolbar button.
3. After specifying your desired settings for the agent configuration, click the **Security and Compliance** group, and then click **Patch and Compliance Scan**.
4. Select how you want the security scanner to run on your managed devices. For more information about an option, click **Help**.
5. Select a scan and repair settings from the available list to apply it to the agent configuration you're creating. You can create a new settings or edit an existing settings by clicking **Configure**. Scan and repair settings determine whether the security scanner displays on devices while running, reboot options, user interaction, and the security content types scanned.
6. Finish specifying any other desired settings for the agent configuration and then click **Save**.

When creating or editing an agent configuration, you can specify some of the security scanner options, such as when and how often the scanner runs automatically on managed devices, whether the scanner displays progress and prompts on the end user device, as well as global settings for remediation operations such as device reboot and autofix. For more information on customizing the behavior of the security scanner agent as part of creating and deploying agent configurations to managed Windows devices, see "Deploying Security services" on page 626.

Note: WinSock2 is required on Windows 9x devices in order for the security scanner agent to run.

After agent configuration occurs, a program icon for the security scanner is added to the **LANDesk Management** program group in the **Start** menu on the managed device. This program can be used to run the scanner directly from the device as opposed to any runkey launch, recurring local scheduler launch, or scheduled task via the console.

Additional security settings in agent configurations

When defining a device agent configuration (for Windows devices), you can also enable and configure complementary security features, such as:

- Frequent security scanning for critical security risks
- Spyware monitoring
- Application Blocker
- Windows Firewall
- Endpoint Security which includes the security components: HIPS, LANDesk Firewall, and Device Control
- Agent Watcher to monitor files and services
- 802.1X NAC support that extends network access control (NAC) with authentication and compliance

See the sections below for more information.

About the Frequent Security scan page

Use this page to enable and configure high frequency scanning for critical, time-sensitive security risks such as recently discovered and malignant viruses, and firewall configuration risks.

This page contains the following options:

- **Use the frequent security scanner:** Enables a frequent security scan on devices with this agent configuration.
- **Scan only when a user is logged in:** Restricts the frequent security scan so that it runs only if a user is logged into the target device.
- **Every:** Specifies the time interval for a the frequent security scan.
- **Scan and repair settings (that scans for a group):** Specifies the scan and repair settings that control the security scanner for frequent security scans. Scan and repair settings determine whether the security scanner displays on devices while running, reboot options, and user interaction. The setting you select must be configured to scan a group, not a type. You can also click **Configure** to create a new scan and repair setting that is associated with a group.

About the Spyware and Application Blocker pages

Use these pages to enable and configure spyware detection and real-time application blocking and removal on managed devices configured with this agent configuration.

Blocked application disclaimer
For legal information about blocked application content, see the "Legal disclaimer for the blocked applications type" on page 314.

Real-time spyware detection checks only for spyware definitions that reside in the **Scan** group, and that have autofix turned on. You can either manually enable the autofix option for downloaded spyware definitions, or configure spyware definition updates so that the autofix option is automatically enabled when they are downloaded.

Real-time spyware detection monitors devices for new launched processes that attempt to modify the local registry. If spyware is detected, the security scanner on the device prompts the end user to remove the spyware.

This page contains the following options:

- **Enable real-time spyware blocking:** Turns on real-time spyware monitoring and blocking on devices with this agent configuration.

  Note: In order for real-time spyware scanning and detection to work, you must manually enable the autofix feature for any downloaded spyware definitions you want included in a security scan. Downloaded spyware definitions don't have autofix turned on by default.

- **Notify user when spyware has been blocked:** Displays a message that informs the end user a spyware program has been detected and remediated.
- **If an application is not recognized as spyware, require user's approval before it can be installed:** Even if the detected process is not recognized as spyware according to the device's current list of spyware definitions, the end user will be prompted before the software is installed on their machine.

With real-time application blocking, remediation is NOT a separate task. Application blocking takes place as part of the security scan itself, by editing the registry on the local hard drive to disable user access to those unauthorized applications. Security services uses the Software license monitoring tool's softmon.exe feature to deny access to specified application executables even if the executable file name has been modified because softmon.exe reads the file header information.

This page contains the following options:

- **Enable blocking of unauthorized applications:** Turns on real-time application blocking on devices with this agent configuration.
- **Notify user when an application has been blocked:** Displays a message that informs the end user they have attempted to launch an unauthorized application and access has been denied.

Configuring Linux and UNIX devices for security scanning

Patch and Compliance also supports vulnerability scanning on:

- Red Hat Linux
- SUSE Linux
- Sun Sparc (Solaris 8)

For each platform, security content can be downloaded with Patch and Compliance just as with Windows vulnerabilities.

Linux and UNIX devices can't be configured with the security scanner agent via the console's agent configuration tool. Linux and UNIX device configuration is a manual process. For more information about setting up Linux and UNIX devices, see "Configuring Linux and UNIX device agents" on page 83. You can also see the README file contained in the respective platform's tar file located in the platforms folder under ManagementSuite\LDLogon on the core server.

Once configured, Linux and UNIX platforms can be scanned for vulnerabilities via scheduled tasks from the console. If vulnerabilities are detected, remediation must be performed manually at the affected device.

Configuring Mac OS X devices for security scanning

On Macintosh OS X devices, Patch and Compliance supports security content downloads, as well as security scanning and remediation.

Additionally, you can create and configure agent configuration for your Macintosh devices with the Agent configuration tool. As with Windows agent configuration, the security scanner agent is part of the default standard LANDesk agent for Macintosh devices. To create and deploy a Macintosh agent configuration with security scanner support, see "Managing Macintosh devices" on page 280.

Once configured, Macintosh devices can be scanned for vulnerabilities via scheduled tasks from the console. If vulnerabilities are detected, remediation must be performed at the affected device.

To launch the security scanner manually on Mac devices

1. Open the Mac OS X **System Preferences** and select the **LANDesk Client** page.
2. On the **Overview** tab, click **Check Now** in the **Security** section.

Legal disclaimer for the blocked applications type

Disclaimer

As a convenience to its end users, LANDesk provides access to a database containing certain information regarding executable files that an end user may utilize in connection with the application blocker functionality of the LANDesk Security Suite. THIS INFORMATION IS PROVIDED AS-IS WITHOUT ANY EXPRESS, IMPLIED, OR OTHER WARRANTY OF ANY KIND, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. As such, LANDesk does not guarantee the accuracy, completeness or currency of this information and the end user is responsible to review and confirm this information before use. Any use of this information is at the end users own risk.

Some of the Summary information in the blocked applications definitions are provided from: http://www.sysinfo.org, and is copyrighted as follows: "Presentation, format and comments Copyright © 2001-2005 Paul Collins; Portions Copyright © Peter Forrest, Denny Denham, Sylvain Prevost, Tony Klein; Database creation and support by Patrick Kolla; Software support by John Mayer; All rights reserved."

Managing security content and patches

This section provides information on downloading, viewing, and organizing security content; downloading and working with patches; and creating and using custom definitions.

Scanning and remediating devices
For information on performing security and compliance scans on managed devices for all types of security risks (such as OS and application vulnerabilities, software updates, spyware, system configuration exposures, etc.), remediating affected devices, as well as generating security alerts, logging, and reports, see "Scanning and remediating devices" on page 332.

Read this section to learn about:

Managing security content

- "Downloading security content" on page 315
- "Viewing security content" on page 319
- "Searching for vulnerabilities by CVE names" on page 319
- "Using filters to customize item lists" on page 320
- "Purging unused definitions" on page 320
- "Viewing security information for a scanned device" on page 321

Working with patches

- "Downloading patches" on page 322
- "Uninstalling patches (patch rollback)" on page 323
- "Removing patches from the core database" on page 323

Using custom definitions

- "Creating custom definitions and detection rules" on page 324
- "Importing and exporting custom definitions" on page 328
- "Deleting custom definitions" on page 329

Downloading security content

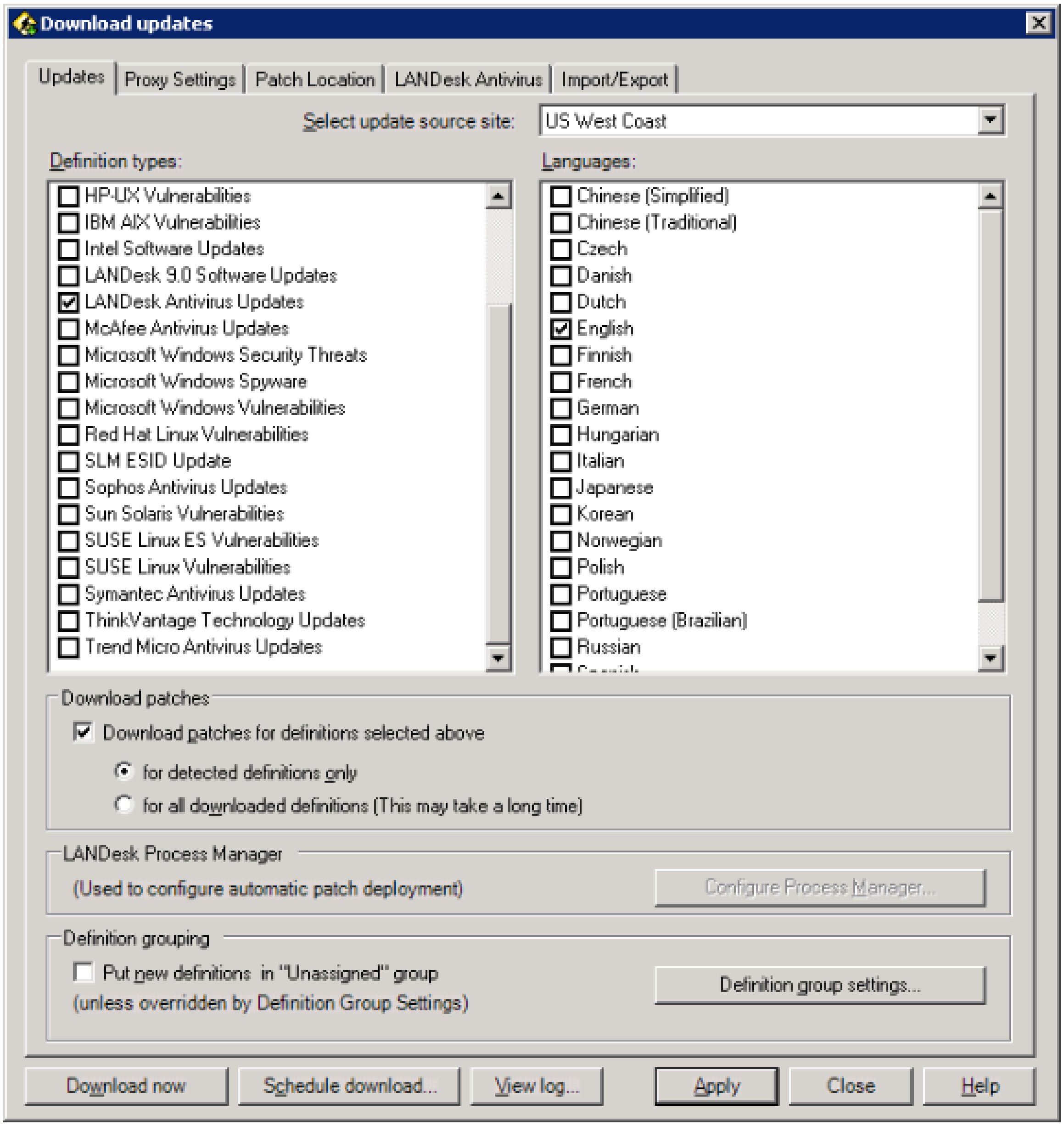
Your network and devices are continuously vulnerable to security risks and exposures from many harmful sources: worms, viruses, spyware, as well as ordinary maintenance issues like software updates and bug fixes. Patches are released regularly to repair inevitable operating system and application vulnerabilities. The Patch and Compliance tool makes the process of gathering the latest security type's definitions and patches quick and easy by letting you download content via a LANDesk-hosted database. LANDesk Security Suite services consolidates known definitions from trusted, industry/vendor sources and sends reliable information directly to you.

Patch and Compliance also supports custom vulnerability definitions
In addition to known vulnerabilities, you can also create your own custom vulnerability definitions and associated detection rules. For more information, see "Creating custom definitions and detection rules" on page 324.

By establishing and maintaining up-to-date security content, you can better understand the nature and extent of the security risks for each platform and application you support, determine which vulnerabilities and other types of risks are relevant to your environment, and customize security scanning and remediation tasks. The first step in this security management strategy is to download a current listing of the latest known security content.

Using Download Updates

Use the Download Updates dialog (**Tools > Security > Patch and Compliance > Download Updates**) to configure and perform security content updates at once, or create a scheduled update task to occur at a set time or as a recurring task (see "Scheduling automatic security content updates" on page 319).



Select update source site: US West Coast

Definition types:

☐ HP-UX Vulnerabilities
☐ IBM AIX Vulnerabilities
☐ Intel Software Updates
☐ LANDesk 9.0 Software Updates
☑ LANDesk Antivirus Updates
☐ McAfee Antivirus Updates
☐ Microsoft Windows Security Threats
☐ Microsoft Windows Spyware
☐ Microsoft Windows Vulnerabilities
☐ Red Hat Linux Vulnerabilities
☐ SLM ESID Update
☐ Sophos Antivirus Updates
☐ Sun Solaris Vulnerabilities
☐ SUSE Linux ES Vulnerabilities
☐ SUSE Linux Vulnerabilities
☐ Symantec Antivirus Updates
☐ ThinkVantage Technology Updates
☐ Trend Micro Antivirus Updates

Languages:

☐ Chinese (Simplified)
☐ Chinese (Traditional)
☐ Czech
☐ Danish
☐ Dutch
☑ English
☐ Finnish
☐ French
☐ German
☐ Hungarian
☐ Italian
☐ Japanese
☐ Korean
☐ Norwegian
☐ Polish
☐ Portuguese
☐ Portuguese (Brazilian)
☐ Russian

Download patches

☑ Download patches for definitions selected above

● for detected definitions only
○ for all downloaded definitions (This may take a long time)

LANDesk Process Manager

(Used to configure automatic patch deployment)

Definition grouping

☐ Put new definitions in "Unassigned" group
(unless overridden by Definition Group Settings)

Note: Only one LANDesk user on a specific core server (including additional consoles) can update security content at a time. If a user attempts to update content while the process is already running, a message prompt appears indicating there is a conflict.

To download security content (and patches)

1. Click **Tools > Security > Patch and Compliance**.
2. Click the **Download updates** toolbar button.

3. Select the update source site from the list of available content servers.
4. Select the definition types whose security content you want to update. You can select one or more types in the list depending on your LANDesk Security Suite content subscription. The more types you select, the longer the update will take.
5. Select the languages whose content you want to update for the types you've specified.

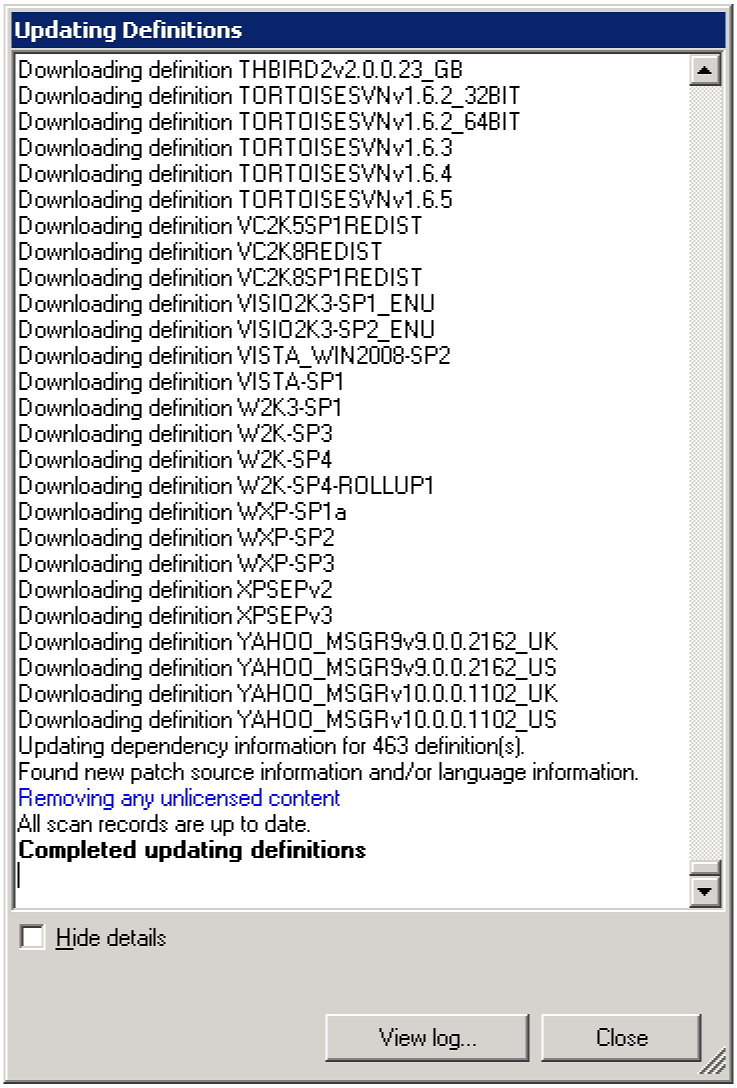
   Some vulnerability and other definition types, and any associated patches, are language neutral or independent, meaning they are compatible with any language version of the OS or application addressed by that definition. In other words, you don't need a unique language-specific patch to remediate those vulnerabilities because the patch covers all supported languages. For example, Linux and UNIX platforms use only language neutral definitions and patches. However, Microsoft Windows and Apple Macintosh platform vulnerability definitions and patches are nearly always language specific.

   When downloading content for any platform (with the appropriate subscription), all of the selected platform's language neutral vulnerability definitions are automatically updated by default. If you've selected a Windows or Mac content type, you must also select the specific languages whose definitions you want to update. If you've selected the Sun Solaris or a Linux platform, you do not have to select a specific language because their content is language neutral and will be updated automatically.

6. If you want new content (content that does not already reside in any groups) to automatically be placed in the Unassigned group instead of the default location, which is the Scan group, check the **Put new definitions in the Unassigned group** check box.
7. If you want to automatically download associated patch executable files, click the **Download patches** check box, and then click one of the download options. (**Note:** Patches are downloaded to the location specified on the **Patch Location** page of the Download updates dialog.)

   - **For detected definitions only:** Downloads only the patches associated with vulnerabilities, security threats, or LANDesk updates detected by the last security scan (i.e., the definitions that are currently residing in the Detected group).
   - **For all downloaded definitions:** Downloads ALL of the patches associated with vulnerability, security threats, and LANDesk updates currently residing in the Scan group.

8. If you have a proxy server on your network that is used for external Internet transmissions (that is required to update security content and download patches), click **Proxy Settings** and specify the server's address, port number, and authentication credentials if a login is required to access the proxy server.
9. Click **Apply** at any time to save your settings.
10. Click **Update Now** to run the security content update. The **Updating Definitions** dialog (see below) displays the current operation and status. (To create a scheduled task, click **Schedule Update**.)
11. When the update has completed, click **Close**. Note that if you click **Cancel** before the update is finished, only the security content that has been processed to that point is downloaded to the core database. You would need to run the update again in order to obtain all of the remaining security content.



```
Downloading definition THBIRD2v2.0.0.23_GB
Downloading definition TORTOISESVNv1.6.2_32BIT
Downloading definition TORTOISESVNv1.6.2_64BIT
Downloading definition TORTOISESVNv1.6.3
Downloading definition TORTOISESVNv1.6.4
Downloading definition TORTOISESVNv1.6.5
Downloading definition VC2K5SP1REDIST
Downloading definition VC2K8REDIST
Downloading definition VC2K8SP1REDIST
Downloading definition VISIO2K3-SP1_ENU
Downloading definition VISIO2K3-SP2_ENU
Downloading definition VISTA_WIN2008-SP2
Downloading definition VISTA-SP1
Downloading definition W2K3-SP1
Downloading definition W2K-SP3
Downloading definition W2K-SP4
Downloading definition W2K-SP4-ROLLUP1
Downloading definition WXP-SP1a
Downloading definition WXP-SP2
Downloading definition WXP-SP3
Downloading definition XPSEPv2
Downloading definition XPSEPv3
Downloading definition YAHOO_MSGR9v9.0.0.2162_UK
Downloading definition YAHOO_MSGR9v9.0.0.2162_US
Downloading definition YAHOO_MSGRv10.0.0.1102_UK
Downloading definition YAHOO_MSGRv10.0.0.1102_US
Updating dependency information for 463 definition(s).
Found new patch source information and/or language information.
Removing any unlicensed content
All scan records are up to date.
Completed updating definitions
```

Note: Do not close the console while an update security process is running or the process will be terminated. However, this rule does not apply to a Download Security Content scheduled task, which will finish processing even if the console is closed while it is running.

To configure the patch download location

1. On the **Download updates** dialog, click the **Patch Location** tab.
2. Enter a UNC path where you want the patch files copied. The default location is the core server's \LDLogon\Patch directory.
3. If the UNC path entered above is to a location other than the core server, enter a valid username and password to authenticate to that location.
4. Enter a Web URL where devices can access the downloaded patches for deployment. This Web URL should match the UNC path above.
5. You can click **Test Settings** to check to see if a connection can be made to the Web address specified above.
6. If you want to restore the UNC path and Web URL to their default locations, click **Restore to Default**. Again, the default storage location is the core server's \LDLogon\Patch directory.

Scheduling automatic security content updates

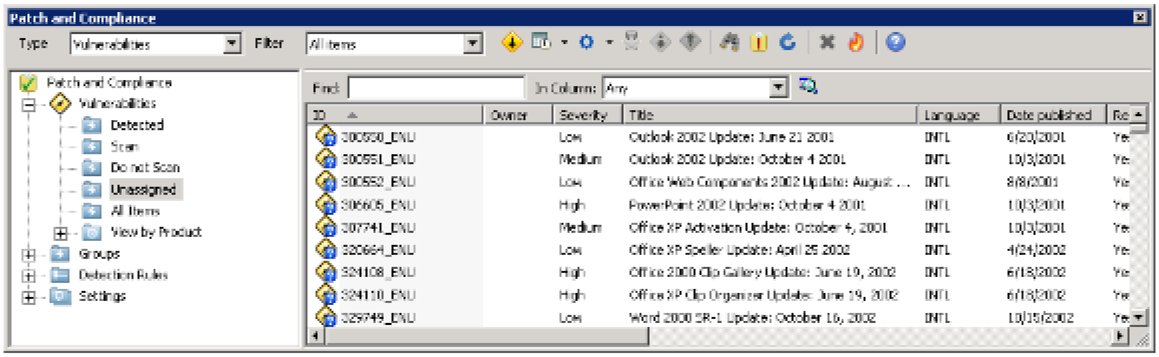
You can also configure security content updates as a scheduled task to occur at a set time or as a recurring task. To do this, simply click the **Schedule download** toolbar button. The **Scheduled update information** dialog shows task-specific settings for the task. Click **OK** to create a Download Security Content task in the Scheduled Tasks window, where you can specify the scheduling options.

Task-specific settings and global settings
Note that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific. However, all of the settings on the other pages of the **Download updates** dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global settings it is effective for all security content download tasks from that point on.

Viewing security content

After security content has been updated with the LANDesk Security service, you can view the definitions and detection rules (for vulnerabilities and custom definitions) only in their respective groups in the Patch and Compliance tool window.

Use the **Type** drop-down list to view content for a specific definition type or for all definition types. You can also use the **Filter** control to further customize the content you want to display.



Type: Vulnerabilities
Filter: All items
Find:
In Column: Any

ID	Owner	Severity	Title	Language	Date published	Re
300550_ENU		Low	Outlook 2002 Update: June 21 2001	INTL	6/20/2001	Ye
300551_ENU		Medium	Outlook 2002 Update: October 4 2001	INTL	10/3/2001	Ye
300552_ENU		Low	Office Web Components 2002 Update: August ...	INTL	8/8/2001	Ye
306605_ENU		High	PowerPoint 2002 Update: October 4 2001	INTL	10/3/2001	Ye
307741_ENU		Medium	Office XP Activation Update: October 4, 2001	INTL	10/3/2001	Ye
320664_ENU		Low	Office XP Speller Update: April 25 2002	INTL	4/24/2002	Ye
324108_ENU		High	Office 2000 Clip Gallery Update: June 19, 2002	INTL	6/18/2002	Ye
324110_ENU		High	Office XP Clip Organizer Update: June 19, 2002	INTL	6/18/2002	Ye
329749_ENU		Low	Word 2000 SR-1 Update: October 16, 2002	INTL	10/15/2002	Ye

Once security content has been downloaded, you can move items into different status groups, or copy them into your own custom groups. For information on how to use the different groups, see "Understanding and using the Patch and Compliance tool" on page 302.

You can also view property details for each of the updated definitions and detection rules by right-clicking an item and selecting **Properties**. This information can help you determine which definitions are relevant to your network's supported platforms and applications, how detection rules check for the presence of definitions, what patches are available, and how you want to configure and perform remediation for affected devices.

Custom definitions can be modified
If you select a downloaded industry definition, its properties dialog is primarily for information viewing purposes only. However, if you select a custom definition, or are creating a new custom definition, the pages and fields in the properties dialog are editable, allowing you to define the definition and its detection rules.

Searching for vulnerabilities by CVE names

LANDesk supports the CVE (Common Vulnerabilities and Exposures) naming standard. With Patch and Compliance you can search for vulnerabilities by their CVE names, and view CVE information for downloaded vulnerability definitions.

For more information about the CVE naming convention, LANDesk compatibility with the CVE standard, and how to use CVE identification to find individual security vulnerability definitions, see "Using CVE names" on page 330.

Using filters to customize item lists

The **Filter** drop-down list lets you create and apply custom display filters to control the items that display in the right-hand frame of the tool window. Filters can help you streamline a large amount of security content. You can filter content by operating system and severity.

The **Filter** control can be used in conjunction with the **Type** control to display exactly the security content you're interested in viewing.

To create a new display filter

1. In Patch and Compliance, click the **Filter** drop-down list, and then click **Manage filters**.
2. Click **New**.
3. Enter a name for the new filter.
4. If you want to filter content by operating system, click the check box, and then select the operating systems you want to display.
5. If you want to filter by the severity of the definition, click the check box, and then select the severities you want to display. Click **OK**

To apply a filter to a content group's display

1. Click the content group in the left-hand pane of the window.
2. Click the **Filter** drop-down list, and then select a filter from the list.

Purging unused definitions

You can purge unused definitions from the Patch and Compliance tool window and the core database if you determine that it isn't relevant to your environment or if a successful remediation makes the information obsolete.

When you purge definitions, associated detection rule information is also removed from the Detection Rules groups in the tree view. However, the actual associated patch files aren't removed by this process. Patch files must be removed manually from the local repository, which is typically on the core server.

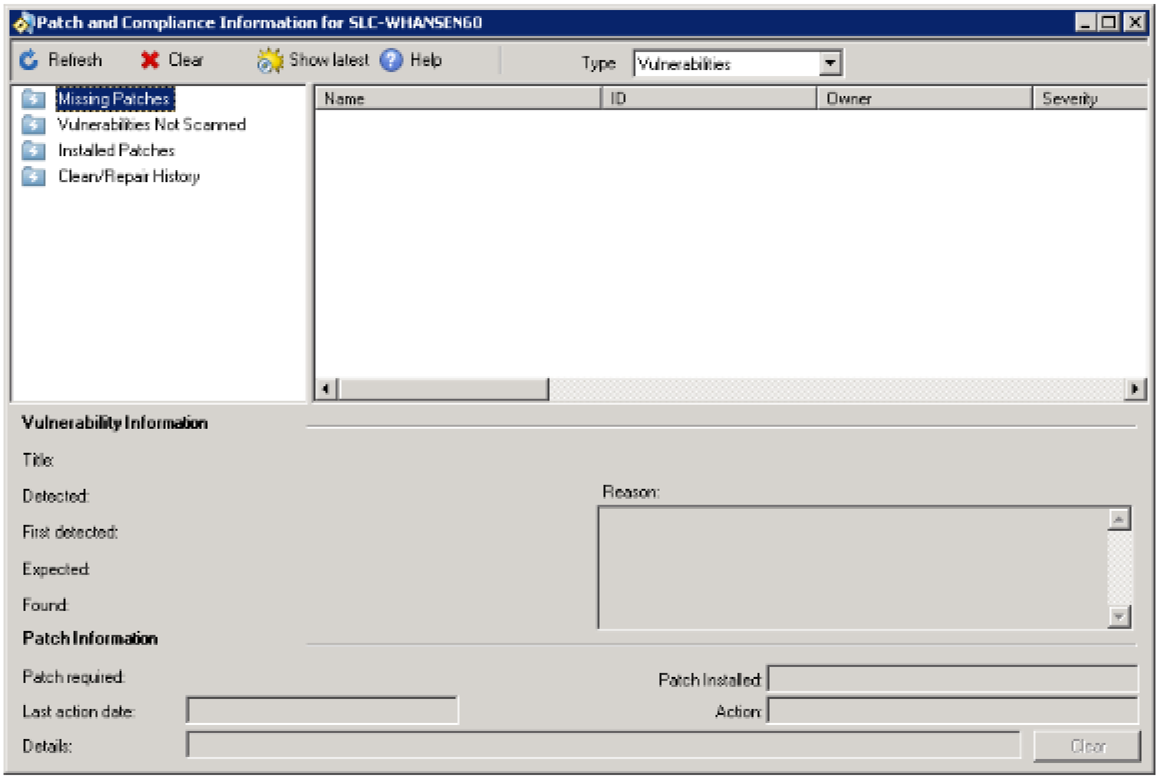
To purge unused definitions

1. Click **Tools > Security > Patch and Compliance**.
2. Click the **Purge unused definitions** toolbar button.
3. Select the platforms whose definitions you want to remove. You can select one or more platforms in the list. If a definition is associated with more than one platform, you must select all of its associated platforms in order for the definition to be removed.
4. Select the languages whose definition you want to remove (associated with the platform selected above). If you select a Windows or Macintosh platform above, you should specify the languages whose definition you want to remove. If you select a UNIX or Linux platform above, you must specify the Language neutral option in order to remove their language independent definitions.
5. Click **Remove**.

Viewing security information for a scanned device

You can also view information specific to scanned devices directly from the network view by right-clicking one or more selected devices, and then clicking **Security and Patch Information**.

This dialog lets you view detection, installation, and repair history, and perform patch management tasks.



Working with patches

The following section describes various tasks that can be performed specifically with patch executable files.

Downloading patches

In order to deploy security patches to affected devices, the patch executable file MUST first be downloaded to a local patch repository on your network. The default location for patch file downloads is this directory on the core server:

/LDLogon/Patches

You can change this location on the Patch Location page of the Download updates dialog.

You can download one patch at a time, or a set of patches together.

Patch download location and proxy server settings
Patch downloads always use the download location settings currently found on the Patch Location page of the Download updates dialog. Also note that if your network uses a proxy server for Internet access, you must first configure the proxy server's settings on the Proxy Settings page before you can download patch files.

Patch and Compliance first attempts to download a patch file from the URL (shown on the Patch Properties dialog). If a connection can't be made, or if the patch is unavailable for some reason, then the patch is downloaded from the LANDesk Security content service, which is a LANDesk-hosted database containing patches from trusted industry sources.

Download methods

Use one the following methods to download patches:

- From the Download Updates dialog
- From a detection rule
- From a security definition

You can download patches from the Download Updates dialog concurrently with their associated security definitions. This procedure is described above, see "Using Download Updates" on page 316.

You can also download patches directly from a detection rule or a security definition.

To download patches from a detection rule

1. From any **Detection Rules** group, right-click a detection rule, and then click **Download Patch**. (You can also download patches for custom definitions from the detection rule dialog when creating or editing a custom definition.)
2. Or, to download a set of patches, select any number of rules in any **Detection Rules** group, right-click the selection, and then click **Download Patch**.
3. The download operation and status displays in the **Downloading Patches** dialog. You can click **Cancel** at any time to stop the entire download process.
4. When the download is finished, click the **Close** button.

Note: With a detection rule, you can also download patches from its properties dialog (**Properties > Patch Information > Download**)

To download associated patches from a security definition

1. Right-click the security definition(s), click **Download associated patches**.
2. Select whether to download all associated patches or only current patches.

3. Click **Download**.

For more information on patch file download status, see "Understanding and using the Patch and Compliance tool" on page 302.

Uninstalling patches (patch rollback)

You can uninstall (i.e., rollback) patches that have been deployed to managed devices. For example, you may want to uninstall a patch that has caused an unexpected conflict with an existing configuration. By uninstalling the patch, you can restore the device to its original state.

To uninstall or rollback a patch

1. From any detection rule listing, right-click one or more rules, and then click **Uninstall Patch**.
2. Enter a name for the uninstall task.
3. Specify whether the uninstall is a scheduled task or a policy-based scan, or both.
4. If you selected scheduled task, specify which devices from which you want to uninstall the patch.
5. If the patch can't be uninstalled without accessing its original executable file (i.e., to use command-line parameters), and you want to deploy the executable using Targeted Multicast, check the **Use multicast** check box. To configure Multicast options, click the **Multicast Options** button. For more information, see "About the Multicast options dialog" on page 669.
6. If you selected policy, and you want to create a new query based on this uninstall task that can be used later, click the **Add a query** check box.
7. Select a scan and repair settings from the available list (or create a custom settings for this scan), to determine how the scanner operates on end user devices.
8. Click **OK**. For a scheduled task, you can now add target devices and configure the scheduling options in the Scheduled tasks tool. For a policy, the new policy appears in the Application Policy Management window with the task name specified above. From there you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

If a patch installation failed, you must first clear the install status information before attempting to install the patch again. You can clear the install (repair) status for the selected device by clicking **Clear** on the **Security and Patch Information** dialog. You can also clear the patch install status by vulnerability.

Removing patches from the core database

To remove patch files permanently, you must delete them from the patch repository, which is typically on the core server.

Using custom definitions

Creating custom definitions and detection rules

In addition to the known vulnerabilities that you update via the Patch and Compliance tool, you can also create your own custom (or user-defined) definitions, complete with custom detection rules, associated patch files, and special additional commands to ensure successful remediation.

Vulnerability definitions consist of a unique ID, title, publish date, language, and other identifying information, as well as the detection rules that tell the security scanner what to look for on target devices. Detection rules define the specific platform, application, file, or registry conditions that the security scanner checks for in order to detect a vulnerability (or practically ANY system condition or status) on scanned devices.

Custom vulnerability definitions is a powerful, flexible feature that lets you implement an additional, proprietary level of patch security on your LANDesk system. In addition to enhancing patch security, custom vulnerabilities can be used to assess system configurations, check for specific file and registry settings, and deploy application updates, among other innovative uses that take advantage of the scanning capabilities of the vulnerability scanner.

Creating custom blocked application definitions
You can also create your own custom definitions for the blocked application type. From the **Type** drop-down list, select **Blocked Applications**, enter an executable filename and a descriptive title for the definition, and then click **OK**.

Custom definitions don't necessarily have to perform remediation actions (deploying and installing patch files). If the custom definition is defined with a Detect Only detection rule or rules that can only be detected by Patch and Compliance, the security scanner looks at target devices and simply reports back the devices where the rule's prescribed condition (i.e., vulnerability is found). For example, you can write a custom Detect Only rule for the security scanner to check managed devices for the following:

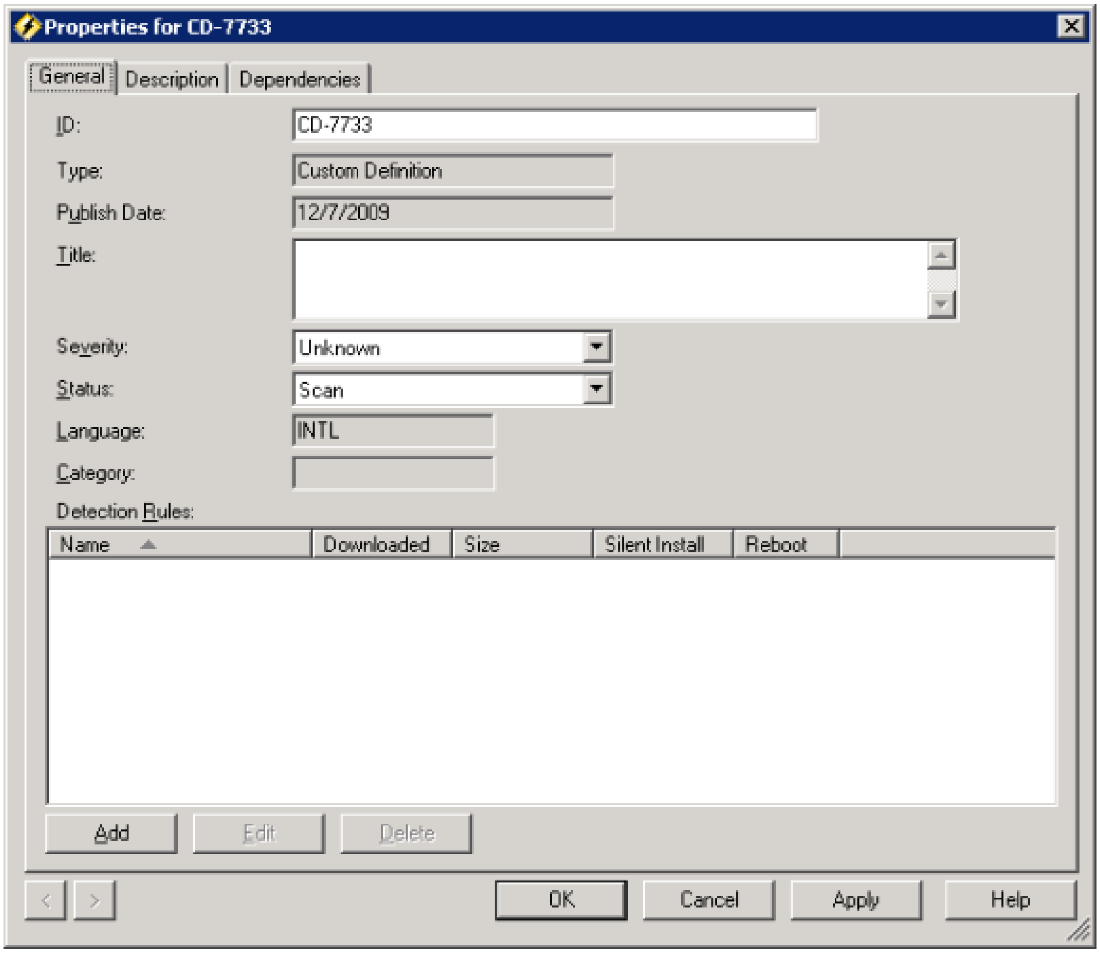
- Application existence
- File existence
- File version
- File location
- File date
- Registry setting
- And more...

You can create as many custom vulnerability definitions as you need to establish and maintain the optimal level of patch security for your environment.

Creating custom definitions

To create custom definitions

1. Click **Tools > Security > Patch and Compliance**.
2. From the **Type** drop-down list, select **All Types** or **Custom Definitions**. (The **Create custom definition** toolbar button is available only with one of these two types selected; or with the **Blocked Applications** type selected, if you want to create a custom blocked application definition.)
3. Click the **Create custom definition** toolbar button. An editable version of the properties dialog opens, allowing you to configure vulnerability settings.



Properties for CD-7733

ID: CD-7733

Type: Custom Definition

Publish Date: 12/7/2009

Title:

Severity: Unknown

Status: Scan

Language: INTL

Category:

Detection Rules:

Name	Downloaded	Size	Silent Install	Reboot

4. Enter a unique ID for the vulnerability. (The system-generated ID code can be edited.)
5. The type is a Custom Definition and can't be modified.
6. The publish date is today's date and can't be modified.
7. Enter a descriptive title for the vulnerability. This title displays in vulnerability lists.
8. Specify the severity level. Available options include: Unknown, Service Pack, Critical, High, Medium, Low, and Not Applicable.

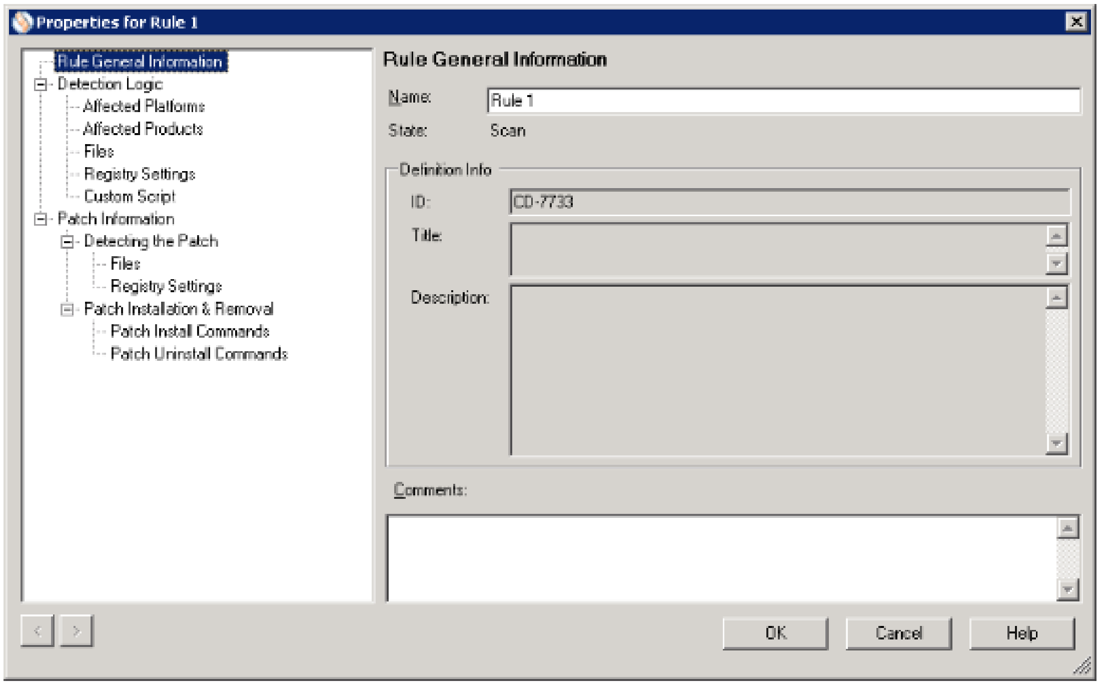
9. Specify the status for the vulnerability. Available options include: Don't Scan, Scan, and Unassigned. When you specify a status, the vulnerability is placed in the corresponding group in the tree view (see "Tree view" on page 304).
10. The language settings for user-defined vulnerabilities is automatically set to INTL (International or Language neutral, which means the vulnerability can be applied to any language version of operating systems and/or applications).
11. The Detection Rules list displays all the rules used by this vulnerability. If you are creating a new custom vulnerability, you should configure at least one detection rule that is used by the security scanner to scan devices for the vulnerability. To add detection rules, click **Add**. (See the procedure below for step-by-step instructions.)
12. If you want to provide additional information about this vulnerability, click **Description** and type your comments in the text box and/or enter a valid Web address where more information is posted.

As with known vendor vulnerabilities, custom vulnerabilities should include one or more detection rules that tell the security scanner what conditions to look for when scanning managed devices. Follow the steps below to create a detection rule for a custom vulnerability.

Creating custom detection rules

To create custom detection rules

1. Right-click a custom definition, and then click **Properties**. (Or double-click the vulnerability definition.)
2. Click the **Add** button located under the Detection Rules list. An editable version of the Rules Properties dialog opens at the dialog's General Information page, allowing you to configure a detection rule.



Name: Rule 1

State: Scan

ID: CD-7733

3. At the General Information page, enter a unique name for the rule. The rule's status cannot be modified here. To change the status of a detection rule, right-click the rule in any list view, and then click **Enable** or **Disable**, depending on the current state. The

rule's definition information cannot be modified here either. However, you can enter any information you want in the Comments box.

4. Use the various pages of the Rules Properties dialog to define the detection rule, as described in the rest of this procedure.
5. Open the Detection Logic pages.
6. At the Affected Platforms page, select the platforms you want the security scanner to run on to check for this detection rule's definition. The list of available platforms is determined by the vulnerabilities you've updated via the Patch and Compliance tool. Click **Load default platform list** to add the available platforms to the list. You must select at least one platform.
7. At the Affected Products page, associate the rule with one or more specific software applications. First, click **Edit** to open the Selected Affected Products dialog where you can add and remove products in the Affected Products list (this list can be shortened if you like, by clicking the check box at the bottom of the dialog). The list of available products is determined by the content you've updated. You do not need to have a product associated with a detection rule. Associated products act as a filter during the security scan process. If the specified associated product is found on the device, the scan quits. However, if the product is found, or if no products are specified, the scan continues to the files check.
8. At the Files page, configure specific file conditions that you want the rule to scan for. Click **Add** to make the fields on this page editable. The first step in configuring a file condition is to specify the verification method. The fields on this page depend on the verification method you select. To save a file condition, click **Update**. You can add as many file conditions as you like. For a detailed description of this option, see "About the Detection logic: Files used for detection page" on page 659.
9. At the Registry Settings page, configure specific registry conditions that you want the rule to scan for. Click **Add** to make the fields editable. To save a registry condition, click **Update**. You can add as many registry conditions as you like. For a detailed description of this option, see "About the Detection logic: Registry settings used for detection page" on page 660.
10. At the Custom Script page, you can create a custom VB script to assist with detection for this detection rule. The security scanner's runtime properties that can be accessed with a custom script to report its results are: Detected, Reason, Expected, and Found.

    Note: You can click the **Use editor** button to open your default script editing tool, associated with this file type. When you close the tool you're prompted to save your changes in the Custom Script page. If you want to use a different tool you have to change the file type association.

11. At the Patch Information page, specify whether the vulnerability associated with this detection rule can be repaired or can only be detected on your managed devices. If you select the repair option, the Patch Download Information and Repair Information fields become editable.
12. If you can repair by deploying a patch, enter the URL to that patch file and specify whether it can be downloaded automatically. (You can attempt to download the associated patch file at this time by clicking **Download**, or you can download it at another time.)
13. Also, if you can repair by deploying a patch, enter a unique filename for the patch file and specify whether the patch requires a reboot in order to complete remediation and if the patch requires user input during remediation. (For a detection rule that includes remediation, we strongly recommend you create a hash for the patch file by clicking **Generate MD5 Hash**. The actual patch file must be downloaded before you can create a hash. For more information on the hash, see "About the Detection rule: General information page" on page 658.)

14. For a rule that allows remediation of the associated vulnerability, you can configure additional commands that are run during the remediation process on affected devices. To configure additional remediation commands, click the Patch Install Commands page, and then click **Add** to select a command type and to make the command's argument fields editable. Additional patch install commands are NOT required. If you don't configure special commands, the patch file executes as it normally would by itself. For a detailed description of this option, see "About the Patch install commands page" on page 663.

Now that you've created a custom vulnerability definition, you can do the same things with it as you would with a known vulnerability from an industry source. You can set the vulnerability's status to Scan or place it in the Scan group to be included in the next security scan, place it in the Don't Scan or Unassigned group, view affected computers, enable Auto Fix, create a repair job, or clear scan/repair status. To choose an option, right-click a custom vulnerability definition to access its shortcut menu.

Two operations that are unique to user-defined definitions are importing and exporting, and deleting.

Importing and exporting custom definitions

The Patch and Compliance tool provides a way for you to import and export custom definitions and their detection rules. You can't import and export known industry vulnerability definitions.

Custom definitions are exported and imported as an XML-formatted file.

Import and export is useful if you want to share custom definitions with other core servers. Exporting makes it possible for you to save a backup copy for a definition that you want to remove temporarily from the core database.

You can also use the export/import feature to export a definition, manually edit the exported file as a template and save multiple variations of the definition, and then import the new definitions. If the definition is complex, this procedure can be faster and easier than creating multiple definitions in the console.

To export custom definitions

1. From a Custom Definitions list, select one or more custom definitions.
2. Click the **Export** toolbar button. (Or, right-click the selected definitions, and then click **Export**.)
3. Enter the path to the folder where you want to export the definitions as an individual XML file.
4. If you've exported the definitions before to the specified location and you want to replace it, click the **Overwrite existing definitions**.
5. Click **Export**. Check the Export Status window to see whether the definitions are successfully exported.
   Note: An exported definition continues to exist in the core database, and therefore still appears in the Custom Definitions group that corresponds to its status: Unassigned, Scan, or Don't Scan.
6. Click **Close**.

To import custom definitions

1. In Patch and Compliance, click the **Import Custom Definitions** toolbar button.
2. Locate and select one or more definitions (in the XML file you want to import), and then click **Open**. If the definition already exists in the core database, you're prompted whether you want to overwrite it. Check the status window to see whether the definition is successfully imported.

3. Click **Close**. Imported definitions (new and updated) are placed in the Custom Definitions Unassigned group.

Deleting custom definitions

If you no longer need a custom definition, you can delete it. Deleting a custom definition removes its information and its associated detection rules from the core database, and from the Patch and Compliance tool window. (Exporting does not remove the definition information.)

As with purging known vulnerability information, deleting custom definitions does not remove any downloaded associated patch files. Patch files must be removed manually from the patch repository.

To delete custom definitions, select one or more custom definitions, and then click the **Delete selected custom definitions** button in the toolbar.

Restoring exported custom definitions
If you delete a custom definition that had previously been exported as an XML file, you can restore that definition by importing it back into the database via the Patch and Compliance tool.

Using CVE names

Patch and Compliance supports the CVE (Common Vulnerabilities and Exposures) naming standard. You can search for a downloaded vulnerability by its CVE name. You can also view the CVE name(s) associated with an individual vulnerability.

Read this section to learn about:

- "What is CVE?" on page 330
- "LANDesk compatibility with the CVE standard" on page 330
- "Using CVE names when searching for vulnerabilities" on page 331

What is CVE?

CVE is short for Common Vulnerabilities and Exposures, a collaborative initiative by several leading security technology organizations to compile and maintain a list of standardized names for vulnerabilities and other information security exposures. CVE is a dictionary of names rather than a database.

In short, the stated purpose of the CVE naming standard is to make it easier to search for, access, and share data across vulnerability databases and security tools. For more details about CVE and the CVE Editorial Board, visit the MITRE Corporation's Web site.

LANDesk compatibility with the CVE standard

LANDesk security products, including the flagship LANDesk Management Suite as well as LANDesk Security Suite and LANDesk Patch Manager, offer tools for vulnerability definition updating, viewing, and reporting that fully support the CVE standard.

When you download vulnerability definition updates, the vulnerability data contains CVE name references that are based on the most recent information from the CVE board. Additionally, the vulnerability definition includes a hyperlink to the CVE dictionary Web site where you can find the most recent CVE version information at its source. The accuracy and currency of the CVE data is validated by this direct link.

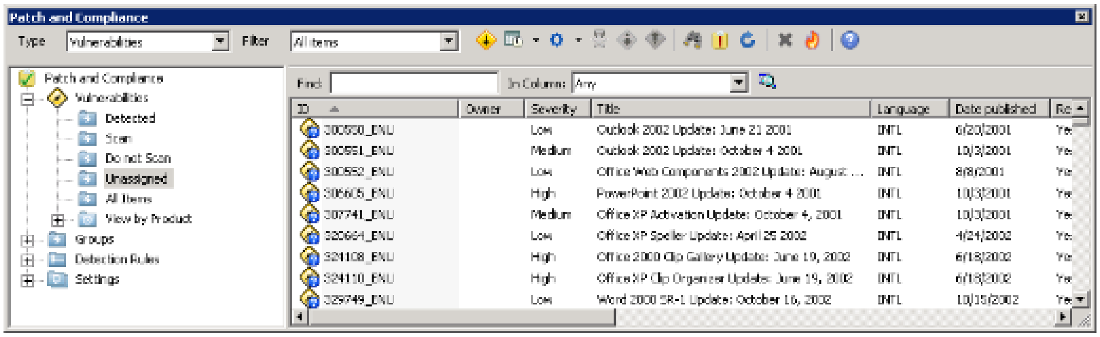
Using CVE names when searching for vulnerabilities

Patch and Compliance lets you search for vulnerabilities by their unique CVE names.

You can also find CVE names for downloaded vulnerabilities as well as access the CVE Web site for more information about the vulnerability and its CVE status.

To find security vulnerability definitions by using CVE names

1. In the **Patch and Compliance** tool window, select **Vulnerabilities** from the **Type** drop-down list. A complete list of downloaded vulnerability definitions displays.



Type: Vulnerabilities

Filter: All items

Find:

In Column: Any

ID	Owner	Severity	Title	Language	Date published	Re
300550_ENU		Low	Outlook 2002 Update: June 21 2001	INTL	6/20/2001	Ye
300551_ENU		Medium	Outlook 2002 Update: October 4 2001	INTL	10/3/2001	Ye
300552_ENU		Low	Office Web Components 2002 Update: August ...	INTL	8/8/2001	Ye
306605_ENU		High	PowerPoint 2002 Update: October 4 2001	INTL	10/3/2001	Ye
307741_ENU		Medium	Office XP Activation Update: October 4, 2001	INTL	10/3/2001	Ye
320664_ENU		Low	Office XP Speller Update: April 25 2002	INTL	4/24/2002	Ye
324108_ENU		High	Office 2000 Clip Gallery Update: June 19, 2002	INTL	6/18/2002	Ye
324110_ENU		High	Office XP Clip Organizer Update: June 19, 2002	INTL	6/18/2002	Ye
329749_ENU		Low	Word 2000 SR-1 Update: October 16, 2002	INTL	10/15/2002	Ye

2. Enter the CVE name (CVE ID) in the **Find** field, select **Any** or **CVE ID** from the **In Column** drop-down list, and then click the **Search** button. (You can enter the entire CVE ID, including the cve- prefix, or as much of the ID as you know, and search your downloaded security repository for matching vulnerabilities.)
3. If a vulnerability with a matching CVE ID is found in the repository of vulnerabilities you've downloaded, it displays in the list.
4. Right-click the vulnerability to access its shortcut menu for available options.

To find CVE names for downloaded security vulnerability definitions

1. In **Patch and Compliance**, select **Vulnerabilities** or **All Types** from the **Type** drop-down list. A list of downloaded definitions displays. (If the column for CVE ID data has been selected, you can view CVE IDs in the item list. To configure columns, right-click a column title bar, select **Columns**, and make sure the **CVE ID** column is in the **Selected Columns** list.)
2. Double-click a vulnerability definition (or right-click the definition and select **Properties**) to open its **Properties** dialog.
3. Click the **Description** page.
4. If the selected vulnerability has a CVE name, it displays in the **CVE ID** drop-down list. Some vulnerabilities might have more than one CVE name, which you can access by scrolling through the drop-down list.
5. To access the Web page for a specific CVE ID, click the **More information for CVE ID** link. The CVE Web site provides detailed information about each vulnerability with a CVE name, including its current status with the CVE board (approved Entry, or Candidate under review).

Scanning and remediating devices

This section provides information on scanning managed devices for a variety of security risks (such as OS and application vulnerabilities, software updates, spyware, system configuration exposures, etc.); remediating affected devices; and generating security alerts, logging, and reports.

Managing security content and patches
For information on downloading and organizing security content, working with patches, and using custom definitions, see Managing security content and patches.

Read this section to learn about:

Scanning devices

- Scanning devices for security risks
- How Patch and Compliance scans for different security risks
- Creating security and compliance scan tasks
- Configuring scan options with scan and repair settings
- Using custom variables and custom variable override settings
- Viewing detected security data
- Forwarding security scan results to a rollup core

Remediating devices

- Remediating devices that detected security risks
- How Patch and Compliance remediates different security risks
- Remediation methods
  - Using a scheduled repair task
  - Using a repair policy (Windows only)
  - Using an autofix repair
- What happens on a device during remediation
- Viewing patch and compliance information for scanned devices
  - Verifying remediation status
  - Clearing vulnerability scan and repair status by vulnerability

Other patch and compliance management tasks

- Creating a scheduled reboot task
- Using patch and compliance alerts
- Using patch and compliance reports

Scanning devices for security risks

Traditionally, security scanning meant checking the currently installed versions of operating system and application specific files and registry keys on a device against the most current known vulnerabilities in order to identify and resolve security risks. LANDesk Security services offers expanded security content types, enabling you to scan for and remediate even more of today's prevalent security risks and exposures.

Depending on your Security Suite content subscription, you can scan for:

- Known vulnerabilities (for Windows, Mac, Linux, and UNIX)
- Custom vulnerabilities (defined by a LANDesk Administrator)
- Spyware
- Antivirus scanner status (third-party scanner engines, as well as the LANDesk Antivirus tool)
- Viruses (using the integrated LANDesk Antivirus tool, you can: download the latest virus definition files, create and deploy antivirus scans, configure antivirus scanner settings and the antivirus scan options available to end users, enable real-time file and email protection, and more. For more information, see LANDesk Antivirus.)
- Security threats (local system or platform configuration errors; includes firewall detection and configuration)
- Blocked applications
- LANDesk software updates
- Driver updates
- Software updates

Security Suite content subscriptions
For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

How Patch and Compliance scans for different security risks

The table below describes how the security scanner searches for each type of security risk:

When scanning for...	Patch and Compliance scans by...
LANDesk software updates	Using software update definitions published by LANDesk to check for the latest LANDesk software versions.
Windows vulnerabilities	Using vulnerability definitions published by LANDesk (based on official vendor security bulletins to check for known operating system and/or application vulnerabilities).
Macintosh vulnerabilities	Using vulnerability definitions published by LANDesk (based on official security bulletins to check for known vulnerabilities).
Linux/UNIX vulnerabilities	Using vulnerability definitions published by LANDesk (based on official security bulletins to check for known vulnerabilities).
Custom definitions	Using custom vulnerability definitions created by a LANDesk Administrators to check for a user-defined platform, application, file, or registry settings conditions.
Security threats	Using security threat definitions published by LANDesk to check for local Windows system configuration errors and exposures. You can modify security threat definitions that use editable custom variables to check for specific conditions.

When scanning for...	Patch and Compliance scans by...
Spyware	Using spyware detection definitions that check for instances of spyware programs on scanned devices. Patch and Compliance uses the LANDesk Software license monitoring tool's softmon.exe program to monitor for spyware. You can also enable real-time spyware monitoring and blocking with a device's agent configuration.
Driver updates	Using third-party driver update definitions that check for driver versions.
Software updates	Using third-party software update definitions that check for software versions.
Antivirus updates	Using antivirus scanner detection definitions (NOT actual virus definition/pattern files) that check for: - installation of common antivirus scanner engines (including the LANDesk Antivirus tool) - real-time scanning status (enabled or disabled) - scanner-specific pattern file versions (up to date or old) - last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)
Blocked applications	Using application definitions published by LANDesk (or user-defined application definitions) to immediately deny end user access to the application by editing the local registry. Remediation is NOT a separate procedure. Patch and Compliance uses the LANDesk Software license monitoring tool's softmon.exe program to deny access to specified application executables, even if the executable file name has been modified, by reading the file header information. (See the legal disclaimer for the blocked application type.)

To understand how Patch and Compliance remediates these different content types, see the How Patch and Compliance remediates different security risks.

Configuring the content of a security scan

After reviewing downloaded definitions and deciding which items you want to scan for, you can perform customized security assessment on managed devices by moving definitions into their respective Scan groups. When the security scanner runs, it always reads the contents of the Scan group and scans for those specific definitions (**Important:** If that type is selected in the task's scan and repair settings). Before scanning devices, you should always make sure the appropriate definitions are in the Scan group. You can move definitions into and out of the Scan group manually at any time.

You can also update security content which, by default, automatically adds new definitions into the Scan group.

Blocked applications are placed in the Unassigned group by default
Keep in mind that the blocked application type is handled differently than the other types. By default, blocked application definitions are placed in the Unassigned group, not in the Scan group.

Security scans add patch and compliance information to a device's inventory in the core database. This information can be used to generate specific queries, policies, and reports. To view this information, right-click the device and then click **Security and Patch Information**.

Caution about moving definitions from the Scan group
When you move definitions from the Scan to the Don't Scan group, the current definition assessment information (information located in the core database about which scanned devices detected those definitions) is removed from the core database and is no longer available in either the definition Properties dialogs or in the device Security and Patch Information dialogs. To restore that information, you would have to move the definitions back into the Scan group and run the scan again.

Creating security and compliance scan tasks

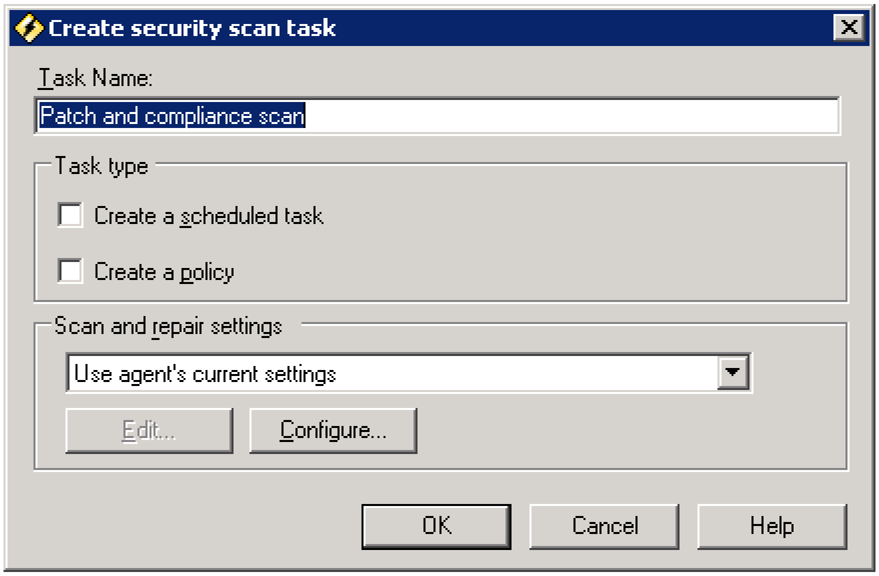
The security scanner can be run directly at a device (Click **Start | All Programs | LANDesk Management | Security Scanner**). The security scanner can also be run as a scheduled task or a policy from the core server.

IMPORTANT: LANDesk Script Writers group permission required
In order to create scheduled tasks and policies in the Patch and Compliance tool and the Security Configurations tool (for security and compliance scan tasks, repair tasks, and change settings tasks), a user must have the LANDesk Script Writers group permission. In other words, they must belong to a group that has the LANDesk Script Writers permission assigned. For more information about role-based administration, see Role-based administration.

Scheduled tasks can be thought of as a push distribution because the task is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.

To create a security scan task

1. Click **Tools > Security > Patch and Compliance**.
2. Make sure security content has been updated recently.
3. Make sure the **Scan** group contains only those definitions you want to scan for.
4. Click the **Create a task** toolbar button, and then click **Security scan**. The Create security scan task dialog displays.



Task Name: Patch and compliance scan

□ Create a scheduled task

□ Create a policy

Use agent's current settings

5. Enter a name for the scan.
6. Specify whether the scan is a scheduled task or a policy-based scan, or both.
7. Select a scan and repair settings from the available list (or create a custom settings for this scan), to determine how the scanner operates on end user devices.

8. Click **OK**. For a scheduled task scan, you can now add target devices and configure the scheduling options in the Scheduled tasks tool.

Compliance security scans
With the Patch and Compliance tool you can also create a compliance-specific scan task, that checks target devices for compliance with your customized security policy. A compliance scan is based on the contents of the **Compliance** group (and the options specified on the compliance settings), and can be run as a scheduled task, a policy, and even initiated by LANDesk Antivirus when a virus is detected that can't be removed or quarantined.

Running an on-demand security or compliance scan

You can also run an immediate on-demand scan on one or more target devices.

To do this, right-click the selected device (or up to 20 multi-selected devices), click **Security / Compliance scan now**, select a scan and repair settings, choose the type of scan, and then click **OK**.

About the security scan log file

The security scanner writes a log file for the most recent scan on the device called **vulscan.log**, and also saves the last five log files in chronological order by number. These log files record useful information about the time of the scan, language, platform, and the processes run by the scan.

Viewing the most recent security scan dates in the device Inventory

To see when the last security scan was run on a device, right-click the device, click **Inventory**, and then scroll down to the **Last Scan Dates** in the right-hand pane of the Inventory view.

Configuring scan options with scan and repair settings

Patch and Compliance gives you complete control over what the end user sees, device reboot behavior, and the level of interaction the end user is allowed when the security scanner runs on devices. For example, depending on the purpose or scheduled time of a scan you may want to show the end user scanner progress and give them the opportunity to cancel or defer an assessment scan or patch deployment remediation. You can do this by creating and applying scan and repair settings.

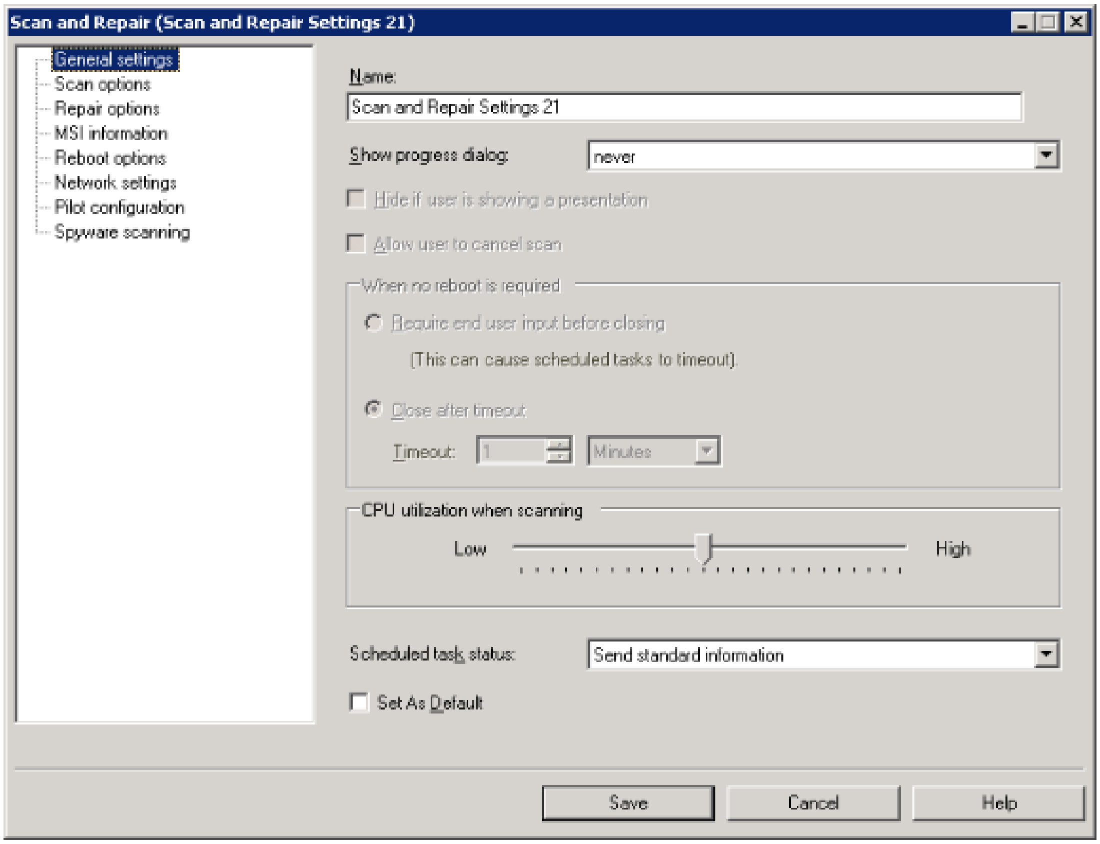
Scan and repair settings is also where you determine the content of a security scan, by selecting specific definition types.

You can create and apply scan and repair settings (a saved set of configured options) to scan tasks. You can create as many scan and repair settings as you like. Some scan and repair settings might be well suited for a variety of scanning or remediation tasks, while others might be specifically designed for a single task.

All of the scan and repair settings you create are stored in the **Scan and Repair** group located under **Settings** in the tree view.

To create scan and repair settings

1. In the **Patch and Compliance** tool window, click the **Configure settings** toolbar button, and then click **Scan and repair settings**.
2. Click **New**. Or, you can click **Edit** or **Configure** on any of the task dialogs that let you apply an scan and repair settings.



Name: Scan and Repair Settings 21

Show progress dialog: never

□ Hide if user is showing a presentation

□ Allow user to cancel scan

When no reboot is required

○ Require end user input before closing

(This can cause scheduled tasks to timeout)

● Close after timeout

Timeout: 1 Minutes

CPU utilization when scanning

Low — High

Scheduled task status: Send standard information

□ Set As Default

3. Enter a name for the scan and repair settings.
4. Specify the various settings on each page as desired for the particular task (scan, repair, reboot). For more information about an option, click **Help**.

Once configured, you can apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, reboot tasks, and change settings tasks.

Compliance settings
With the Patch and Compliance tool you can also create compliance-specific settings, that determine when the frequent security scan runs and how detected risks are remediated. A compliance scan is based on the contents of the **Compliance** group (and the options specified on the compliance settings), and can be run as a scheduled task, a policy, and even initiated by LANDesk Antivirus when a virus is detected that can't be removed or quarantined.

Changing a device's default scan and repair settings

A device's default scan and repair settings are deployed as part of the initial agent configuration. When a task has a different scan and repair settings associated or assigned to it, the default settings are overridden. You can also choose to use the device's default settings by selecting it when you create a task.

At some point you may want to change these default scan and repair settings on certain devices. Patch and Compliance provides a way to do this without having to redeploy an entirely new and complete agent configuration. To do this, use the **Change settings** task located in the drop-down list of the **Create a task** toolbar button.

The dialog that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select an existing scan and repair settings as the default or use the **Edit** button to create a new scan and repair settings as the default for target devices.

Using custom variables and custom variable override settings

With custom variables you can fine-tune security threat scanning by modifying one or more setting's values so that the scanner checks for conditions you define, and therefore determines a device to be vulnerable only if that condition is met (i.e., the value you specify is detected). Some system configuration security threat definitions have variable settings that you can change before including them in a security scan. Typically, antivirus definitions also have custom variable settings.

Edit Custom Variables right required
In order to edit custom variable settings, a LANDesk user must have the Edit Custom Variables role-based administration right. Rights are configured with the **Users** tool.

Every security definition with customizable variables has a unique set of specific values that can be modified. In each case however, the **Custom Variables** page will show the following common information:

- **Name:** Identifies the custom variable. The name can't be modified.
- **Value:** Indicates the current value of the custom variable. Unless the variable is read-only, you can double-click this field to change the value.
- **Description:** Provides additional useful information about the custom variable from the definition publisher.
- **Default value:** Provides the default value if you've changed the settings and want to restore it to its original value.

To change a custom variable, double-click the **Value** field, and either select a value if there's an available drop-down list, or manually edit the value, and then click **Apply**. Note that some variables are read-only and can't be edited (this is usually indicated in the description).

Custom variable override settings
In some situations you may want to ignore a custom variable settings, or in other words create an exception to the rule. You can do this with a feature called custom variable override settings. Custom variable override settings let you decide which custom variables to essentially ignore when scanning devices so that they are not detected as vulnerable and are not remediated even if they meet the actual conditions of a definition's detection rules. A user must have the Edit Custom Variables right in order to create or edit a custom variable override settings. You can create as many custom variable override settings as you like, and apply them to devices using a **Change settings** task. For more information, see About the Custom variable override settings dialog.

Viewing detected security data

If the security scanner discovers any of the selected definitions on target devices, this information is reported to the core server. You can use any of the following methods to view detected security data after running a scan:

By the Detected group

In the Patch and Compliance tool window, select the **Detected** group to view a complete listing of all definitions detected by the most recent scan.

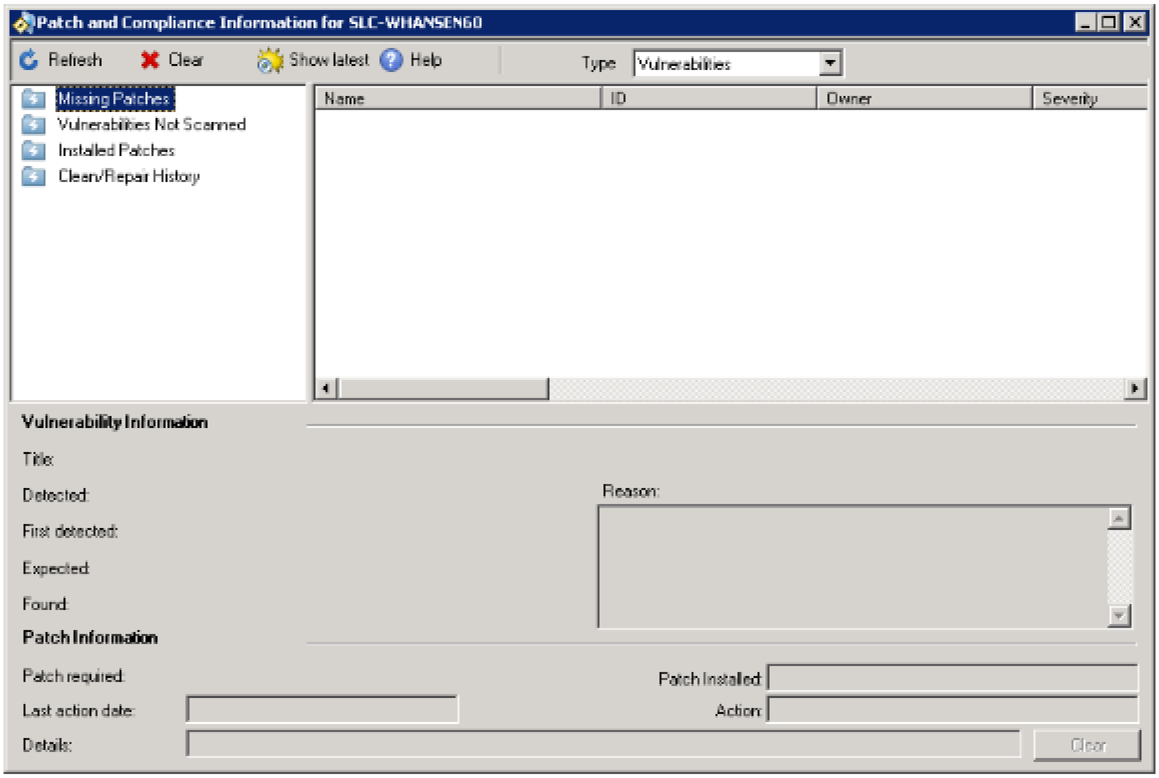
The Scanned column indicates how many devices were scanned for a definition, and the Detected column shows how many of those devices are affected by that definition.

By a definition

Right-click a definition, and then click **Affected computers** to view a list of devices on which the definition was detected by the most recent scan.

By the device Security and Patch Information dialog

Right-click a specific device in the network view, and then click **Security and Patch Information** to view detailed security assessment information and patch deployment status for the device.



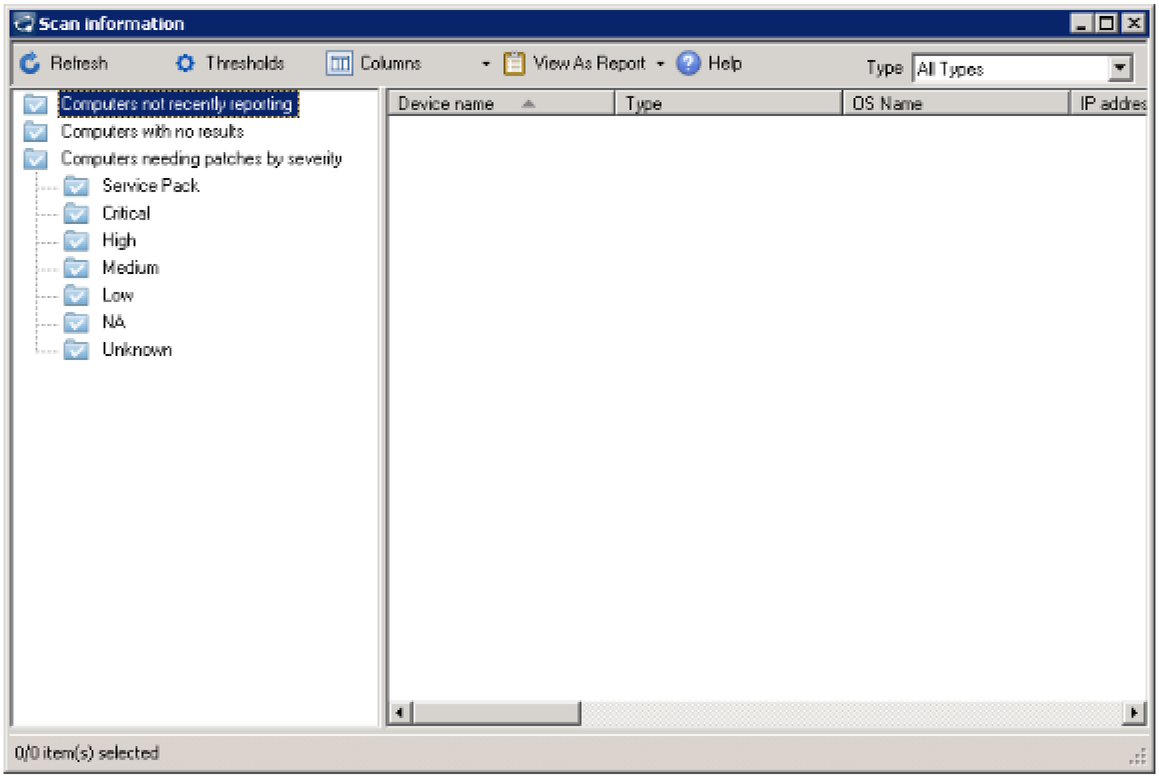
Patch and Compliance Information for SLC-WHANSEN60

Type: Vulnerabilities

You can also select multiple devices in the network view, right-click the group, and then click **Security and Patch Information** to view a list of definitions discovered on one or more of those devices. When you select a definition in the list, the devices on which the definition was detected by the most recent scan display in the bottom pane.

By the Scan Information dialog

In the Patch and Compliance tool window, click the **Scan information** toolbar button to view detailed patch deployment activity and status for scanned devices on your network. You can view scan results for computers not recently reporting, computers with no results, and computers needing patches by selected severity type.



Forwarding security scan results to a rollup core

If you're working in a large, distributed enterprise network, you may want to forward the latest security scan results to a rollup core server located in a specific region in order to facilitate access to real-time vulnerability information for all of your managed devices. You can enable automatic and immediate security scan results forwarding by defining the rollup core settings in the Patch and Compliance tool.

Every time the security scanner runs it writes a scan results file to a folder called VulscanResults on the core server and notifies the LANDesk Security web service, which adds the file to the core database. If the rollup core settings are enabled and a valid rollup core is identified, the rollup core reads the scan results file into its own database, providing faster access to critical vulnerability information.

To enable the immediate forwarding of security scan results to a rollup core

1. In the **Patch and Compliance** tool window, click the **Configure settings** toolbar button, and then click **Rollup core settings**.
2. Check the **Send scan results to rollup core immediately** checkbox.
3. Enter the name of the rollup core you want to receive the latest security scan results.
4. If you want to use the default URL (location on the rollup core) where the scan results file is written, check the **Use default rollup URL** checkbox. Otherwise, you can clear the checkbox and enter a preferred address.

Remediating devices that detected security risks

Once you've updated security content for the content types you've have a license or subscription for, scanned devices, determined which detected security exposures require attention, and downloaded patches, the next step in implementing Patch and Compliance security is to remediate (or repair) the security problem).

Remediation solutions and actions are different depending on the type of security risk. Furthermore, some remediation can be done remotely with the Patch and Compliance tool, while other remediation tasks must be done manually. For example, vulnerabilities are remediated by deploying and installing the necessary security patches on affected devices, while spyware is remediated by removing the infecting spyware itself, and a system configuration security threat is typically remediated by editing the registry or changing some other platform-specific settings.

Remediation for different security risks

Remediation for each type of security risk (i.e., content type) is described below:

Known vulnerabilities

For known vulnerabilities, remediation entails deploying and installing the appropriate security patch. Windows and Macintosh vulnerability remediation can be performed via the console, as a scheduled task, or policy-based remediation, or as an autofix scan. However, Linux and UNIX vulnerability remediation must be done manually at the affected device.

Custom definitions

For custom definitions, remediation can consist of deploying a custom patch or script that addresses the exposure. Like known vulnerability remediation, custom vulnerability repair tasks can be done via the console.

LANDesk software updates

For LANDesk software updates, remediation means the proper version upgrade is installed. You can do this via the console.

Security threats

For security threats (local Windows system or platform configuration errors and exposures), remediation means applying the configuration settings specified by the security threat definition. You can do this via the console. You can also modify security threat definitions that use editable custom variables to apply customized settings.

Some security threats must be remediated manually at the affected device. To find out whether a security threat can be remediated from the console, view its Repairable column value (Yes or No) in the item list view.

Firewall detection and configuration (using Windows firewall settings and security threat definitions)

For Windows firewall configurations, remediation means applying configuration settings specified by Windows firewall settings or predefined security threat definitions.

Windows firewall settings are associated with a change settings task to enable/disable the firewall, and configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, programs) on target devices running the following Windows platforms:

- Windows 2003/XP
- Windows Vista

Additionally, LANDesk Security provides predefined security threat definitions that let you scan for, detect, and configure firewall settings on managed devices running specific Windows platforms. The following security threat definitions let you scan for and modify firewall configurations:

- **ST000102:** Security threat definition for the Windows firewall on Windows 2003 SP1; Windows XP SP.
- **ST000015:** Security threat definition for the Internet Connection Firewall on Windows 2003 SP1; Windows XP SP2.

The Windows firewall security threat properties includes custom variables that let you configure Windows firewall settings. You can use these security threat definitions to scan for your specified settings and return a vulnerability condition if those settings are not matched. You can then use the customized definition in a repair task in order to turn on or off the firewall as well as change or reconfigure the firewall settings on the scanned device.

Windows GPO could change firewall settings
You should be aware that it is possible for a Windows Group Policy Object (GPO) to interfere with firewall settings configured with the security scanner. For example, the firewall settings you define in the Configure the Windows Firewall security threat's custom variables dialog and that are then implemented by a security scanner repair task could be changed back to their original value according to how the settings are defined in an active Group Policy Object.

Spyware

For spyware, remediation consists of removing the violating spyware application. This can be done remotely from the console with a repair task.

You can also configure a device for real-time spyware monitoring (scanning, detection, and removal). In order to use real-time spyware monitoring, you must enable the settings in the device's agent configuration. On the **Spyware** page of the **Agent configuration** dialog, check the appropriate spyware monitoring options to enable real-time spyware monitoring and end user notification. Real-time spyware monitoring uses the LANDesk Software license monitoring tool's softmon.exe program to monitor for spyware and to create log files that are read by the security scanner when it scans for spyware definitions on target devices.

Autofix must be enabled for real-time spyware monitoring
In order for real-time spyware scanning and detection to work, downloaded spyware definitions must have the autofix option enabled. You can manually enable the autofix option for spyware definitions in item lists in the Patch and Compliance tool window. Or you can configure spyware definition updates so that the autofix option is turned on by default when spyware definitions are downloaded.

Blocked applications

For blocked applications, remediation is NOT a separate task. Application blocking takes place as part of the security scan itself, by editing the registry on the local hard drive to disable user access to any unauthorized applications.

Patch and Compliance uses the LANDesk Software license monitoring tool's softmon.exe program to deny access to specified application executables, even if the executable file name has been modified, by reading the file header information.

Antivirus updates

Antivirus updates are available for several common antivirus products, including LANDesk Antivirus. See the **Definition types** list in the **Download updates** dialog to see the antivirus scanner engines that are supported, meaning the antivirus scanners you can download detection definitions for.

Antivirus scanner detection content versus virus definition content
Antivirus updates does not imply actual virus definition (or pattern) files. When you download third-party antivirus updates, only scanner detection content is downloaded to the default repository, but scanner-specific virus definition files are not downloaded. However, when you download LANDesk Antivirus updates, both the scanner detection content AND the LANDesk Antivirus-specific virus definition files are downloaded. LANDesk Antivirus virus definition files are downloaded to a separate location on the core server. The default virus definition file repository is the \LDLogon\Antivirus\Bases folder.

Antivirus updates are scanner definitions that detect:

- Installation of common antivirus scanner engines (including the LANDesk Antivirus tool)
- Real-time scanning status (enabled or disabled)
- Scanner-specific pattern file versions (up to date or old)
- Last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)

When you deploy a security scan with antivirus scanner detection definitions, the security scanner checks whether an antivirus scanner engine is installed on managed devices, whether real-time scanning is enabled or disabled, whether the scanner's pattern files is up to date, and when the latest scan was run on the device. You can remotely enable real-time scanning if it's turned off.

How Patch and Compliance remediates different security risks

The table below describes how Patch and Compliance remediates each type of security risk:

When remediating...	Patch and Compliance remediates by...
LANDesk software updates	Deploying and installing the appropriate LANDesk software update.
Windows vulnerabilities	Deploying and installing the required patch files (patch files must already be downloaded to the local patch repository).
Macintosh vulnerabilities	Deploying and installing the required patch files
Linux/UNIX vulnerabilities	Remediation is performed manually at the affected device.
Custom definitions	Deploying and installing patch files, if the associated detection rule allows remediation, and if the specified patch files are available.
Security threats	Applying configuration settings specified by the security threat definition. You can do this via the console. You can also modify security threat definitions that use editable custom variables to apply customized settings. Some security threats must be remediated manually at the affected device. To find out whether a security threat can be remediated from the console, view its Repairable column value (Yes or No) in the item list view.
Spyware	Removing the detected spyware instance. See the spyware section above for more information on real-time spyware detection and removal.

When remediating...	Patch and Compliance remediates by...
Driver updates	Deploying and installing the appropriate third-party driver update.
Software updates	Deploying and installing the appropriate third-party software update.
Antivirus updates	Allowing you to re-enable real-time scanning if it's been turned off. The other antivirus scanner detection definitions return status information about specific antivirus scanner engine installations, pattern file versions, and last scan dates (related issues can't be remediated remotely from the console).
Blocked applications (published and custom)	Denying access to the application, even if the program's executable file name has been changed, by reading the file header information. Remediation in this case is NOT a separate procedure. Application blocking is done during the security scan process. The security scan immediately denies end user access to the application by editing the registry. (See the Legal disclaimer for the blocked applications type.)

To understand how Patch and Compliance scans for these different content types, see the How Patch and Compliance scans for different security risks.

Remediating from the console

As stated above, Windows and Macintosh vulnerabilities, custom definitions, LANDesk software updates, and blocked applications can be remediated from the console. The Remediation methods section below describes these different methods.

Intelligent patch deployment remediation

Patch and Compliance performs an intelligent remediation by installing only those patches that are needed on each individual device, not all of the patches referenced by all of the vulnerabilities included in the repair job. The tool also takes advantage of LANDesk's enhanced package deployment capabilities for fast and efficient patch deployment, such as: Targeted Multicast, peer download, and checkpoint restart. For more detailed information about these software distribution features, see Software distribution.

Remediating one or more definitions at a time

You can remediate a single detected definition or a set of them with any of the three remediation methods described below.

To remediate one definition at a time, right-click the item and then click **Repair**.

To remediate a set of definitions together, copy definitions from any of the content groups into a custom group (see Understanding and using the Patch and Compliance tool, right-click the group, and then click **Repair**). The Auto Fix method isn't available for custom groups; however, you can multi-select definitions in a listing, right-click and select **Auto Fix**.

Remediating Linux and UNIX devices manually

Supported Windows and Macintosh devices can be remediated remotely from the console, but other platforms such as Linux and UNIX Sun Solaris can only be scanned from the console, not remediated.

You must manually install the appropriate patches on both Linux and UNIX devices in order to remediate them.

Remediation methods

Patch and Compliance provides the following methods to remediate affected devices from the console:

- Using a scheduled repair task
- Using a repair policy (Windows only)
- Using an autofix repair

Scheduled task remediation can be thought of as a push distribution because the patch is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.

Using a scheduled repair task

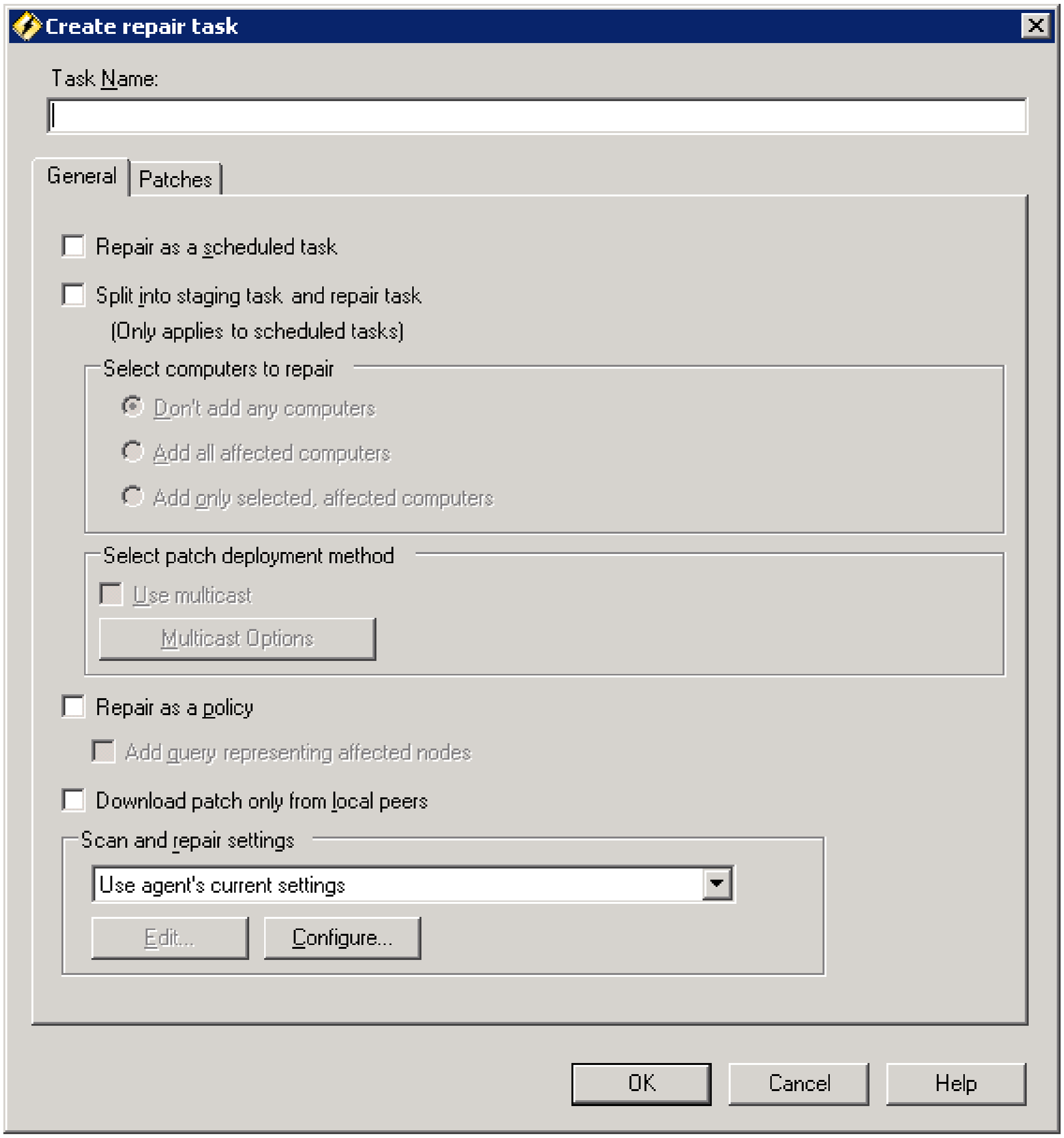
Scheduling a remediation or repair task is useful if you want to set up the task to run at a specific time in the future, or as a recurring task. Patch and Compliance uses the Scheduled Tasks tool to configure and process a scheduled repair task.

Scheduled task remediation is supported on both Windows and Macintosh devices.

IMPORTANT: LANDesk Script Writers group permission required
In order to create scheduled tasks and policies in the Patch and Compliance tool and the Security Configurations tool (for security and compliance scan tasks, repair tasks, and change settings tasks), a user must have the LANDesk Script Writers group permission. In other words, they must belong to a group that has the LANDesk Script Writers permission assigned. For more information about role-based administration, see Role-based administration.

To create a scheduled repair task

1. Click **Tools > Security > Patch and Compliance**.
2. Right-click a single definition from one of the content groups, or right-click a custom group of definitions, and then click **Repair**. Or, you can click the **Create a task** toolbar button, and then click **Repair**. The Create repair task dialog displays.


Create repair task
Task Name:
General
Patches
□ Repair as a scheduled task
□ Split into staging task and repair task
(Only applies to scheduled tasks)
Select computers to repair
● Don't add any computers
○ Add all affected computers
○ Add only selected, affected computers
Select patch deployment method
□ Use multicast
Multicast Options
□ Repair as a policy
□ Add query representing affected nodes
□ Download patch only from local peers
Scan and repair settings
Use agent's current settings
Edit...
Configure...
OK
Cancel
Help

3. Edit the **Task name** if you want to change the name of the repair task.
4. Click the **Repair as a scheduled task** check box.
5. (Optional) If you want this repair task to be divided into two parts: a staging task that deploys the necessary patches to affected devices, and the actual repair task that installs the patch, click the **Split into staging task and repair task**.
6. Specify which devices you want to repair. If you want the current affected devices automatically added to the target list in the Scheduled Tasks window, click the **Add all affected devices** check box. The vulnerable devices are those devices where the vulnerability was detected by the last scan. You can also add more targets once the task is created in the Scheduled Tasks window.
7. If you want patches to be deployed using Targeted Multicast, check the **Use multicast** check box. To configure Multicast options, click the **Multicast Options** button. See About the Multicast options dialog below for details.

8. If you want to use peer download strictly for patch deployment, click the **Download patch only from local peers** check box. If this option is selected, the patch file is only deployed if it currently resides in either the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, it must be in one of these two places.
9. Specify whether to only download the patch and not deploy and install it on affected devices.
10. Select a scan and repair settings for this repair task. The scan and repair settings determines the scanner display, reboot, and user interaction behavior on scanned devices, as well as the actual content that is being scanned.
11. Click **OK**.
12. The task appears in the Scheduled Tasks window with the job name specified above, where you can further customize the target device list and configure scheduling options.

Using a repair policy (Windows only)

Policy-based remediation offers flexibility by letting you dynamically target devices based on the results of a custom LDAP or core database query. For example, you can configure a remediation policy so that it runs only on devices in a particular directory container, or only on devices running a specific OS (or any other inventory attribute that can be queried). Patch and Compliance uses policies in the Scheduled tasks/Software distribution tool to configure and process remediation policies.

Supported platforms for policy-based remediation
Policy-based remediation is supported on Windows devices only. Macintosh devices can't be remediated via the application policy method.

In order to be remediated by a policy, a device must have the Software distribution agent installed. When the agent runs, it checks the core database for policies that might apply to it. If such policies exist, a dialog appears at the device showing recommended and optional policies (required policies are automatically applied).

Remediation (repair) policies operate in much the same way as application policies do, except you're distributing patch files instead of application files. Policy management prerequisites, task flow, policy types, and static and dynamic targeting are essentially identical between repair policies and application policies.

To create a policy-based remediation

1. Click **Tools > Security > Patch and Compliance**.
2. Right-click a single definition from one of the content groups, or right-click a custom group of definitions, and then click **Repair**. Or, you can click the **Create a task** toolbar button, and then click **Repair**. The Create repair task dialog displays.
3. Edit the **Task Name** if you want to change the name of the repair task.
4. Check the **Repair as a Policy** check box.
5. If you want to create a new query, based on this vulnerability definition, that can be used later to scan other managed devices, check the **Add a query** check box.
6. If you want to use peer download strictly for patch deployment, click the **Download patch only from local peers** check box. If this option is selected, the patch file is only deployed if it currently resides in either the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, it must be in one of these two places.
7. Specify whether to only download the patch and not deploy and install it on affected devices.

8. Select a scan and repair settings for this repair policy. The scan and repair settings determines the scanner display, reboot, and user interaction behavior on scanned devices, as well as the actual content that is being scanned.
9. Click **OK**.
10. The new policy appears in the Policies group in the Scheduled Tasks window with the name specified above. From there you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Using an autofix repair

Auto Fix is a convenient, integrated method for quick remediation in cases where you don't want to create a scheduled task or policy-based repair task. For example, if there is a new known vulnerability that you want to scan for and repair in a single process, you can use the Auto Fix feature.

Auto fix is available for the following content types: vulnerabilities, spyware, LANDesk software updates, and custom definitions.

Requirements for using Auto Fix
Only Administrators or users with the Patch Manager right AND the Default All Machines scope can enable the Auto Fix feature for applicable definitions. LANDesk users without either the LANDesk Administrator or Patch Manager right won't even see this option on a definition's shortcut (right-click) menu. For more information on rights and scope, see Role-based administration.

Auto fix has to be enabled in two places in order to work properly. First, the auto-fix option must be turned on, and secondly the scan and repair settings must be applied to the scheduled scan task. If either one of these two item's autofix option is NOT enabled, autofix will not happen.

When Auto Fix is enabled in both places mentioned above, the next time the security scanner runs (either manually or via a scan task), Patch and Compliance automatically deploys and installs the required patch on any affected device. With Auto Fix, if a patch requires a reboot, the target device always automatically reboots.

You can enable Auto Fix for an individual definition, or a multi-selected group of definitions at once.

To configure Auto Fix remediation

1. In the **Patch and Compliance** tool window, right-click one or more selected definitions from one of the content groups, and then click **Autofix when scanning**. (**Note:** You can't enable autofix on a custom group.)
2. Now run the security scanner on the devices you want to scan and automatically remediate using a scheduled security scan task with an scan and repair settings where the autofix option is enabled.

What happens on a device during remediation

Automated remediation entails deploying and installing patches on managed devices, by any of the three methods described in the sections above.

It is important to remember that a repair job can include remediation for one or more detected security definitions. Furthermore, a single detected definition can require the installation of one or more patches to fix. Because of these factors, remediation might imply the installation of just one patch file on the device, or the installation of several patch files on the device, depending on the number and type of detections.

Almost all patch files install silently, meaning transparently, requiring no user interaction at the end user device itself. Some Windows 9.x patches and non-English patches do not install silently. You can tell whether a patch installs silently or not by checking the Silent Install column in a patch listing. For more information, see Understanding and using the Patch and Compliance tool earlier in this section.

Configuring security scanner display and interaction on end user devices

However, whether a patch file can install silently or not, you can now configure how much you want the security scanner to display and prompt for input on the end user device with the scan and repair settings feature.

Consolidated reboot
If a patch file installation requires a reboot (AND the **Never reboot** option isn't selected on the Reboot page of the scan and repair settings applied to the task in question), Patch and Compliance first installs ALL of the specified task's patches on the device, and then reboots the device once.

Additional commands (for custom definitions only)

Custom definition remediation can include special additional commands that are defined when you create a custom detection rule. Additional commands run in the order specified on that rule's Commands tab, and according to the arguments for each command. Additional commands can run before, during, or after the patch file itself executes.

Viewing patch and compliance information for scanned devices

As mentioned above, one way to view scanned security data is by device. To do this, right-click a single device or a group of selected devices, and then click **Security and Patch Information**.

This page provides many useful functions. With one or more devices selected, you can:

- View detected definition lists
- View detailed information about when and why the detection occurred
- View installed patch and software update lists
- View detailed information about when the patch was installed or uninstalled
- Clear patch install status
- View repair history data
- Clear repair history data

You can also right-click definitions and detection rules in their respective item lists to run common tasks for one or more affected devices.

Viewing the most recent security scan dates in the device Inventory

To see when the last security scan was run on a device, right-click the device, click **Inventory**, and then scroll down to the various **Last Scan Dates** in the right-hand pane of the Inventory view.

Verifying remediation status

After performing remediation on affected devices, Patch and Compliance reports the status of each patch installation. You can check the status of patch installation per vulnerability/definition and per target device.

To verify patch installation on a device

1. Run the security scanner on the device.
2. Right-click a remediated device in the network view, and then click **Security and Patch Information**.
3. Click the **Installed Patches** object in the left-hand pane.
4. Check the **Patch Information** fields at the bottom of the dialog.

The **Install status** field indicates whether the installation was successful. Possible states include: Succeeded, Failed, and Failed to Download.

Clearing vulnerability scan and repair status by vulnerability

If a patch installation failed, you must first clear the install status information before attempting to install the patch again. You can clear the install (repair) status for the selected device by clicking **Clear** on the **Security and Patch Information** dialog. You can also clear the patch install status by vulnerability.

You can clear vulnerability scan and repair status information for all devices affected by a vulnerability (or vulnerabilities with the **Clear scan/repair status dialog**. As stated above, if a patch installation fails, you must first clear the install (repair) status before attempting to install the patch again.

You can also use this dialog to remove vulnerability scan information from the database for one or more vulnerabilities.

To clear vulnerability scan and repair status, right-click the vulnerability and select **Clear scan/repair status**, select the desired options, and then click **Clear**.

Other patch and compliance management tasks

The following section describes other tasks you can perform with the Patch and Compliance tool.

Creating a scheduled reboot task

Patch and Compliance provides a tool that lets you create a device reboot task. A reboot task can be useful when you want to install patches, without rebooting, as a single process and then reboot those remediated devices as another separate task. For example, you can run a scan or a patch install task during the day, and then deploy a reboot only task at a more convenient time for end users.

To create a reboot task

1. Click **Tools > Security > Patch and Compliance**.
2. Click the **Create a task** toolbar button, and then click **Reboot**.
3. Specify whether the reboot is a scheduled task or a policy-based scan, or both.
4. Select a scan and repair settings from the available list (or create a custom settings just for this scan task), to determine how the scanner operates on end user devices. (**Note:** Only the reboot settings in the scan and repair settings are used by a reboot task.)
5. Click **OK**. For a scheduled task, you can now add target devices and configure the scheduling options in the Scheduled tasks tool. For a policy, the new policy appears in the Application Policy Management window with the task name specified above, where you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Using patch and compliance alerts

You can configure patch and compliance security alerting so that you can be notified when specific vulnerabilities are detected on managed devices in your system. Patch and Compliance's vulnerability alerting uses the standard LANDesk alerting tool.

A vulnerability must copied to the Alert group in order to generate an alert when detected. A vulnerability in the Alert group is a copy, and also resides in the Scan group. After placing the desired vulnerability definitions in the Alert group (either manually, or by specifying the severity level vulnerabilities to automatically be placed during downloads), you can configure the alert interval in the Configure alerts dialog.

To configure alerting

1. Specify which vulnerabilities will generate an alert by manually placing downloaded vulnerability definitions into the Alert group.
2. Or click the **Configure settings** toolbar button, and then click **Alert settings**.
3. Specify a minimum alert interval for alerting.
4. To configure security alerting, select the definitions (by severity level) you want to be automatically placed in the **Alert** group during a download process. You can select more than one vulnerability severity level. These vulnerability definitions will also automatically be placed in the Scan group.

5. If you want to configure antivirus alerting, select the antivirus events you want to generate alerts.
6. Click **OK**.

Using patch and compliance reports

Patch and Compliance information is represented by several reports in the Reports tool. These reports provide useful information about security risk assessment, compliance, patch deployment, and remediation status for scanned devices on your network, for each of the various security risk content types.

In order to access the Reports tool, and generate and view reports, a user must have the LANDesk Administrator right (implying full rights) and the specific Reporting roles.

For more information about using the Reports tool, see Reports.

Security Configurations

The new Security Configurations tool provides a convenient single window where you can create and manage configurations for several LANDesk Security Suite components and services, as well as corresponding deployment tasks.

Security configurations (i.e., settings) control how security services operate on managed devices. Security services and their associated settings can be deployed to your managed devices as part of the initial agent configuration, separate install or update tasks, and change settings tasks.

Security Configurations lets you create and manage settings for the following security services:

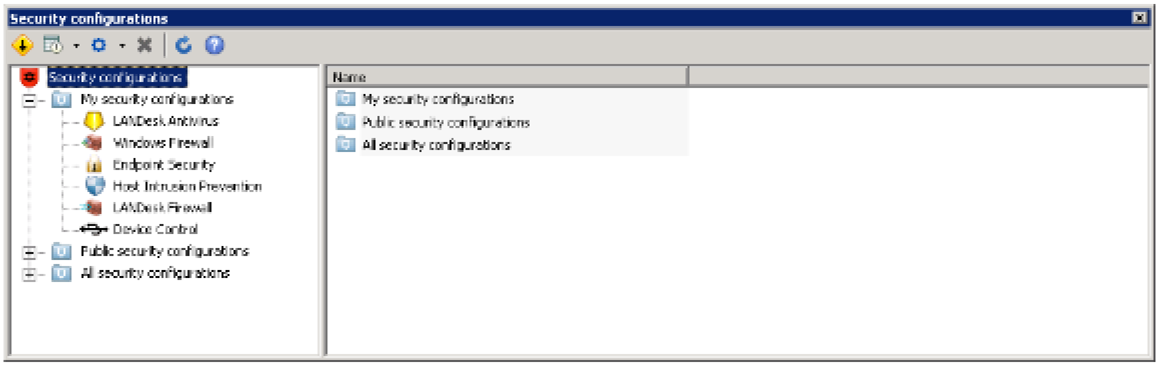
- Antivirus
- Windows Firewall
- Endpoint Security (HIPS, LANDesk Firewall, Device Control)
- Alert settings for security
- Authorization codes

You can also perform security component tasks described below.

IMPORTANT: LANDesk Script Writers group permission required
In order to create scheduled tasks and policies in the Patch and Compliance tool and the Security Configurations tool (for security and compliance scan tasks, repair tasks, and change settings tasks), a user must have the LANDesk Script Writers group permission. In other words, they must belong to a group that has the LANDesk Script Writers permission assigned. For more information about role-based administration, see "Role-based administration" on page 44.

Using the Security Configurations tool

The Security Configurations tool window provides a convenient single interface that lets you manage settings and tasks for several security components and services.


Security configurations
Security configurations
My security configurations
LANDesk Antivirus
Windows Firewall
Endpoint Security
Host Intrusion Prevention
LANDesk Firewall
Device Control
Public security configurations
All security configurations
Name
My security configurations
Public security configurations
All security configurations

Read the sections below to learn about:

- "Configuring antivirus definition downloads" on page 356
- "Creating change settings tasks" on page 356
- "Creating install or update security components tasks" on page 359
- "Creating remove security components tasks" on page 360
- "Creating LANDesk Antivirus tasks" on page 361
- "Configuring alert settings" on page 362
- "Generating security authorization codes" on page 363

Configuring antivirus definition downloads

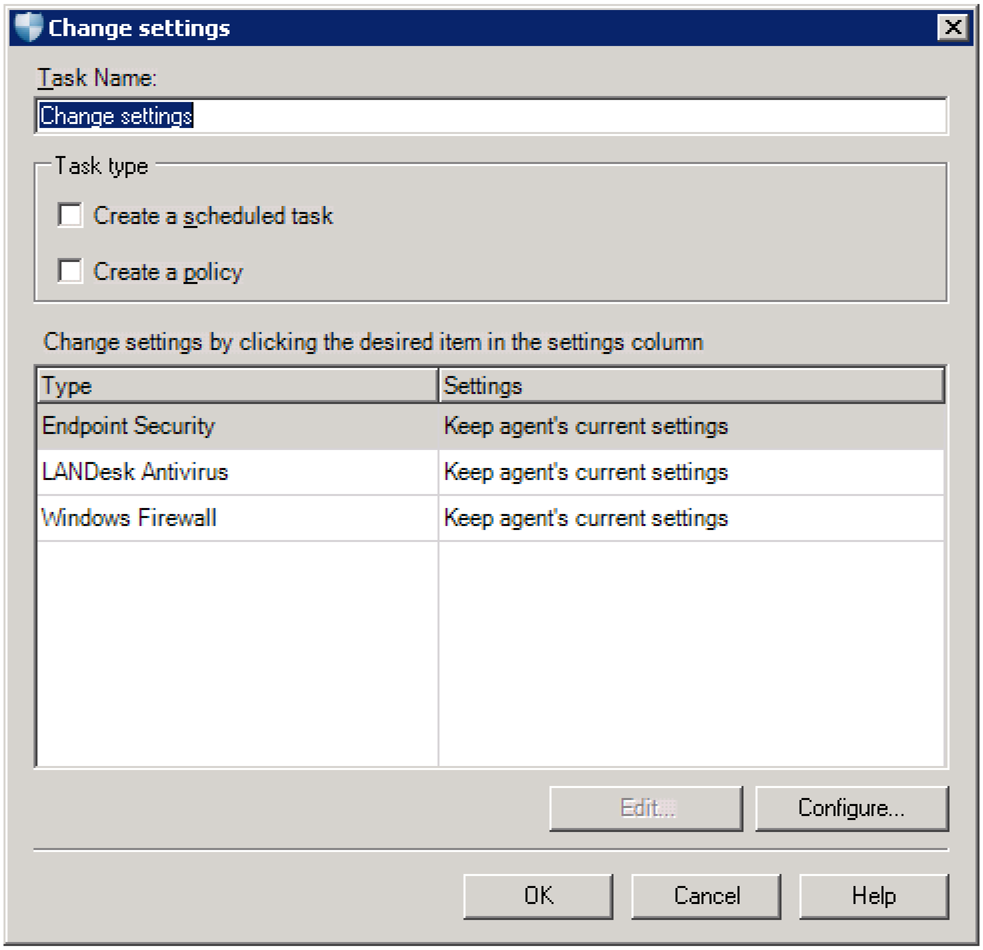
The steps below provide a quick summary outline of the typical processes or tasks involved in implementing antivirus protection on your network with LANDesk Antivirus. Each of these procedures are described in detail in the "LANDesk Antivirus" on page 366 section.

For more information about the specific task of downloading antivirus definitions, see "Updating virus definition files" on page 373.

Creating change settings tasks

The device default security settings are deployed as part of the initial agent configuration. At some point you may want to change these default settings on certain devices. The Security Configurations tool provides a way to do this without having to redeploy an entirely new and complete agent configuration.

To do this, click the **Change settings** task located in the **Create a task** toolbar button.



Change settings

Task Name:

Change settings

Task type

□ Create a scheduled task

□ Create a policy

Change settings by clicking the desired item in the settings column

Type	Settings
Endpoint Security	Keep agent's current settings
LANDesk Antivirus	Keep agent's current settings
Windows Firewall	Keep agent's current settings

The dialog that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select an existing settings as the default or use the Edit button to create a new settings as the default for target devices.

About the Create change settings task dialog

Use this dialog to create and configure a task that changes the default settings on target devices for Endpoint Security components.

With a change settings task you can conveniently change a managed device's default settings (which are written to the device's local registry) without having to redeploy a full agent configuration.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Type:** Identifies the security component.
- **Endpoint Security:** Specifies the Endpoint Security settings associated with this particular change settings task. Keep in mind that although Endpoint Security is a single agent that is deployed to target devices, it provides services for several security components, including: Location awareness (network connections), HIPS, LANDesk

Firewall, and Device Control. Select the settings you want to deploy to target devices, modify an existing settings by selecting the settings and clicking **Edit**, or create a new settings by clicking **Configure | New**.

- **Antivirus:** Specifies antivirus settings used for antivirus scan tasks. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates. Select one of the settings from the drop-down list. Click **Edit** to modify the options for the selected settings. Click **Configure** to create a new settings. For more information, see "About the LANDesk Antivirus settings dialog" on page 602.
- **Windows Firewall:** Specifies Windows firewall settings on target devices. You can enable and disable the firewall, and configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, programs).

About the Configure security component settings dialog

Use this dialog to manage your security components settings. Once configured, you can apply settings to agent configuration tasks, security components install or update tasks, and change settings tasks.

This dialog contains the following options:

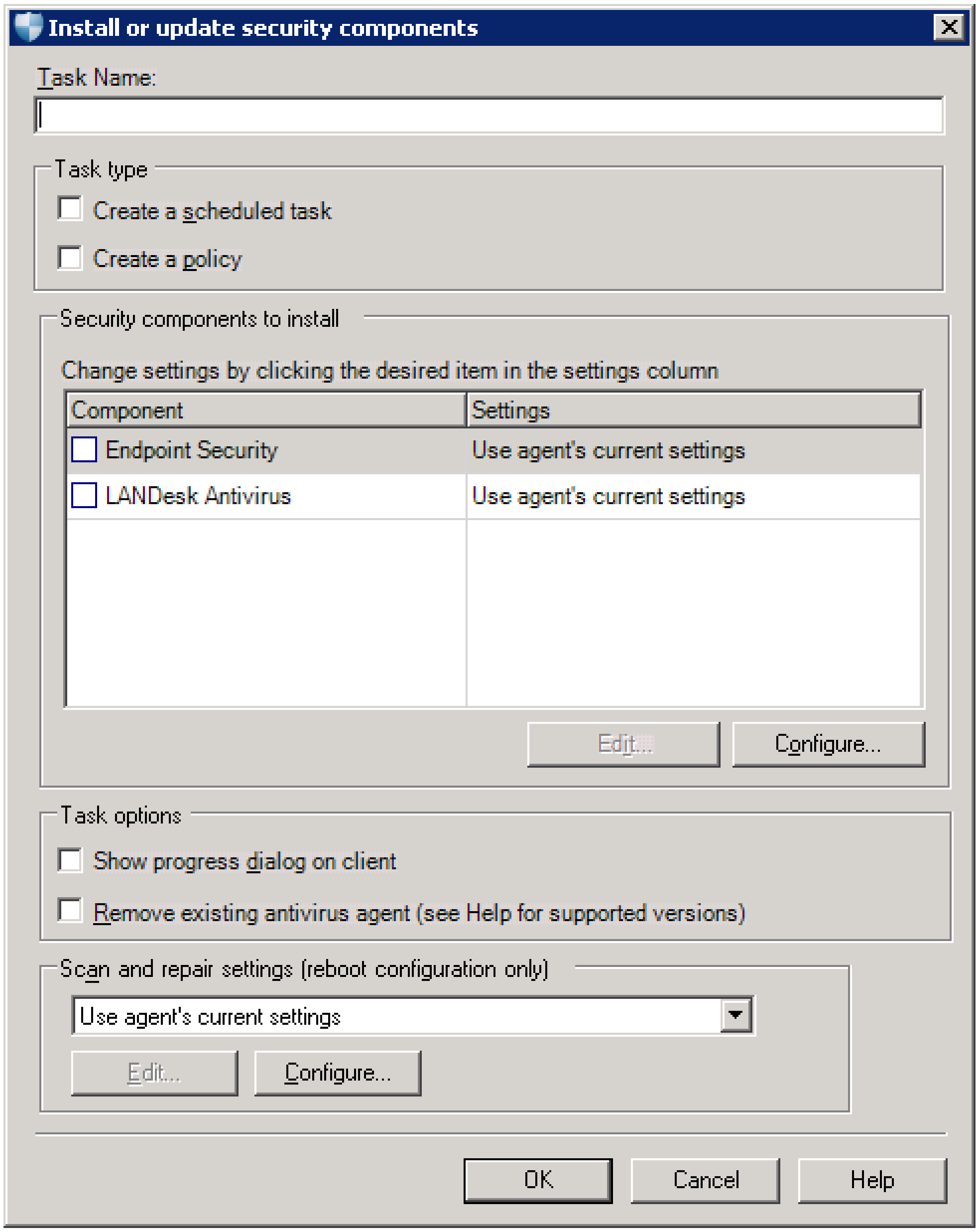
- **New:** Opens the settings dialog where you can configure the various options.
- **Edit:** Opens the settings dialog where you can modify the selected settings.
- **Copy:** Opens a copy of the selected settings as a template, which you can then modify and rename. This is useful if you want to make minor adjustments to settings and save them for a specific purpose.
- **Delete:** Removes the selected settings from the database. (Note the selected settings may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that settings still have it and continue to use it until a new change settings task is deployed; scheduled tasks with that settings still run on target devices, as do local scheduler tasks with that settings, until a new configuration is deployed.)
- **Use selected:** Indicates that the currently selected settings will be used for the task.
- **Close:** Closes the dialog without applying any settings to the task.

Creating install or update security components tasks

If you want to install or update security components, you can do so as a separate task.

To create an install or update security components task

1. In the console, click **Tools > Security > Security Configurations**.
2. Click the **Create a task** toolbar button, and then click **Install/Update security components**.



Install or update security components

Task Name:

Task type

□ Create a scheduled task

□ Create a policy

Security components to install

Change settings by clicking the desired item in the settings column

Component	Settings
□ Endpoint Security	Use agent's current settings
□ LANDesk Antivirus	Use agent's current settings

Task options

□ Show progress dialog on client

□ Remove existing antivirus agent (see Help for supported versions)

Scan and repair settings (reboot configuration only)

Use agent's current settings

3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.

5. Select the component you want to install. You can create a new settings or edit an existing settings by clicking **Configure**.
6. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show progress dialog on client** option.
7. Select a Scan and repair settings from the list to apply its reboot configuration (only) to the agent configuration you're creating. You can create a new settings or edit and existing settings by clicking **Configure**. Keep in mind that ONLY the reboot options specified on the Scan and repair settings you select are used by this agent configuration's Endpoint Security agent deployment to target devices. You can use an existing Scan and repair settings that already includes the reboot configuration you want, or you can create a brand new Scan and repair settings specifically for your agent deployment.
8. Click **OK**.

About the Install or update security components task dialog

Use this dialog to create and configure a task that installs the security components (via the shared Endpoint Security agent) on target devices that don't yet have it installed, or updates the existing version of the security components on target devices.

Note: The installation is executed by the security scanner.

This task lets you conveniently deploy and update a managed device's security components (and associated settings) without having to redeploy a full agent configuration.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Security components to install:** Specifies which security components will be installed with the task. Check the component you want to install. Click in the **Settings** column to select an existing settings. Click **Edit** to modify the options for the selected settings. Click **Configure** to create a new settings.
- **Show progress dialog on client:** Indicates whether the security scanner dialog displays the progress of the installation on target devices.
- **Remove existing antivirus agent:** Automatically removes other antivirus software that might already be installed on devices before installing LANDesk Antivirus (see the list below). (**Note:** You can also select to remove existing antivirus software from managed devices when doing an initial agent configuration.)
- **Scan and repair settings (reboot only):** Specifies the scan and repair settings associated with this particular installation. The task will use the selected scan and repair settings' reboot options ONLY, which determine reboot requirements and actions on target devices during installation.

List of third-party antivirus products that can be automatically removed

To see the current list in the main LANDesk Antivirus section, go to: "List of third-party antivirus products that can be automatically removed" on page 371.

Creating remove security components tasks

If you want to remove security components from managed devices, you can also do that as a separate task from the console.

To create a remove security components task

1. In the console, click **Tools > Security > Security Configurations**.
2. Click the **Create a task** toolbar button, and then click **Remove security components**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. Select the component you want to remove.
6. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show progress dialog on client** option.
7. Select a scan and repair settings from the available list to apply its reboot configuration to the task you're creating. You can create a new settings or edit an existing settings by clicking **Configure**. The task will use the selected scan and repair settings' reboot options ONLY, which determine reboot requirements and actions on target devices during agent removal.
8. Click **OK**.

About the Remove security components task dialog

Use this dialog to create and configure a task that removes the security components from target devices.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Security components to remove:** Specifies which security components will be removed with the task. Check the component you want to remove.
- **Show progress dialog on client:** Indicates whether the security scanner dialog displays the progress of the agent removal from target devices.
- **Scan and repair settings (reboot only):** Specifies the scan and repair settings associated with this particular agent removal task. The task will use the selected scan and repair settings' reboot options ONLY, which determine reboot requirements and actions on target devices during agent removal.

Creating LANDesk Antivirus tasks

The LANDesk Antivirus tool is described in a separate section. For detailed information about antivirus tasks, see "LANDesk Antivirus" on page 366.

Configuring alert settings

You can configure security-related alerting so that you can be notified when specific events are detected on managed devices in your system. Security Antivirus uses the standard LANDesk alerting tool.

The alert settings dialog contains options for both vulnerability alerting and antivirus alerting.

Antivirus alerting

To configure antivirus alerting

Antivirus alert settings are found on the **Antivirus** tab of the **Alert settings** dialog.

You must first configure the antivirus alerts in the Alert Settings tool in the console. Antivirus alerts include:

- An alertable antivirus action failed
- An alertable antivirus action succeeded
- Virus outbreak alert (per virus)

The following antivirus events can generate antivirus alerts:

- Virus removal failed
- Virus removal succeeded
- Quarantine failed
- Quarantine succeeded
- Deletion failed
- Deletion succeeded

Select which alerts you want generated. The time interval option lets you prevent too many alerts. More than one alert (for any antivirus trigger) during the specified time interval is ignored.

You can view the complete antivirus alert history for a device in its Security and Patch Information dialog. Right-click a device, select Security and Patch Information, select the Antivirus type in the Type drop-down list, and then select the Antivirus History object.

Vulnerability alerting

For information on vulnerability alerting, see "Using patch and compliance alerts" on page 353.

Generating security authorization codes

Use this dialog create an authorization code that will allow an end user to perform a blocked operation for a brief period of time. You can use an authorization code to provide temporary access for a specific user or for an IT administrator to have access to a managed device.

For example, if a user attempts to connect a USB device that is not allowed by a Device Control settings, a pop-up message displays on the end user device that includes an operation code. The user would provide that operation code to the administrator, who uses it to generate an authorization code that is given back to the end user that allows them to perform the action on a temporary basis.

To generate an authorization code

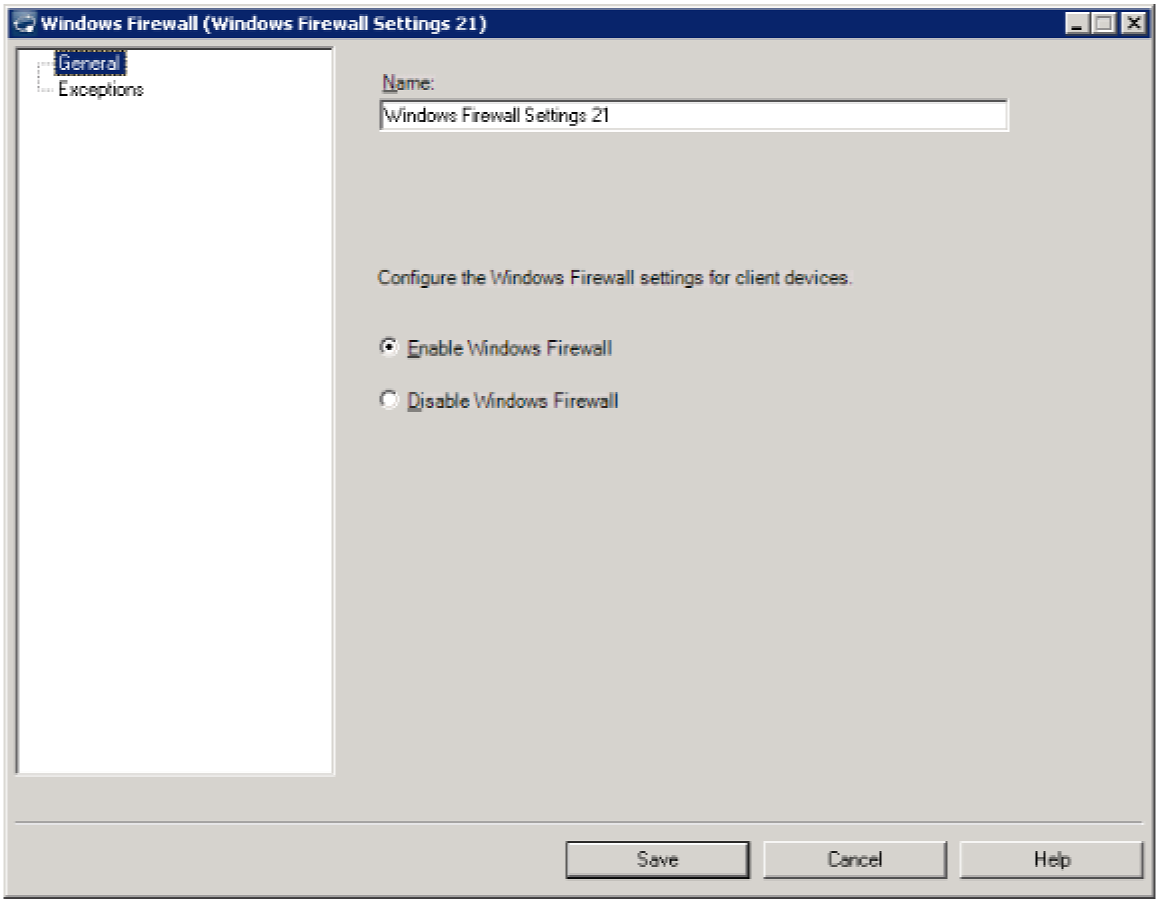
1. In the **Security Configurations** tool, click the **Common settings** toolbar button, and then click **Generate authorization code**.
2. Enter the operation code provided by the end user.
3. If the operation code is valid, an authorization code is automatically generated.
4. Enter the operation type that the end user wishes to perform.
5. Now you can give the new authorization code to the end user, which they can use to perform the blocked operation.

Note about inaccurate pop-up message
When a user is given access via an authorization code, a pop-up message on the end user device may indicate that HIPS has been disabled regardless of the actual action taken by the user. This message can be ignored.

Using Windows Firewall settings

The Security Configurations tool also lets you create, configure, and deploy a Windows Firewall settings to manage the Windows firewall on target devices.

To create a settings, right-click **Windows Firewall**, and then click **New**.



Name: Windows Firewall Settings 21

Configure the Windows Firewall settings for client devices.

● Enable Windows Firewall

○ Disable Windows Firewall

Once configured, you can deploy settings to target devices with an installation or update task, or a change settings task.

About the Create Windows Firewall settings dialog

Use these dialogs to configure Windows firewall settings. Windows firewall settings are associated with a change settings task to enable/disable the firewall, and configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, and programs).

You can use this feature to deploy a configuration for the Windows firewall on the following Windows versions:

- Windows 2003
- Windows XP (SP2 or later)
- Windows Vista

About the Windows Firewall (XP/2003): General page

Use this page to define firewall general settings.

About the Windows Firewall (XP/2003): Exceptions page

Use this page to configure firewall exceptions.

This dialog contains the following options:

- **Current exceptions:** Lists programs, ports, and services whose connection/communication is NOT being blocked by the firewall. The firewall prevents unauthorized access to devices, except for the items in this list.
- **Add program:** Lets you add a specific program to the exception list to allow communication.
- **Add port:** Lets you add a specific port to the exception list to allow communication.
- **Edit:** Lets you edit to the selected exception's properties, including the scope of affected devices.
- **Delete:** Removes the selected exception from the list.
- **OK:** Saves your changes and closes the dialog.
- **Cancel:** Closes the dialog without saving your changes.

Windows firewall security threat definitions

Additionally, LANDesk Security provides predefined security threat definitions that let you scan for, detect, and configure firewall settings on managed devices running specific Windows platforms. The following security threat definitions let you scan for and modify firewall settings:

- **ST000102:** Security threat definition for the Windows firewall on Windows 2003, and Windows XP.
- **ST000015:** Security threat definition for the Internet Connection Firewall on Windows 2003, and Windows XP.

The Windows firewall security threat properties includes custom variables that let you configure Windows firewall settings. You can use these security threat definitions to scan for your specified settings and return a vulnerability condition if those settings are not matched. You can then use the customized definition in a repair task in order to turn on or off the firewall as well as change or reconfigure the firewall settings on the scanned device.

About the Windows Firewall (Vista): General rules page

Use this page to configure firewall general rules.

About the Windows Firewall (Vista): Inbound rules

Use this page to configure firewall inbound rules.

About the Windows Firewall (Vista): Outbound rules

Use this page to configure firewall outbound rules.

LANDesk Antivirus

LANDesk Antivirus is one of the major components of LANDesk Security Suite. Antivirus protects your managed devices from malicious virus attacks by scanning and cleaning viruses based on the latest known virus definition files.

Antivirus offers configurable virus protection features, including: both scheduled and on-demand virus definition file updates, pilot tests, configurable antivirus scan operation and end user interactive options, infected object handling, real-time file and email protection, status and activity views, reports, and more.

Read this section to learn about:

Antivirus overview

LANDesk Antivirus is comprised of a built-in antivirus agent scanner, a continuously updated virus signature database, and antivirus configuration options and features available in the Security Configurations tool.

Antivirus agent
The Antivirus agent is distinct from the Patch and Compliance security scanner.

LANDesk Security Suite services maintains a current database of virus definition/pattern files that can be downloaded, evaluated and tested, and distributed to target devices on your network.

With Antivirus, you can:

- Download the latest virus definition\pattern file updates (the LANDesk Security Suite service's antivirus signature database is updated several times a day)
- Schedule recurring virus definition file updates
- Archive previous virus definition files
- Create and deploy Antivirus agent installation tasks
- Run on-demand and scheduled antivirus scans on target devices
- Configure antivirus scan behavior and end user options
- Select which types of files to scan, and whether to scan for riskware
- Enable real-time file and email virus protection
- Scan for third-party antivirus scanner engines, and enable/disable real-time virus scanning and ensure up-to-date virus pattern files for those specific antivirus products
- View antivirus activity and status information for scanned devices
- Configure antivirus alerts
- Generate antivirus reports

Security content types and subscriptions

When you install LANDesk Management Suite or LANDesk Security Suite, the Patch and Compliance tool is included by default. However, without a Security Suite content subscription, you can only scan for LANDesk software updates and custom definitions. A Security Suite content subscription enables you to take full advantage of the Patch and Compliance tool (and Security Configurations tool) by providing access to additional security content (definition types), including antivirus scanner detection rules and the actual Antivirus virus definition files used by the antivirus scanner.

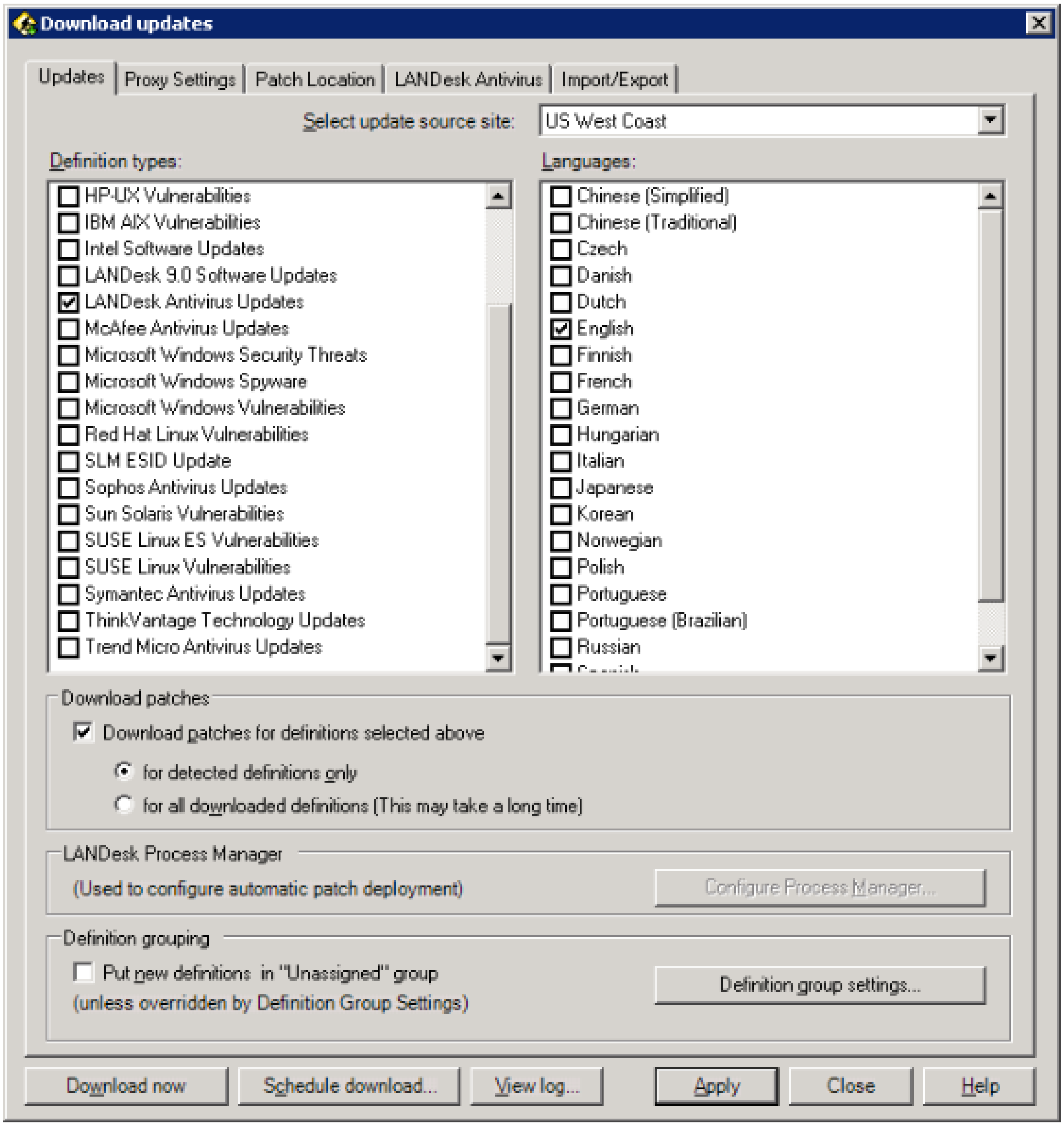
Security content types include:

- Antivirus updates (for third-party scanners, includes antivirus scanner detection content only; for Antivirus, includes both scanner detection content AND virus definition files, as well as riskware definition files available in an extended database)
- Blocked applications (see the "Legal disclaimer for the blocked applications type" on page 314)
- Custom vulnerability definitions
- Driver updates
- LANDesk software updates
- Security threats (system configuration exposures; includes firewall detection and configuration)
- Software updates
- Spyware
- Vulnerabilities (known platform vulnerabilities, and application-specific vulnerabilities)

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Using Download Updates

Note that the **Updates** page of the **Download updates** dialog includes several antivirus updates in the definition types list, including one named LANDesk Antivirus Updates. When you select LANDesk Antivirus Updates, both the scanner detection content AND the LANDesk Antivirus virus definition file updates are downloaded.



Select update source site: US West Coast

Definition types:

- □ HP-UX Vulnerabilities
- □ IBM AIX Vulnerabilities
- □ Intel Software Updates
- □ LANDesk 9.0 Software Updates
- ☑ LANDesk Antivirus Updates
- □ McAfee Antivirus Updates
- □ Microsoft Windows Security Threats
- □ Microsoft Windows Spyware
- □ Microsoft Windows Vulnerabilities
- □ Red Hat Linux Vulnerabilities
- □ SLM ESID Update
- □ Sophos Antivirus Updates
- □ Sun Solaris Vulnerabilities
- □ SUSE Linux ES Vulnerabilities
- □ SUSE Linux Vulnerabilities
- □ Symantec Antivirus Updates
- □ ThinkVantage Technology Updates
- □ Trend Micro Antivirus Updates

Languages:

- □ Chinese (Simplified)
- □ Chinese (Traditional)
- □ Czech
- □ Danish
- □ Dutch
- ☑ English
- □ Finnish
- □ French
- □ German
- □ Hungarian
- □ Italian
- □ Japanese
- □ Korean
- □ Norwegian
- □ Polish
- □ Portuguese
- □ Portuguese (Brazilian)
- □ Russian
- □ Spanish

Download patches

☑ Download patches for definitions selected above

● for detected definitions only

○ for all downloaded definitions (This may take a long time)

LANDesk Process Manager

(Used to configure automatic patch deployment)

Definition grouping

□ Put new definitions in "Unassigned" group
(unless overridden by Definition Group Settings)

For third-party scanner engines, antivirus updates include scanner definitions that detect:

- Installation of common antivirus scanner engines (including the Antivirus tool)
- Real-time scanning status (enabled or disabled)
- Scanner-specific pattern file versions (up to date or old)
- Last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)

For the Antivirus scanner, antivirus updates includes not only the scanner detection content listed above, but also the virus definition files used by the Antivirus scanner.

Antivirus scanner detection content versus virus definition content
Antivirus updates does not imply actual virus definition/pattern files. When you download third-party antivirus updates, only scanner detection content is downloaded to the default repository, but scanner-specific virus definition files are not downloaded. However, when you download Antivirus updates, both the scanner detection content AND the Antivirus-specific virus definition files are downloaded. Antivirus virus definition files are downloaded to a separate location on the core server. The default virus definition file repository is the \LDLogon\Antivirus\Bases folder.

Supported device platforms

Antivirus supports most of the same platforms supported by Patch and Compliance's security scanning capabilities and the standard LANDesk-managed device platforms, including the following operating systems:

- Windows NT (4.0 SP6a and higher)
- Windows 2000 SP2
- Windows 2003
- Windows XP SP1
- Windows XP 64-bit
- Windows XP Home Edition/Professional
- Windows Vista (32-bit, and 64-bit)

Reboot required for Windows NT 4.0 machines
In order for the Antivirus service to be activated, Windows NT 4 machines must be rebooted after agent configuration deployment.

Other system requirements

Make sure the managed devices you want to configure with the Antivirus agent meet the following system requirements:

- Microsoft Internet Explorer 6.0 or higher
- No other antivirus products installed (For information on automatically removing antivirus products, see "Deployment considerations" on page 371.)

Role-based administration with Antivirus

LANDesk Antivirus, just like Patch and Compliance, uses role-based administration to allow users access to features. Role-based administration is the access and security framework that lets Administrators restrict user access to tools and devices. Each user is assigned specific roles and scope that determine which features they can use and which devices they can manage.

Administrators assign these roles to other users with the Users tool in the console. Antivirus is included in the Security Configurations right, which appears under the Security rights group in the Roles dialog. In order to see and use Antivirus features, a user must be assigned the necessary Security Configurations access rights.

IMPORTANT: LANDesk Script Writers group permission required
In order to create scheduled tasks and policies in the Patch and Compliance tool and the Security Configurations tool (for security and compliance scan tasks, repair tasks, and change settings tasks), a user must have the LANDesk Script Writers group permission. In other words, they must belong to a group that has the LANDesk Script Writers permission assigned. For more information about role-based administration, see "Role-based administration" on page 44.

With the Security Configurations right, you can provide users the ability to:

- Deploy agent configurations with Antivirus to target devices

- Download virus definition file updates
- Create scheduled updates
- Create scheduled antivirus scan tasks
- Create antivirus settings
- Deploy antivirus scan tasks and change settings tasks associated with antivirus settings
- Enable real-time file and email protection
- Configure antivirus scans to scan for certain file types
- Exclude certain files, folders, and file types (by extension) from antivirus scans
- View antivirus scan activity and status information for scanned devices
- Enable antivirus alerts.
- Generate antivirus reports (also requires Reporting roles)

Antivirus task workflow

The steps below provide a quick summary outline of the typical processes or tasks involved in implementing antivirus protection on your network with LANDesk Antivirus. Each of these procedures are described in detail in subsequent sections.

Basic steps in implementing and using LANDesk Antivirus:

1. Configure managed devices for antivirus scanning.
2. Download virus definition/pattern file definition updates from a security content server.
3. Determine whether to make virus definition files available to managed devices immediately, or to first evaluate them in a pilot test environment.
4. Create on-demand and scheduled antivirus scan tasks and policies.
5. Configure antivirus settings to determine scan operation and end user options.
6. Scan managed devices for known viruses and suspicious files.
7. View antivirus scan results for scanned devices.
8. Configure antivirus alerts.
9. Generate antivirus reports.

Configuring devices for Antivirus protection

Before managed devices can be scanned for viruses and cleaned, they must have the Antivirus agent installed. You can do this either during initial device agent configuration or with a separate installation or update task.

Deployment considerations

If you deploy Antivirus to a device that already has another antivirus solution installed and running, Antivirus does not enable its real-time protection functionality in order to avoid any potential software conflicts. Once you remove the other antivirus product, you can enable Antivirus real-time antivirus protection.

You can select to automatically remove existing antivirus software from target devices when deploying LANDesk Antivirus, either during initial agent configuration or as a separate Antivirus install/update task. For a current list of antivirus products that can be removed from devices, see "List of third-party antivirus products that can be automatically removed" on page 371.

Clear password protected antivirus software
If the existing antivirus software is password protected, you must first clear the password before Antivirus can uninstall the software.

List of third-party antivirus products that can be automatically removed

Other antivirus products that can be automatically removed when deploying (or updating) LANDesk Antivirus include:

- Symantec* Antivirus (versions 7, 8, 9, 10)
- Symantec Endpoint Protection 11
- McAfee* Enterprise (versions 7.0, 8.0i, 8.5)
- McAfee ePolicy Orchestrator EPO
- Trend Micro* PC-cillin (versions 2004, 2005, 2006, 2007 15.3 on Windows Vista 64-bit)
- Trend Micro OfficeScan
- Trend Micro ServerProtect
- Trend Micro Internet Security 2008
- CA eTrust* Antivirus (versions 6, 7.x, 8, 8.1)

Configuring devices for Antivirus protection

To configure devices with Antivirus via an agent configuration

1. In the console, click **Tools > Configuration > Agent Configuration**.
2. Click the **New Windows** toolbar button.
3. After specifying your desired settings for the agent configuration, you must first click the **Start** page, and select the **LANDesk Antivirus** option. Now you can access the options on the **LANDesk Antivirus** page.
4. Click the **Security and Compliance** group, and then click **LANDesk Antivirus**.
5. If you want to automatically remove an existing antivirus product from target devices, check the **Remove existing antivirus agent** option. For a current list of antivirus products that can be removed from devices, see "List of third-party antivirus products that can be automatically removed" on page 371.
6. Select an antivirus settings from the available list to apply it to the agent configuration you're creating. You can create a new settings or edit an existing settings by clicking

Configure. Antivirus settings determine whether the Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates.

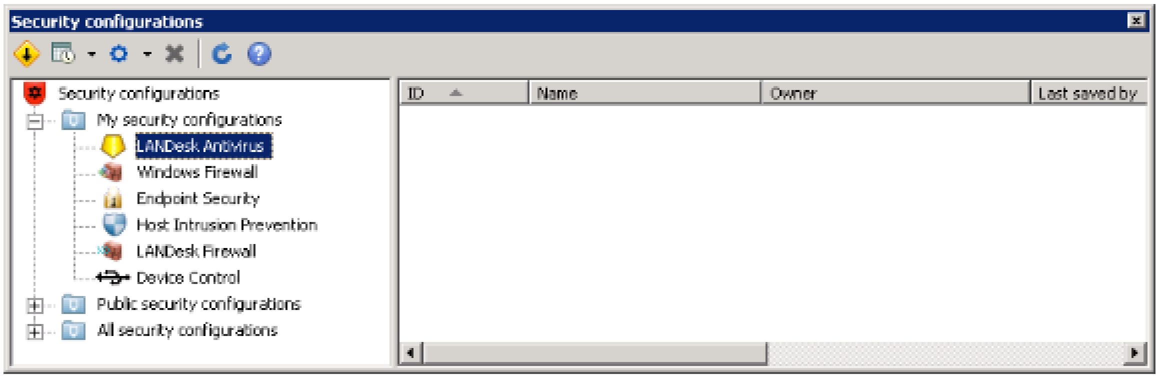
7. Finish specifying any other desired settings for the agent configuration and then click **Save**.

You can also configure devices for Antivirus with the Security Configurations tool.

Using the Security Configurations tool

If you want to install or update Antivirus at a later time, you can do so as a separate task from the console.

Use the Security Configurations tool (**Tools > Security > Security Configurations**) to create install or update tasks, remove tasks, and antivirus definition file update and scan tasks.



To install or update Antivirus as a separate task

1. In the console, click **Tools > Security > Security Configurations**.
2. Click the **Create a task** toolbar button, and then click **Install or update security components**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. Select the component you want to install, in this case select LANDesk Antivirus. You can select an antivirus settings from the available list to apply it to the task you're creating. You can also create a new settings or edit an existing antivirus settings.
6. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show progress dialog on client** option.
7. If you want to automatically remove an existing antivirus product from target devices, check the **Remove existing antivirus agent** option. For a current list of antivirus products that can be removed from devices, see "List of third-party antivirus products that can be automatically removed" on page 371.
8. Select a scan and repair settings from the available list to apply its reboot configuration to the task you're creating. You can create a new settings or edit an existing settings by clicking **Configure**. The task will use the selected scan and repair settings' reboot options ONLY, which determine reboot requirements and actions on target devices during Antivirus agent installation.
9. Click **OK**.

Removing Antivirus from devices

If you want to remove Antivirus from managed devices, you can also do that as a separate task.

To remove Antivirus

1. In the console, click **Tools > Security > Security Configurations**.
2. Click the **Create a task** toolbar button, and then click **Remove security components**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show progress dialog on client** option.
6. Select a scan and repair settings from the available list to apply its reboot configuration to the task you're creating. You can create a new settings or edit an existing settings by clicking **Configure**. The task will use the selected scan and repair settings' reboot options ONLY, which determine reboot requirements and actions on target devices during Antivirus agent removal.
7. Click **OK**.

Updating virus definition files

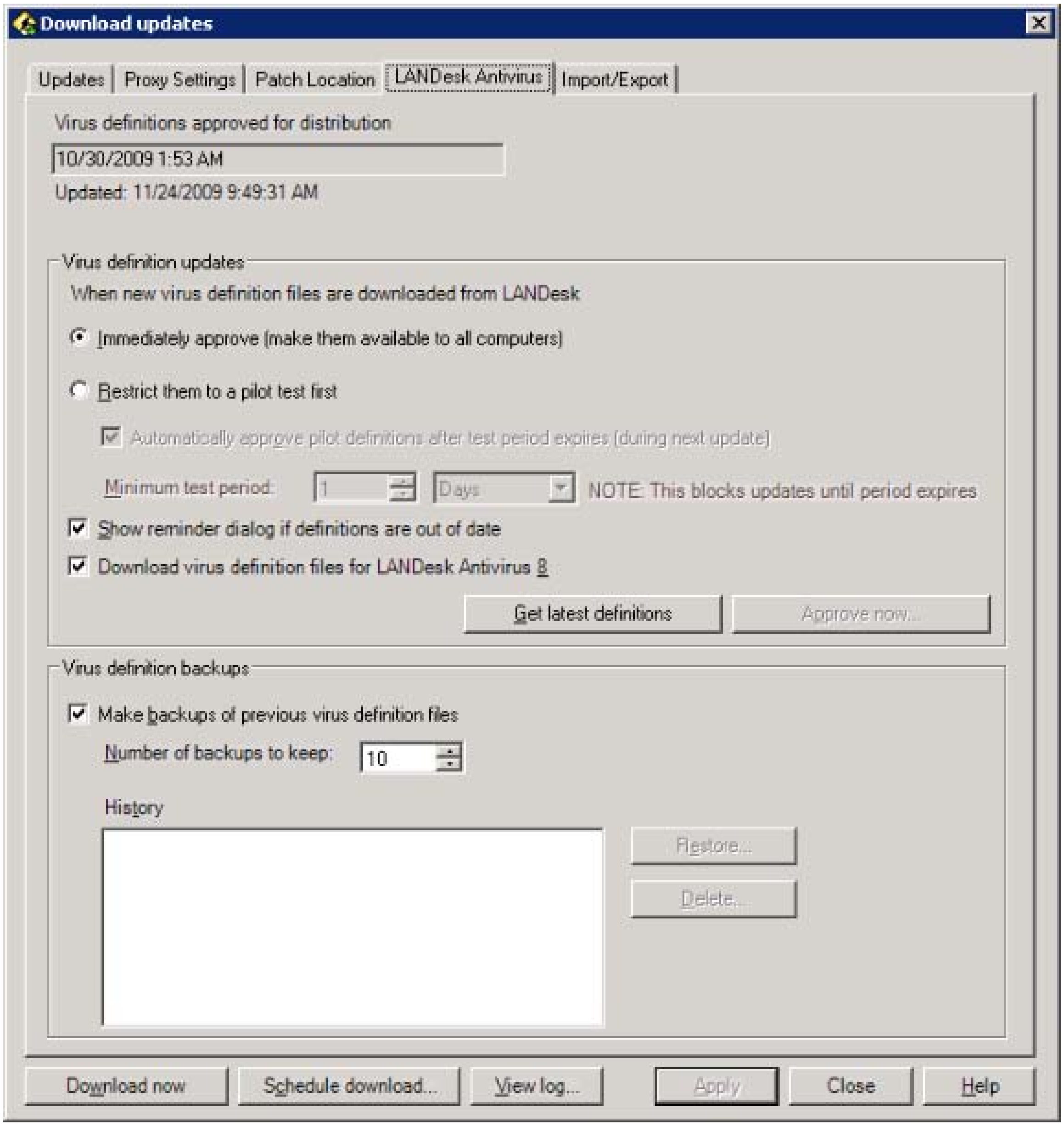
Antivirus lets you download the most current virus definition files from the LANDesk Security Suite content servers. The virus signature database is updated several times a day in order to ensure you have all of the latest known virus definitions so that you can protect your managed devices from these rapidly evolving threats.

You can download virus definition file updates from the console, either immediately as a one-time task or as a regularly scheduled task.

Using Download Updates for virus definition files

Use Download updates (**Security Configurations > Download Updates**) to specify where definition files are copied, whether they are stored in the default virus definition file repository where they are deployed to target devices or in a pilot test folder where they can be deployed to a limited scope of devices in order to test them before full deployment.

You can also access this dialog directly when creating an Antivirus task. For more information, see "Scanning devices for viruses" on page 377.



Virus definitions approved for distribution

10/30/2009 1:53 AM

Updated: 11/24/2009 9:49:31 AM

Virus definition updates

When new virus definition files are downloaded from LANDesk

● Immediately approve (make them available to all computers)

○ Restrict them to a pilot test first

☑ Automatically approve pilot definitions after test period expires (during next update)

Minimum test period: 1 Days NOTE: This blocks updates until period expires

☑ Show reminder dialog if definitions are out of date

☑ Download virus definition files for LANDesk Antivirus 8

Virus definition backups

☑ Make backups of previous virus definition files

Number of backups to keep: 10

Deploying virus definition files to end user devices
The virus definition updates that you download can be deployed to end user devices remotely from the core server. From their own computer, users can also perform the task of updating virus definition files. By default they download files from their LANDesk core server. However, if they need to be able to download the latest virus definition updates while they're not connected to the network (for example, while traveling or using a laptop), you can provide the option of letting users download files directly from the LANDesk security content server via an Internet connection.

To download virus definition file updates

1. Click **Tools > Security > Security Configurations**.
2. Click the **Download updates** toolbar button. The dialog opens to the **Antivirus** page. (You can also access the **Download updates** dialog from the Patch and Compliance tool.)
3. At the **Updates** page, select the update source site from the list of available content servers. Choose the one closest to your location.

4. At the **Updates** page, select **Antivirus Updates** in the Definition types list. (You can select more than one definition type for a single download. However, you must have the corresponding depending on your LANDesk Security Suite content subscription. The more types you select, the longer the update will take.)
5. At the **Updates** page, select the languages whose content you want to update for the types you've specified.
6. If you want new content (content that does not already reside in any groups in the tree) to automatically be placed in the Unassigned group instead of the default location, which is the Scan group, check the **Put new definitions in the Unassigned group** check box.
7. Now click **LANDesk Antivirus** to view the current status of virus definition files and to configure specific virus definition file updates settings.
8. If you want virus definition files to be downloaded to the default repository on the core server (\LDLogon\Antivirus\Bases) where they can be deployed to target devices, click **Immediately approve**. However, if you want to first evaluate virus definition files, before deploying them to your managed devices, click **Restrict definitions to a pilot test first**. (You can also set an automatic approval time period, and minimum test period, to avoid having to do this manually after the test). If you choose to do a pilot test first, virus definition files are downloaded to a pilot test folder so that they are deployed to only those devices whose antivirus settings says to download the "pilot" version of definition files.
9. If you want a pop-up message to display on the core server console when virus definition files have not been updated in the past seven (7) days, click **Show reminder dialog if definitions are out of date**.
10. If you want to download the latest definition files right now, click **Get latest definitions**. The **Updating Definitions** dialog displays the current operation and status.
11. If you want to approve virus definitions currently residing in the pilot test folder, click **Approve now**. This moves definition files from the pilot test folder to the default folder (\LDLogon\Antivirus\Bases).
12. If you want to save a backup copy of the virus definition files currently residing in the Bases folder, check the **Make backups** option. You can restore definition file backups at anytime. Backups are useful if you want to revert to an earlier virus definition file version. (Virus definition file backups are saved in separate folders named by the date and time they were created, under: \LDLogon\Antivirus\Backups\)
13. Click **Download Now** to download your selected security content updates. The **Updating Definitions** dialog displays the current operation and status. Or you can click the **Schedule download** button to create a scheduled task (see below).
14. When the update has completed, click **Close**. Note that if you click **Cancel** before the update is finished, only the security content that has been processed to that point is downloaded to the core database. You would need to run the update again in order to obtain all of the remaining security content.

Note: Whenever virus definition files are updated on managed devices, a mini-scan of memory processes runs on the device. This scan is performed to ensure that the processes running in memory at the time of the update are still clean.

Scheduling automatic virus definition file updates

You can also configure virus definition file updates as a scheduled task to occur at a set time in the future, or as a recurring task.

To do this, configure security content download options in the **Update downloads** dialog, making sure to select LANDesk Antivirus updates in the definition type list on the **Updates** tab, configure virus definition file options on the **LANDesk Antivirus** tab, and then click the **Schedule Update** button. The **Scheduled update information** dialog shows task-specific settings for the task. Enter a name for the task, and then click **OK** to create a Download Security Content task in the Scheduled Tasks tool, where you can specify the scheduling options.

Task-specific settings and global settings
Note that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific. However, all of the settings on the other pages of the **Download updates** dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global settings it is effective for all security content download tasks from that point on.

Evaluating virus definition files with a pilot test

You may want to first evaluate virus definition files before deploying them to all of your managed devices. You can easily do this by specifying to restrict virus definition file updates to a pilot test folder, and then applying an antivirus settings with the **Download pilot version of virus definition files** option selected.

To run a pilot test of virus definition files

1. On the **Download update** dialog's **LANDesk Antivirus** tab, click **Restrict them to a pilot test first**.
2. If you don't want to have to manually move tested virus definition files from the pilot test folder to the default folder (\LDLogon\Antivirus\Bases), click **Automatically approve**, and specify the minimum time period. When this time period elapses, the virus definition files are automatically approved and moved.
3. To download the most recent virus definition files from the LANDesk security content server, click **Get latest definitions**.
4. To immediately approve the virus definition files currently residing in the pilot test folder, click **Approve now**.
5. Next, create a pilot test antivirus settings that allows you to deploy virus definition files to a limited set of testing machines. On the antivirus setting's **Virus definition updates** page, select **Download pilot version of definition files**.
6. Apply that pilot test antivirus settings to an antivirus scan task that you can use to target your limited set of test machines. Now you can observe the antivirus scan activity and results on these devices in order to evaluate the effectiveness of the downloaded virus definition files before deploying them to a wider audience.

Backing up virus definition files

If you want to save older versions of downloaded virus definition files, use the **Virus definition backups** settings on the **LANDesk Antivirus** tab.

Backing up virus definition files can be very useful if you need to go back to an older virus definition file to scan and clean specific infected files, or to restore a virus definition file that resolved a particular problem.

Virus definition file backups are saved in separate folders, named by the date and time the files were saved, under the parent \LDLogon\Antivirus\Backups\ folder.

Scanning devices for viruses

This section provides information on scanning managed devices for known viruses as well as suspicious objects.

Scanning requires the proper content subscription
Remember that in order to scan for a specific security content type, including viruses, you must have the corresponding LANDesk Security Suite content subscription. For information about content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Scanning methods

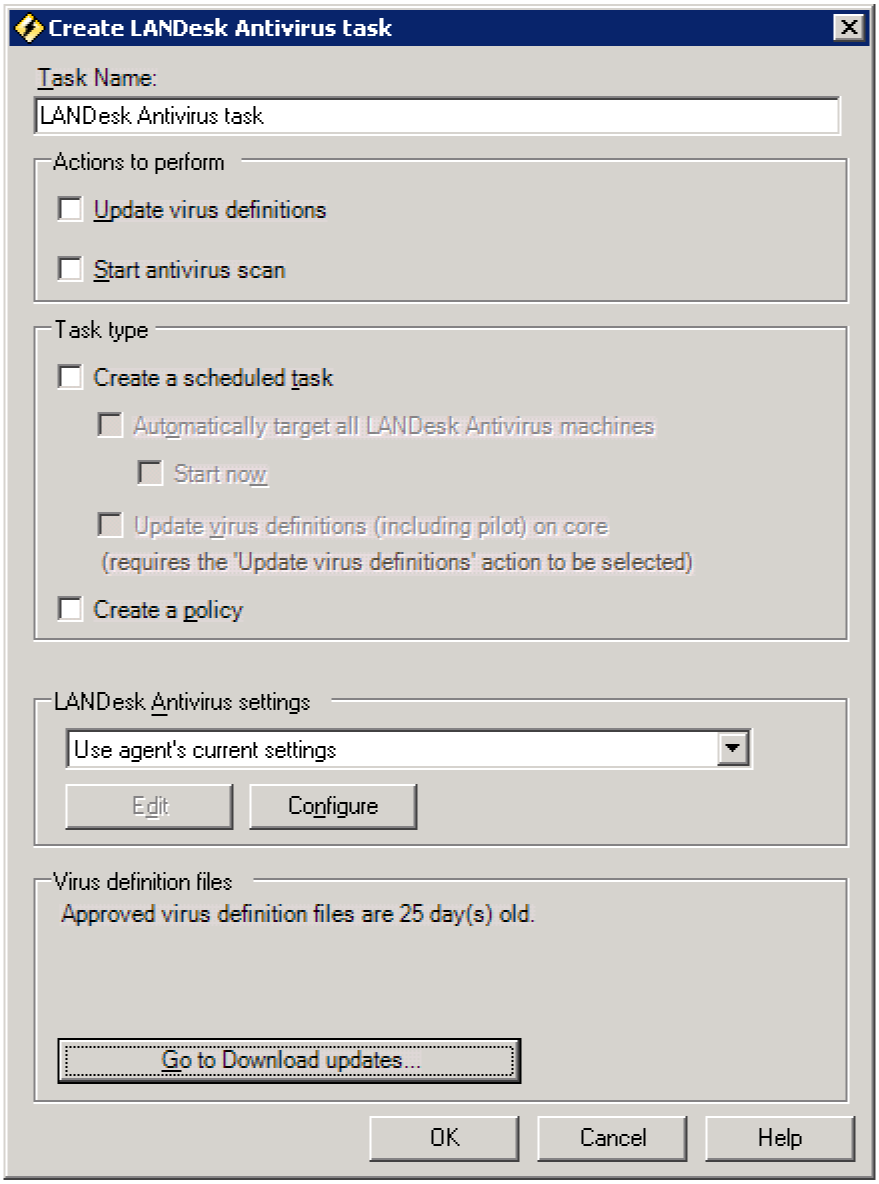
There are several different methods of running an antivirus scan on managed devices that have Antivirus installed:

- Scheduled antivirus scan
- On-demand antivirus scan
- User-initiated antivirus scan
- Real-time file protection
- Real-time email protection

Running a scheduled antivirus scan from the console

From the console, you can configure antivirus scan tasks that can be run as either an on-demand scan or as a scheduled task or policy.

Scheduled task remediation can be thought of as a push distribution because the patch is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.



Task Name:
LANDesk Antivirus task

Actions to perform

□ Update virus definitions

□ Start antivirus scan

Task type

□ Create a scheduled task

□ Automatically target all LANDesk Antivirus machines

□ Start now

□ Update virus definitions (including pilot) on core
(requires the 'Update virus definitions' action to be selected)

□ Create a policy

LANDesk Antivirus settings

Use agent's current settings

Virus definition files

Approved virus definition files are 25 day(s) old.

To create an antivirus scan task

1. Click **Tools > Security > Security Configurations**.
2. Make sure virus definition files have been updated recently.
3. Make sure the default virus definition file folder (\LDLogon\Antivirus\Bases) contains only those definitions you want to scan for.
4. Click the **Create a task** toolbar button, and then click **LANDesk Antivirus**.
5. Enter a name for the task.
6. Specify whether you want this task to update virus definitions, perform an antivirus scan, or do both.
7. Specify whether the task is a scheduled task or a policy-based scan, or both.
8. If you want to scan ALL of your managed devices with Antivirus agent installed, select a scheduled task, and then select to target all devices. You can also select to start the antivirus scan of all devices immediately.

9. If you want to ensure that the scan uses the latest known virus definition files, check the **Update virus definitions** option.
10. Select an antivirus settings from the available list (or create a custom settings for this scan by clicking the **Configure** button), to determine how the scanner operates on end user devices. If you want the antivirus scan to use the device's local antivirus settings (default settings), select that option from the drop-down list. For more information about configuring the antivirus scan with an antivirus settings, see "About the LANDesk Antivirus settings dialog" on page 602.
11. Click **OK**. (For a typical scheduled task scan, click **OK**, and then add target devices and configure the scheduling options in the Scheduled tasks tool.)

Running an on-demand antivirus scan from the console

You can also run an immediate on-demand antivirus scan on one or more target devices.

To do this, right-click the selected device (or up to 20 multi-selected devices), click **LANDesk Antivirus scan now**, select an antivirus settings, choose whether to update virus definition files before scanning, and then click **OK**.

When you click OK, the **Status of requested actions** dialog displays the following information:

- Progress
- Results
- Scan time information

Running an antivirus scan at a managed device

Additionally, if you've configured antivirus settings to display the Antivirus icon in the device system tray, end users can perform their own on-demand antivirus scans.

To do this at the managed device, right-click the **LANDesk Antivirus** taskbar icon, and then select **Scan my computer**. Or from the Antivirus dialog, click **Scan my computer**.

Enabling real-time antivirus protection (file, email)

Real-time antivirus protection provides ongoing background scans of specified files, file types, email messages, and email attachments, based on known virus definitions. You can also enable real-time notification to inform end users about infected files.

Real-time file protection, email scanning, and notification are all configured with antivirus settings.

LANDesk Antivirus system tray icon indicator
When real-time antivirus protection is enabled, the LANDesk Antivirus system tray icon (on the end user device) is yellow. When real-time protection is disabled, the icon is gray.

Real-time file protection

Configure real-time file protection with the options on the **Real-time protection** page of the **Antivirus settings** dialog. For more information, click **Help**.

When real-time protection is running, files are scanned for viruses every time the file is:

- Opened
- Closed
- Accessed
- Copied
- Saved

Real-time email scanning

Configure real-time email scanning with the **Enable email scanning option** on the **General** page of the **Antivirus settings** dialog.

Real-time email protection provides on ongoing scan of incoming and outgoing messages. Antivirus scans the message body as well as attached message's bodies and file attachments.

Antivirus real-time email protection supports:

- Microsoft Outlook

When real-time email protection is running, messages and attachments are:

- Scanned when opened or previewed
- Not scanned when selected

When an infected email is discovered on a managed device, Antivirus attempts to clean it. If it can be cleaned: a new header is placed in the message body to inform the end user. If the infected email can't be cleaned: the entire message body is deleted and replaced with a new header.

When a suspicious email message is discovered, the message body is converted to plain text and a header is added to the message.

Also, a dialog displays on the end user device that shows:

- File path
- File name
- Virus name
- Note telling the end user to contact their network administrator

Real-time (infected file) notification

End users can be notified when a file infected by a virus is detected, quarantined, deleted, skipped, or cleaned.

Configure real-time infected file notification with the option on the **Real-time protection** page of the **Antivirus settings** dialog.

A dialog displays on the end user device that shows:

- File path
- File name
- Virus name
- Note telling the end user to contact their network administrator

Configuring antivirus scan options with antivirus settings

Antivirus gives you complete control over how antivirus scans run on target devices, and which options are available to end users. For example, depending on the purpose or scheduled time of an antivirus scan, you may want to show the Antivirus client on end user devices, allow the end user to perform antivirus scans, view and restore quarantined objects, download virus definition file updates on their own, etc. You can do this by creating and applying antivirus settings to a scan task.

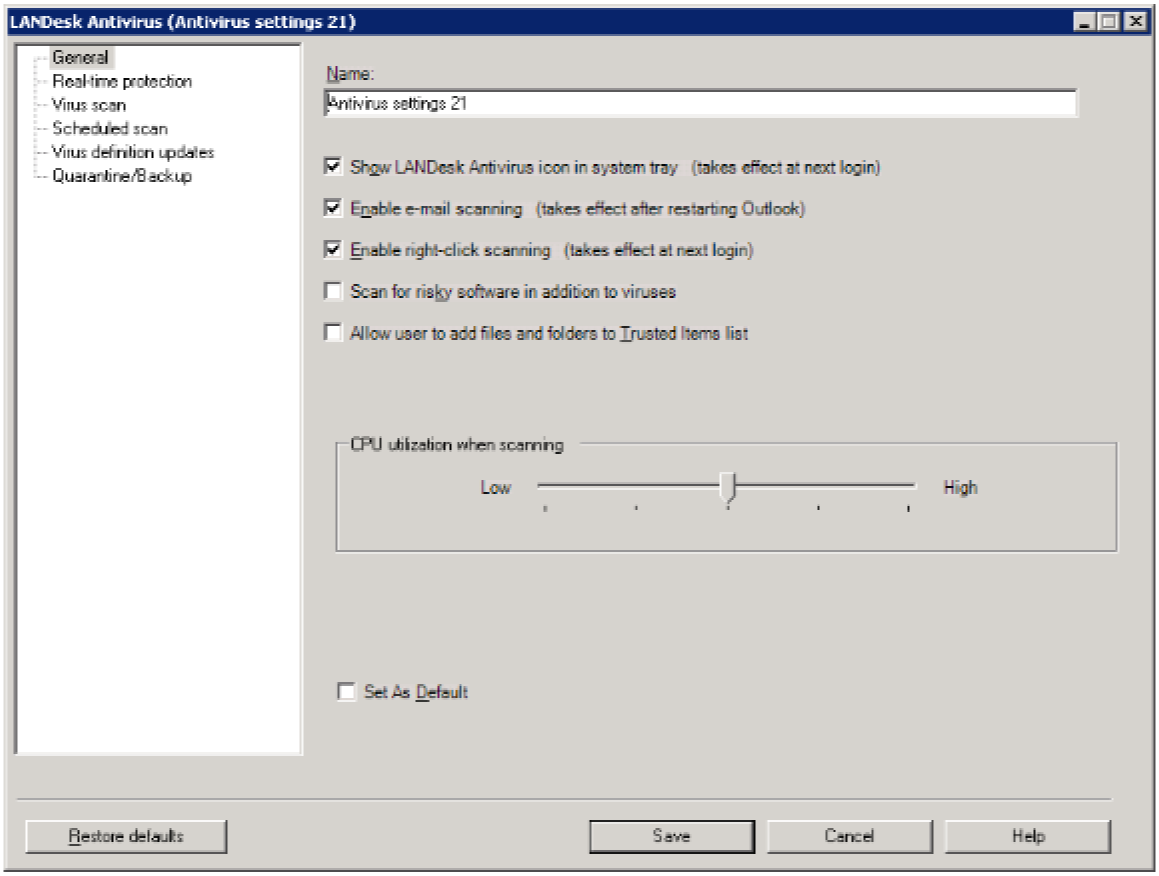
With antivirus settings, you can configure the following options:

- Whether the Antivirus icon appears in device system trays (providing end user access to antivirus scanning, quarantine and backup viewing, and file handling tasks)
- Real-time email scanning
- End user right-click scans
- CPU usage
- Owner (to restrict access)
- Scheduled antivirus scans
- Quarantine/backup folder size
- Restoring infected and suspicious objects
- Which files, folders, and file types to scan
- Scan exclusions
- Whether to use heuristic analysis for detecting suspicious files
- Whether to scan for riskware
- Real-time file protection (including which files to scan, heuristics, and exclusions)
- Downloading virus definition file updates (pilot test versions, scheduled downloads, end user download permission, and direct downloads from the security content server)

All of the antivirus settings you create are stored in the **LANDesk Antivirus** group in the **Security Configurations** tool.

Using Antivirus settings

Create and apply antivirus settings (a saved set of configured options) to antivirus scan tasks. You can create as many antivirus settings as you like. Antivirus settings can be designed for a specific purpose, time, or set of target devices.



LANDesk Antivirus (Antivirus settings 21)

Name: Antivirus settings 21

☑ Show LANDesk Antivirus icon in system tray (takes effect at next login)

☑ Enable e-mail scanning (takes effect after restarting Outlook)

☑ Enable right-click scanning (takes effect at next login)

☐ Scan for risky software in addition to viruses

☐ Allow user to add files and folders to Trusted Items list

CPU utilization when scanning: Low – High

☐ Set As Default

To create antivirus settings

1. In the **Security Configurations** tool, right-click the **LANDesk Antivirus** object, and then click **New**. (Note: You can also access this dialog by clicking **Edit** or **Configure** on any of the task dialogs that let you apply an antivirus settings.)
2. Enter a name for the antivirus settings.
3. Specify the settings on the pages as desired for the particular task. For more information about an option, click **Help**.

Once configured, you can apply antivirus settings to antivirus tasks (or to a change settings task).

Changing device default antivirus settings

A device's default antivirus settings are deployed as part of the initial agent configuration. When a specific task has a different antivirus settings associated or assigned to it, the default settings are overridden. You can also choose to use the device's default settings by selecting it when you create a task.

At some point you may want to change these default antivirus settings on certain devices. Patch and Compliance provides a way to do this without having to redeploy an entirely new and complete agent configuration. To do this, use the **Change settings** task located in the drop-down list of the **Create a task** toolbar button. The dialog that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select an existing antivirus settings as the default or use the Edit button to create a new antivirus settings as the default for target devices.

Viewing device antivirus settings in the Inventory

You can discover and/or verify device antivirus settings in their Inventory view.

To do this, right-click the selected device, click **Inventory > LANDesk Management > AV Settings**.

Configuring which files to scan (infectable files only, exclusions, heuristics, riskware)

You can specify which files (items) you want to scan which files you don't want to scan with both antivirus scans and real-time antivirus file protection.

See the following sections for information on customizing what to scan:

- "All files or infectable files only" on page 383
- "Excluding items from antivirus scans and real-time protection" on page 385
- "Using heuristic analysis to scan for suspicious objects" on page 385
- "Scanning for riskware (extended database)" on page 385

All files or infectable files only

Configure to scan all files or infectable files only on the **Virus scan** and **Real-time protection** pages of an antivirus settings.

- **Scan all file types:** Specifies that files of all types on the target device are scanned by an antivirus scan. This may take a long time so it is a good idea to scan all file types with an on-demand scan rather than real-time protection.
- **Scan infectable files only:** Specifies that infectable files only are scanned. Infectable files are those types of files known to be vulnerable to virus infections. Scanning only infectable files is more efficient than scanning all files because some viruses affect only certain file types. However, you should make a habit of regularly scanning all the files with an on-demand scan in order to ensure devices are clean.

Infectable file types

Infectable file types are identified by their format identifier in the file header rather than by their file extension, ensuring that renamed files are scanned.

Infectable files include: document files such as Word and Excel files; template files that are associated with document files; and program files such as Dynamic Link Libraries (.DLLs), communication files (.COM), Executable files (.EXEs), and other program files. See below for a list of infectable file types by the file format's standard or original file extension.

- ACM
- ACV
- ADT
- AX
- BAT
- BIN

- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML
- HTT
- INF
- INI
- JS
- JSE
- JTD
- MDB
- MSO
- OBD
- OBT
- OCX
- PIF
- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH
- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD

- WSF
- WSH

Excluding items from antivirus scans and real-time protection

You can also specify what not to scan for with both antivirus scans and real-time file protection. Configure antivirus scan exclusions by adding files, folders, and file types to the exclusion list on the **Virus scan** and **Real-time protection** pages of an antivirus settings.

Trusted Items list on managed devices
Note that you can also enable an option that allows end users to specify files and folders they don't want to be scanned by LANDesk Antivirus. This feature is called the trusted items list, and is configured on the **General** page of an antivirus settings.

Using heuristic analysis to scan for suspicious objects

You can enable heuristic analysis to check for suspicious (possibly infected) files with both antivirus scans and real-time file protection.

Enable heuristic scanning on the **Virus scan** and **Real-time protection** pages of an antivirus settings.

Heuristic analysis scanning attempts to detect files suspected of being infected by an unknown virus (not defined in the virus signature database) by looking for suspicious behavior. Suspicious behavior can include a program that is self-modifying, immediately tries to find other executables, or that is modified after terminating. A heuristic analysis emulates program execution to make protocols of observed suspicious activity, and uses those protocols to identify possible virus infections. In almost all cases, this mechanism is effective and reliable, and rarely leads to false positives.

Antivirus utilizes a heuristic analyzer to verify files that have already been scanned by an antivirus scan based on known virus definitions.

Note that heuristic scanning may negatively affect performance on managed devices.

Scanning for riskware (extended database)

Antivirus lets you enable scanning for risky software, also known as riskware, on target devices. Risky software is essentially client software whose installation presents a possible but not definite risk for the end user.

For example: adware, proxy-programs, pornware, remote admin utilities, IRC, dialers, activity monitors, password utilities, and Internet tools such as FTP, Web, Proxy and Telnet.

When you specify to scan managed devices for risky software, Antivirus loads an extended database that contains definition files used to perform the scan. The extended database scan requires more time than the standard antivirus scan.

Additional notes about scanning files

- **System restore point scanning:** Antivirus will scan the files in any system restore point folders that may exist on the managed device.

What happens on a device during an antivirus scan

This section describes how Antivirus displays on end user devices with Antivirus installed and what happens when devices are scanned for viruses by an antivirus scan or through real-time virus protection. Possible end user options are listed as well as the actions end users can take when an infected object is discovered by the scan.

Antivirus client interface and end user actions

If the **Show LANDesk Antivirus icon in the system tray** option is checked on the device's antivirus settings, the Antivirus client appears and shows the following elements:

System tray icon

- Real-time protection is enabled (system tray icon is yellow) or disabled (system tray icon is gray)

Antivirus window

- Real-time protection is enabled or disabled (If the option is enabled in antivirus settings, the end user can disable real-time protection for as long a period of time as you specify)
- Email scanning is enabled or disabled
- Latest scan (date and time)
- Scheduled scan (date and time)
- Scan engine version number
- Virus definitions (the last time pattern files were updated)
- Quarantine (shows the number of objects that have been quarantined. End users can click **View details** to access the Quarantined objects dialog. If the option is enabled, end user can also restore files. If the password requirement option is enabled, the end user must enter that password.)
- Backup (shows the number of objects that have been backed up)
- Trusted items (shows the items the end user has added to their trusted items list that won't be scanned for viruses or risky software)

End user actions

If Antivirus is installed on their computer, and their antivirus settings (default or task-specific) allow, users can perform the following tasks:

- Scan my computer (can view scan status, and pause and cancel the scan)
- Right-click to perform antivirus scan on files and folders in Windows Explorer (if the option is enabled by the antivirus setting)
- View local scheduled antivirus scans tasks
- Create local scheduled antivirus scans on their own machine (if the option is enabled by the antivirus setting).
- Update virus definition files
- Temporarily disable real-time protection (if the option is enabled by the agent configuration, and limited to a specified period of time)
- View quarantined objects
- View backup objects
- View trusted items
- Restore suspicious objects (if the option is enabled by the antivirus setting)

- Restore infected objects and risky software (if the option is enabled by the antivirus setting)
- Add and remove files and folders\subfolders to their trusted items list

Note that end users can't configure antivirus scan settings, or disable email scanning.

When an infected object is detected

This process applies to both infected files and email messages.

The infected object is:

1. Automatically backed up. (The backup file is saved in \LDClient\Antivirus\ folder, with a *.bak extension.)
2. An attempt is made to clean the infected object.
3. If the infected object can be cleaned, it is restored to its original location.
4. If the infected object can't be cleaned, it is quarantined. (The virus string is removed and the file is encrypted so it can't be run. The quarantined file is saved in \LDClient\Antivirus\ folder, with a *.qar extension.)

If the corresponding option is enabled in their antivirus settings (default or task-specific), end users can restore, delete, and rescan quarantined objects.

Automatic scanning of quarantined files

When an on-demand antivirus scan is executed, or when the virus definition files are updated, the antivirus scanner automatically scans objects in the quarantine folder to see if any infected files can be cleaned with the current virus definition files.

If a quarantined file can be cleaned, it is automatically restored and the user is notified.

End users can open a backup file to see a header that provides information on the original file location, and the reason for the file being backed up.

Note that only the original user is allowed to delete or modify backup files. The user that is logged in when the infected file is discovered.

Using antivirus alerts

You can configure antivirus alerting so that you can be notified when specific virus outbreaks are detected on managed devices in your system. Antivirus uses the standard LANDesk alerting tool.

You define virus outbreak parameters based on the number of managed devices infected by a virus in a specified period of time.

To configure antivirus alerting

Antivirus alert settings are found on the **Antivirus** page of the **Alert settings** dialog.

You must first configure the antivirus alerts in the Alert Settings tool in the console. Antivirus alerts include:

- An alertable antivirus action failed
- An alertable antivirus action succeeded
- Virus outbreak alert (per virus)

The following antivirus events can generate antivirus alerts:

- Virus removal failed
- Virus removal succeeded
- Quarantine failed
- Quarantine succeeded
- Deletion failed
- Deletion succeeded

Select which alerts you want generated. The time interval option lets you prevent too many alerts. More than one alert (for any antivirus trigger) during the specified time interval is ignored.

You can view the complete antivirus alert history for a device in its Security Information dialog. Right-click a device, select Security Information, select the Antivirus type in the Type drop-down list, and then select the Antivirus History object.

Using antivirus reports

Antivirus information is represented by several reports in the Reports tool. These reports provide useful information about antivirus scan activity and status for scanned devices on your network.

In order to access the Reports tool, and generate and view reports, a user must have the LANDesk Administrator right (implying full rights) and the specific Reporting roles.

For more information about using the Reports tool, see "Reports" on page 113.

Viewing antivirus information in the Executive Dashboard

You can also view antivirus scan information in the Web console Executive Dashboard. This data is useful in identifying virus outbreaks and to show antivirus protection over time.

LANDesk Antivirus-specific widgets show:

- Top five viruses detected (in the past 10 days or weeks)
- Managed devices infected with viruses (in the past 10 days or weeks)
- Percentage gauge of managed devices with real-time protection enabled
- Percentage gauge of managed devices with up-to-date virus definitions

Endpoint Security

The new Endpoint Security tool is actually a set of complementary features and settings that lets you strongly secure and protect the managed devices on your network. You can restrict network connections for managed devices, restrict access to those managed devices by other types of devices, and use the HIPS and Firewall tools to protect prevent unauthorized application operations.

Although Endpoint Security is a consolidated single agent that is deployed to target devices, it is fully configurable and provides services for several security components.

The Endpoint Security components are:

- **Location Awareness:** Provides network connection control (see below).
- **Host Intrusion Prevention (HIPS):** Prevents unauthorized intrusions. For information, see "Host Intrusion Prevention System (HIPS)" on page 395.
- **LANDesk Firewall:** Prevents unauthorized application operations and connections. For information, see "LANDesk Firewall" on page 410.
- **Device Control:** Restricts access for storage volumes, devices, interfaces, etc. For information, see "Device Control" on page 415.

With Endpoint Security you can define trusted locations (network connections) for managed devices, create settings for each of the Endpoint Security components listed above, and deploy those settings based on whether the device is inside the trusted network location or outside the trusted location.

As stated above, Endpoint Security is a single agent that enforces protection rules on managed devices and controls the functionality of each of the distinct security components. Endpoint Security has the flexibility to allow you to enable and configure the security components independently or in a coordinated deployment. For example, you can deploy HIPS protection only, or HIPS and Device Control (via their respective settings), or any other combination of security components.

This section describes how to enable Endpoint Security on your managed devices, and directs you to information about each of the encompassed Endpoint Security components.

Enabling and deploying Endpoint Security

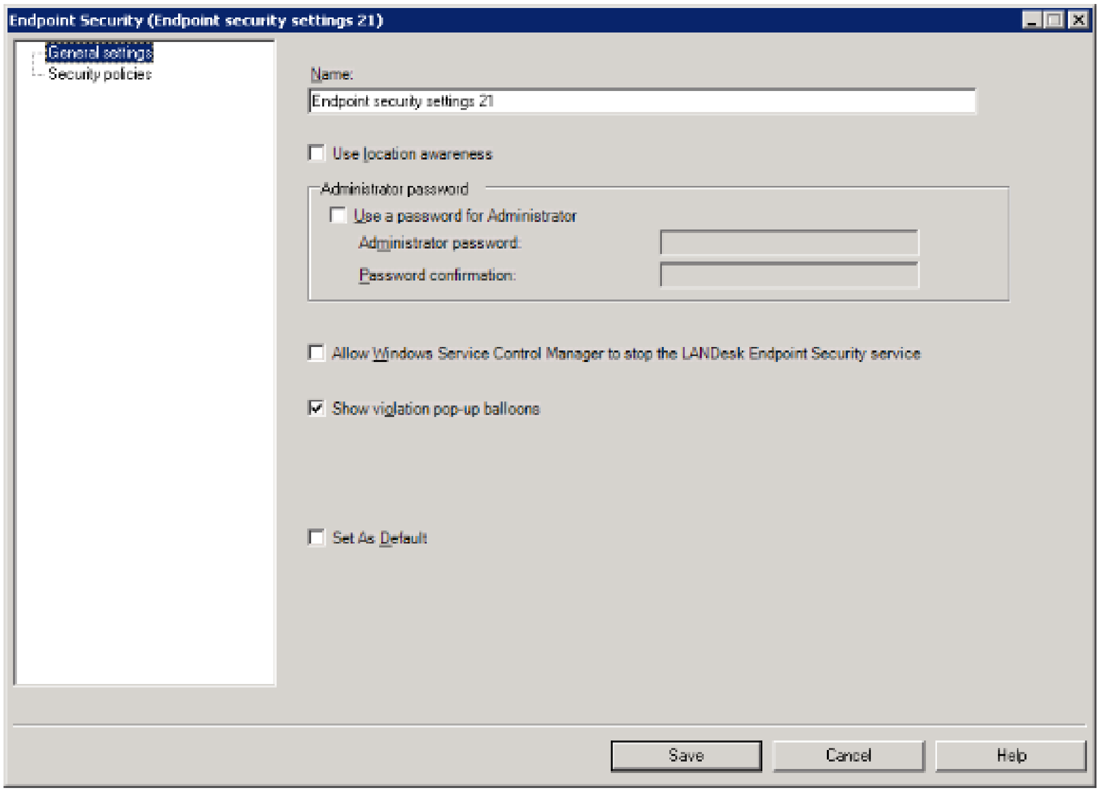
Endpoint Security is enabled on managed devices with an Endpoint Security settings.

Endpoint Security can be enabled on managed devices via the initial agent configuration. You can also use a change settings task to install or update Endpoint Security settings to target devices.

Creating Endpoint Security settings

To create Endpoint Security settings

1. In the **Security Configurations** tool window, right-click **Endpoint Security**, and then click **New**.



Endpoint Security (Endpoint security settings 21)

- General settings
- Security policies

Name: Endpoint security settings 21

□ Use location awareness

Administrator password

□ Use a password for Administrator

Administrator password:

Password confirmation:

□ Allow Windows Service Control Manager to stop the LANDesk Endpoint Security service

☑ Show violation pop-up balloons

□ Set As Default

2. At the **General settings** page, enter a name for the settings, and then specify the general requirements and actions. For information about an option, click **Help**.
3. If you want to manage network connections, select the **Use location awareness** option. When this option is selected, the **Trusted location** page displays. Also, by selecting this option, two separate groups are made available on the **Security policies** page, one for when the device is inside the trusted location and one for when the device is outside the trusted location. If location awareness is not enabled, only one policy group is needed.
4. At the **Security policies** page, select which Endpoint Security components you want to deploy to target devices with this Endpoint Security settings.
5. At the **Trusted location** page, define the allowed network connections (by IP address, IP range, or subnet).
6. Click **Save**.

Once configured, you can deploy settings to target devices with an installation or update task, or a change settings task.

Endpoint Security settings help

Use this dialog to create and edit Endpoint Security settings.

This dialog contains the following pages.

About the Endpoint Security: General settings page

Use this page to configure location awareness (trusted network) and other access settings.

- **Name:** Identifies the settings with a unique name.
- **Use location awareness:** Lets you manage network connections. You can restrict the network IP addresses that devices are allowed to connect with. You configure network restrictions by specifying which network addresses are allowed. The device can only receive IP addresses that are within the range of addresses that are explicitly allowed.
- **Administrator password:** Specifies the password required on devices configured with this Endpoint Security settings in order to perform certain actions on the protected device. Actions requiring a password include: accessing the HIPS client interface, installing unsigned software, authorizing HIPS violations, unloading HIPS, erasing the local report, and switching the HIPS operating mode.
- **Allow Windows Service Control Manager to stop the Endpoint Security service:** Lets the end user stop the Endpoint Security service on the client.
- **Show violation pop-up messages:** Displays a message on the end user device if a blocked operation occurs.
- **Set as default:** Assigns this settings as the default settings for tasks that use Endpoint Security.
- **Save:** Saves your changes and closes the dialog.

About the Endpoint Security: Policies page

Use this page to configure security policies for devices inside the trusted network and polices for devices outside the trusted network.

- **When inside the trusted location:** Specifies the component settings to be applied to devices when they are connected to a trusted location.
- **When outside the trusted location:** Specifies the component settings to be applied to devices when they are not connection to a trusted location.

About the Endpoint Security: Trusted Locations page

Use this page to define trusted locations. A trusted location is made up of a collection of network addresses, by IP address, IP range, or subnet.

- **Trusted location:** Lists the trusted locations for the settings.
- **Import:** Click to import the subnet range for the core server.
- **Add:** Lets you add a trusted location to the list.
- **Edit:** Lets you modify the selected existing trusted location.
- **Delete:** Removes the selected trusted location.
- **Verify core server existence on the network:** Check this option to ensure that the core server is running on a network before a device is allowed to connect to that network. A range of IP addresses can sometimes be used by more than one network, and this option provides added security in restricting network access. If no core server is found on the network being accessed, the connection will be disabled. (Note: Leave this option clear if you're confident that the network addresses in the access list are trusted, or if you prefer to reduce traffic on the network by not sending pings to the core server.)

- **Add:** Lets you add a core server to the list.
- **Remove:** Removes the selected core server.

What happens on a device configured with Endpoint Security components

This section describes how the Endpoint Security client displays on managed devices, what happens on end user devices when they are being protected by Endpoint Security, and the actions end users can take when a security violation is discovered.

Client interface and user actions

Once Endpoint Security has been deployed to managed devices, the client can be accessed through either the **Start** menu or the system tray icon.

Administrator password protection
If the administrator has enabled the password protection option in the Endpoint Security settings, the correct password must be entered in order to access and use certain client features.

System tray icon

The system tray icon shows whether the HIPS component of Endpoint Security is running in learn mode or automatic blocking mode.

End users can right-click the icon to access its shortcut menu and select the following options:

- **Open:** Opens the client.
- **Options:** Displays the options that have been configured by the administrator at the console (ready-only).
- **Automatic mode:** Enables the HIPS component to run in automatic mode where all predefined security violations are blocked.
- **Learn mode:** Enables the HIPS component to run in learn mode where all security violations are allowed, but are monitored and recorded in an action history file.
- **Install software:** Opens a file explorer window where the end user can select an installation or setup program to run.
- **Unload:** Lets the end user uninstall the client from their machine.

End user actions

The client displays in a window that includes the following elements:

- View the activity log.
- View the options that have been configured by the administrator at the console (read-only).
- On the **Status** page: View HIPS component information, current operating mode, and activity occurring on the client. Change the operating mode (automatic or learn).
- On the **Programs** page: View running applications and their authorizations. Select programs and view all of their authorizations or kill the process. Modify display options.
- On the **Startup** page: View and edit the contents of the system startup. Also, services running on the client and Internet Explorer extensions.
- On the **Protection** page: View program access rights and folder protections. Create, edit, and delete file protection rules, and change rule priority in the ordered list.
- On the **Certifications** page: View programs with special file certifications. Add and delete file certifications.

Host Intrusion Prevention System (HIPS)

Host Intrusion Prevention System, or HIPS, is an important tool in the LANDesk Security Suite and one of the components of Endpoint Security.

HIPS gives you the ability to protect managed devices from known and unknown internal malware attacks before they contaminate your network. HIPS adds an extra layer of protection to your managed devices by monitoring processes and files and using rules to determine allowed actions and behaviors. In a sense, HIPS protects systems from themselves.

Read this section to learn about:

Host Intrusion Prevention (HIPS) overview

HIPS stands for Host-based Intrusion Prevention System. HIPS provides another layer of protection on top of antivirus, anti-spyware, patch management and firewall configuration to prevent malicious activity on your machine. HIPS constantly and continuously monitors specified processes, files, applications, and registry keys to prevent unauthorized behavior. You control which applications run on devices and how they are allowed to execute.

Because it is a rule-based system, instead of a definition-based system, HIPS is more effective at protecting systems against zero-day attacks (malicious exploitation of vulnerable code before patches are available).

Unlike vulnerability detection and remediation, spyware detection and removal, or antivirus scanning, HIPS protection does not require ongoing file updates (patch files, definition/pattern files, or signature database files).

HIPS protects servers and workstations by placing software agents between applications and the operating system’s kernel. Using predetermined rules based upon the typical behavior of malware attacks, these systems evaluate activities such as network connection requests, attempts to read or write to memory, or attempts to access specific applications. Behavior known to be good is allowed, behavior known to be bad is blocked, and suspicious behavior is flagged for further evaluation.

The HIPS tool and features are accessed from the main console (**Tools > Security > Security Configurations**). The HIPS tool lets you create HIPS agent installation, update, and removal tasks; configure HIPS settings that can be deployed to target devices you want to protect; and customize HIPS display/interaction settings that determine how HIPS appears and operates on managed devices, and which interactive options are available to end users. You can also view HIPS activity and status information for protected devices.

Component of Endpoint Security

HIPS is one of the components of the comprehensive Endpoint Security solution, along with the LANDesk Firewall and Device Control tools.

Proactive security

HIPS proactively protects your managed devices from by:

- Providing kernel-level protection against applications that would attempt to modify binaries (or any files you specify) on your machine or application memory of running processes. It will also block changes to certain areas of the registry and can detect rootkit processes.
- Using memory protection against buffer-overflow and heap exploits.
- Executing protection schemes to keep an attacker from building and executing code in a data segment.
- Watching for unauthorized or unusual file access.
- Offering real-time protection for your computer without relying on signature databases.

System-level security

HIPS offers the following system-level security:

- Kernel-level, rule-based file-system protection
- Registry protection
- Startup control
- Detection of stealth rootkits
- Network filtering
- Process and file/application certification
- File protection rules that restrict actions that executable programs can perform on specified files

HIPS console features

HIPS provides administrators with the ability to define and manage separate profiles for different user groups with HIPS settings. HIPS settings accommodates the needs of any and all user groups by allowing administrators to create multiple, highly flexible configurations for different user profiles.

Each HIPS settings can include custom password protection, WinTrust handling, protection mode, custom whitelists, network and application access control policies, file certifications, and file protection rules.

HIPS client features

The HIPS client gives administrators a powerful new tool for controlling what applications run on enterprise desktops and servers, and how those applications are allowed to execute.

HIPS client software uses proven heuristic and behavior-recognition techniques to recognize typical patterns and actions of malicious code. For example, a file that attempts to write to the system registry could be blocked and flagged as potentially malicious. The HIPS client uses a variety of proprietary techniques to reliably detect malware even before a signature has been identified.

Supported device platforms

HIPS supports many of the same desktop and server platforms supported by the standard LANDesk-managed device platforms, including the following operating systems:

- Windows 2000 SP2
- Windows 2003
- Windows 2008
- Windows XP SP1
- Windows Vista (32-bit, and 64-bit)

HIPS is not supported on core servers or rollup cores
You should not install/deploy HIPS to a core server or a rollup core. However, you can deploy HIPS on an additional console.

Supported antivirus products

HIPS is compatible with the LANDesk Security Suite Antivirus solution as well as several third-party antivirus products. Compatibility means that HIPS will not interfere with antivirus processes such as scans, real-time protection, etc.

Make sure the managed devices you want to configure with HIPS have one of the following antivirus products installed:

- LANDesk Antivirus
- Symantec* Antivirus (versions 7, 8, 9, 10.1, 10.2)
- McAfee VirusScan (versions 7.0, 8.0, 8.5i)
- Trend Micro* PC-cillin (versions 2005, 2006)
- Trend Micro OfficeScan (versions 6.5, 7.3)
- Trend Micro ServerProtect (version 5.58)
- CA eTrust InoculateIT (version 6.0)
- CA eTrust* Antivirus (versions 7.0, 7.1, 8.0, 8.1)
- ESET NOD32* (version 2.7)

Do NOT deploy HIPS to devices with any other antivirus product installed.

HIPS licensing

In order to access the HIPS tool you must first activate your core server with a HIPS license.

For information about HIPS licensing, contact your reseller, or visit the LANDesk Web site.

Role-based administration with HIPS

HIPS, like Patch and Compliance, uses role-based administration to allow users access to features. Role-based administration is the access and security framework that lets LANDesk Administrators restrict user access to tools and devices. Each user is assigned specific roles and scope that determine which features they can use and which devices they can manage.

Administrators assign these roles to other users with the Users tool in the console. HIPS is included in the Security Configurations right, which appears under the Security rights group in the Roles dialog. In order to see and use HIPS features, a user must be assigned the necessary Security Configurations access rights.

IMPORTANT: LANDesk Script Writers group permission required
In order to create scheduled tasks and policies in the Patch and Compliance tool and the Security Configurations tool (for security and compliance scan tasks, repair tasks, and change settings tasks), a user must have the LANDesk Script Writers group permission. In other words, they must belong to a group that has the LANDesk Script Writers permission assigned. For more information about role-based administration, see "Role-based administration" on page 44.

With the Security Configurations right, you can provide users the ability to:

- See and access the Host Intrusion Prevention System (HIPS) features in the console's Tools menu and Toolbox
- Configure managed devices for HIPS protection
- Manage HIPS settings (password protection, signed code handling, action, protection mode, file certifications, file protection rules, etc.)
- Deploy HIPS install or update tasks, and change settings tasks
- View HIPS activity for protected devices
- Define HIPS data threshold settings for recording and displaying HIPS activity

HIPS task workflow

The steps below provide a quick summary outline of the typical processes or tasks involved in implementing HIPS protection on your network. All of these procedures are described in detail in subsequent sections.

Basic steps in implementing and using HIPS:

1. Configuring managed devices for HIPS protection (i.e., deploying the agent to target devices).
2. Configuring HIPS options with HIPS settings, such as: signed code handling, protection mode, whitelists (applications allowed to execute on devices), file certifications, file protection rules, and end user interactive/options.
3. Discovering file and application behavior on devices with the HIPS learn mode.
4. Enforcing HIPS protection on managed devices with the HIPS automatic block mode.
5. Viewing HIPS activity for protected devices.

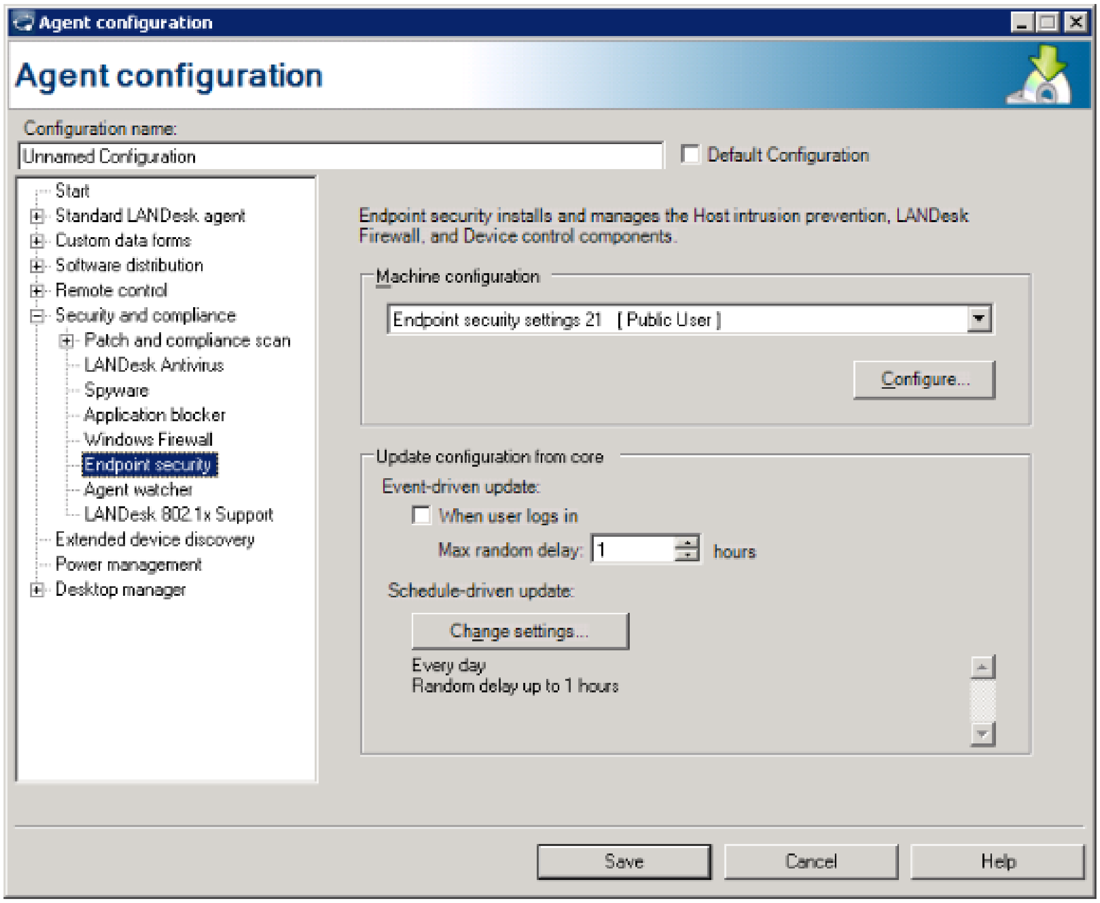
Configuring devices for HIPS protection

Before managed devices can be protected from zero-day attacks, they must have the Endpoint Security agent installed. The Endpoint Security agent is a single agent service that manages all of the Endpoint Security components, including HIPS.

You can configure devices for HIPS either during initial device agent configuration or with a separate installation or update task.

To install or update HIPS on managed devices via an agent configuration

1. In the console, click **Tools > Configuration > Agent Configuration**.
2. Click the **New Windows** toolbar button.
3. After specifying your desired settings for the agent configuration, you must first click the **Start** page, and select the **Endpoint Security** option under **Security**. (This deploys the agent to target devices, but you still need to select a HIPS settings.)
4. Now you can access the options on the **Endpoint Security** page.



Configuration name: Unnamed Configuration

☐ Default Configuration

Endpoint security installs and manages the Host intrusion prevention, LANDesk Firewall, and Device control components.

Machine configuration

Endpoint security settings 21 [Public User]

Update configuration from core

Event-driven update:

☐ When user logs in

Max random delay: 1 hours

Schedule-driven update:

Every day
Random delay up to 1 hours

5. Select one of the settings from the available list to apply it to the agent configuration you're creating. You can create a new settings or edit an existing settings by clicking **Configure**. The Endpoint Security settings contains a HIPS settings (among other security component settings). The HIPS settings determine whether the HIPS client is password protected, WinTrust signed code handling, action on programs added to

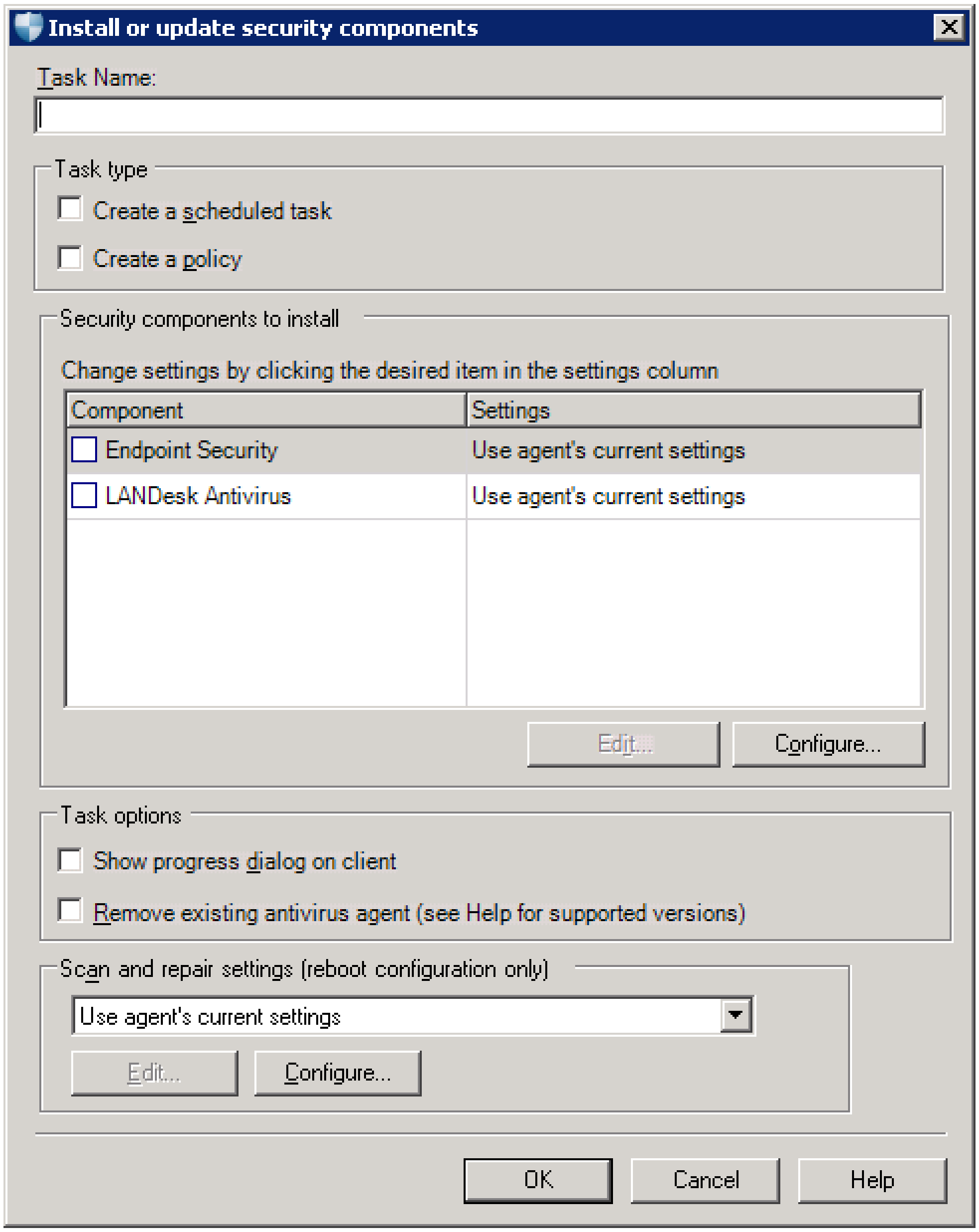
system startup, buffer overflow protection, operating mode, whitelists, file certifications, and file protection rules.

6. Finish specifying settings for the agent configuration and then click **Save**.

If you want to install or update HIPS at a later time, you can do so with as a separate task from the **Security Configurations** tool in the console.

To install or update HIPS as a separate task

1. In the console, click **Tools > Security > Security Configurations**.
2. Click the **Create a task** toolbar button, and then click **Install/Update security components**.



Install or update security components

Task Name:

Task type

□ Create a scheduled task

□ Create a policy

Security components to install

Change settings by clicking the desired item in the settings column

Component	Settings
□ Endpoint Security	Use agent's current settings
□ LANDesk Antivirus	Use agent's current settings

Task options

□ Show progress dialog on client

□ Remove existing antivirus agent (see Help for supported versions)

Scan and repair settings (reboot configuration only)

Use agent's current settings

3. Enter a name for the task.

4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. Select an Endpoint Security settings from the available list to apply it to the agent configuration you're creating. You can create a new settings or edit an existing settings by clicking **Configure**. The Endpoint Security settings contains a HIPS settings (among other security component settings).
6. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show progress dialog on client** option.
7. Select a Scan and repair settings from the list to apply its reboot configuration (only) to the agent configuration you're creating. You can create a new settings or edit and existing settings by clicking **Configure**. Keep in mind that ONLY the reboot options specified on the Scan and repair settings you select are used by this agent configuration's Endpoint Security agent deployment to target devices. You can use an existing Scan and repair settings that already includes the reboot configuration you want, or you can create a brand new Scan and repair settings specifically for your agent deployment.
8. Click **OK**.

Removing HIPS from devices

If you want to remove HIPS from managed devices, you can also do that as a separate task from the console.

To remove HIPS

1. In the console, click **Tools > Security > Security Configurations**.
2. Click the **Create a task** toolbar button, and then click **Remove security components**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. Select the Endpoint Security component to remove this agent that includes HIPS.
6. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show progress dialog on client** option.
7. Select a scan and repair settings from the available list to apply its reboot configuration to the task you're creating. You can create a new settings or edit an existing settings by clicking **Configure**. The task will use the selected scan and repair settings' reboot options ONLY, which determine reboot requirements and actions on target devices during agent removal.
8. Click **OK**.

Customizing HIPS protection with HIPS settings

HIPS settings give you complete control over how HIPS operates on target devices, and which options are available to end users.

This section describes how to create and manage HIPS settings:

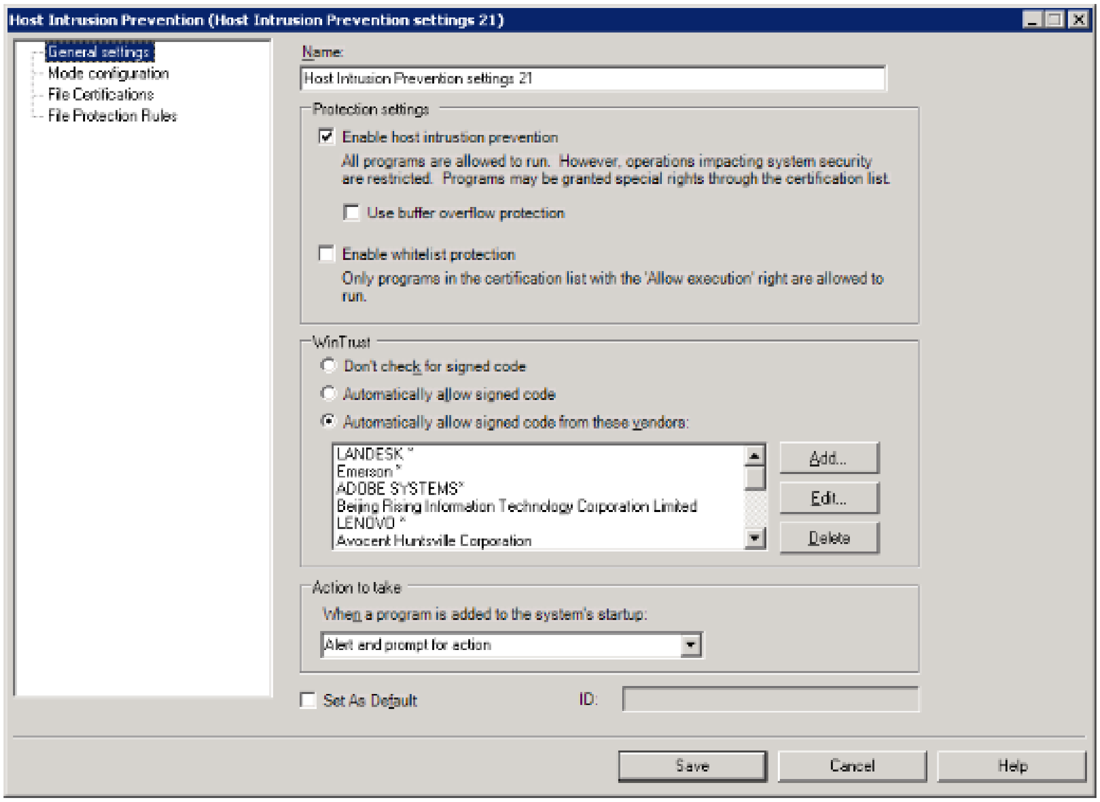
- "Creating HIPS settings" on page 402
- "Changing default HIPS settings" on page 403
- "Viewing device HIPS settings in the Inventory" on page 403
- "HIPS settings help" on page 404

Creating HIPS settings

You can create and apply HIPS settings to a HIPS installation or update task or to a change settings tasks. You can create as many HIPS settings as you like. HIPS settings can be designed for a specific purpose, time, or set of target devices.

To create HIPS settings

1. In the **Security Configurations** tool window, right-click **Host Intrusion Prevention**, and click **New**.



Host Intrusion Prevention (Host Intrusion Prevention settings 21)

Name: Host Intrusion Prevention settings 21

Protection settings

☑ Enable host intrusion prevention

All programs are allowed to run. However, operations impacting system security are restricted. Programs may be granted special rights through the certification list.

☐ Use buffer overflow protection

☐ Enable whitelist protection

Only programs in the certification list with the 'Allow execution' right are allowed to run.

WinTrust

○ Don't check for signed code

○ Automatically allow signed code

● Automatically allow signed code from these vendors:

LANDESK *
Emerson *
ADOBE SYSTEMS*
Beijing Rising Information Technology Corporation Limited
LENOVO *
Avocent Huntsville Corporation

Action to take

When a program is added to the system's startup: Alert and prompt for action

☐ Set As Default

ID:

2. At the General settings page, enter a name for the HIPS settings, and then specify the general requirements and actions. For information about an option, see "HIPS settings help" on page 404.

3. At the Mode configuration page, select whether you want to enforce HIPS automatic blocking protection mode, or learn mode. You can also select to create a whitelist (applications allowed to execute on devices) based on the current certified files, and if you want the whitelist generation to run for a specified period of time initially and then re-enforce automatic blocking mode or continue using learn mode. Note that if you select learn mode as the general protection mode and want to generate a whitelist, the enforce automatic mode option is disabled.
4. At the File certifications page, add, modify, or delete file certifications.
5. At the File protection rules page, add, modify, prioritize, or delete file protection rules. HIPS includes a predefined (default) set of protection rules.
6. At any of the settings pages, click **Save** at any time to save your configured options for the HIPS settings, or click **Cancel** to exit the dialog without saving the settings.

Once configured, you can deploy HIPS settings to target devices with an installation or update task, or a change settings task.

Changing default HIPS settings

The device default HIPS settings are deployed as part of the initial agent configuration. At some point you may want to change these default HIPS settings on certain devices. HIPS provides a way to do this without having to redeploy an entirely new and complete agent configuration.

To do this, use the **Change settings** task located in the drop-down list of the **Create a task** toolbar button. The dialog that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select an existing HIPS settings as the default or use the Edit button to create a new HIPS settings as the default for target devices.

Viewing device HIPS settings in the Inventory

You can discover and/or verify HIPS settings in a device's Inventory view.

To do this, right-click the selected device, click **Inventory > LANDesk Management > Host Intrusion Prevention**.

HIPS settings help

Use this dialog to create and edit a HIPS settings. When creating HIPS settings, you first define the general requirements and actions, and then add specific file certifications. You can create as many HIPS settings as you like and edit them at any time.

If you want to modify the device default HIPS settings without reinstalling the HIPS agent or redeploying a full agent configuration, make your desired change to any of the options on the HIPS settings dialog, assign the new settings to a change settings task, and then deploy the change settings task to target devices.

This dialog contains the following pages:

"About the HIPS: General settings page" on page 404

"About the HIPS: Mode configuration page" on page 405

"About the HIPS: File certifications page" on page 406

"About the HIPS: File protection rules page" on page 407

About the HIPS: General settings page

Use this page to configure the general protection settings and actions for HIPS.

This page contains the following options:

- **Name:** Identifies the HIPS settings with a unique name. This name appears in the HIPS settings drop-down list on an install or update security components task dialog.
- **Protection settings:** There are two types of protection: HIPS and whitelist. You can select one or both. Each protection type shares the same four operating modes (see the Mode configuration page). If you select both HIPS and whitelist protection on this page, then the mode you select on the Mode configuration page applies to both types of protection. (Note: There is one exception. If you specify the Learn mode, there is an option to allow ONLY whitelist learning even if HIPS protection is selected on the General settings page.)
    - **Enable HIPS:** Allows all programs to run (except when the program operation threatens system security) as defined by predefined protection rules. You grant special rights with custom file certifications for program executables. HIPS protection observes application behavior (is the application allowed to modify another executable, modify the registry, etc.) and enforces security rules.
        - **Use Buffer Overflow Protection:** Protects devices from system memory exploits that take advantage of a program or process that is waiting on user input.

          Note: Buffer Overflow Protection (BOP) can be enabled on a 32-bit Windows device regardless of whether the processor has NX/XD (No eXecute / eXecute Disable) support. If the processor doesn't have NX/XD support, it is emulated. However, if the processor has NX/XD support but it's turned off in either the BIOS or boot configuration, BOP can't be enabled. Note that the Endpoint Security client displays whether BOP is enabled or disabled on the end user device. BOP is not supported on 64-bit Windows devices because the Kernel Patch Protection (KPP) feature prevents patching the kernel.

          IMPORTANT: It is strongly recommend that you first test Buffer Overflow Protection (BOP) on your specific hardware configurations before doing a wide-scale deployment to the managed devices on your network. Some configurations of older processors (prior to Pentium 4 with HT or

HyperThreading) running certain Windows OS versions may not fully support Buffer Overflow Protection.

    - **Enable whitelist protection:** Allows to run only those applications whose file certification has the allow execution option enabled.
- **WinTrust:** Determines how rights are provided to digitally signed software. An executable file that is digitally signed by its publisher is considered trusted, and will show this digital signature in its file properties dialog. HIPS allows rights to digitally signed software based on the option you select (Don't check for signed code; Automatically allow signed code; or Automatically allow signed code from these vendors).
- **Action to take:** Determines the action taken when a program is added to the device's Startup folder. This option provides a second line of defense for authorizing processes in the system startup folder. HIPS monitors the contents of startup and if it finds a new process, it performs the action you select (Alert and prompt for action; Simply log in report without alert; or Remove from startup without alerting).
- **Set as default:** Assigns this settings as the default settings for tasks that use HIPS settings.
- **ID:** Identifies this particular settings. This information is stored in the database and can be used to keep track of each settings.
- **Save:** Saves your changes and closes the dialog.
- **Cancel:** Closes the dialog without saving your changes.

About the HIPS: Mode configuration page

Use this page to configure the operating mode of HIPS protection.

This page contains the following options:

- **Protection mode:** Specifies protection behavior when security violations occur on managed devices. The protection mode applies to the protection type(s) selected on the General settings page.
    - **Automatic:** All security violations (software and system modifications) are automatically blocked. In other words, all of the file certification rules you've created for specific files are enforced.
        - **Auto-learn period:** Specifies a period of time during which applications are allowed to run on the end user device while security rules are enforced. During this period, application behavior is observed (or learned) and that information is sent back to the core database.

          Note: These two time period options are executed successive. In other words , if both are selected, the auto-learn period runs first and when it expires, the auto-log period runs.
        - **Auto-log period:** Specifies a period of time during which applications are allowed to run while security rules are not enforced. Application behavior, including violations, are recorded in an action history file.
    - **Learn:** All security violations are allowed, but application behavior is observed (or learned) and that information is sent back to the core database. Use this mode of operation to discover application behavior on a specific device or set of devices, and then use that information to customize your HIPS policies before deploying them and enforcing HIPS protection throughout the network.
        - **Whitelist only learning:** Only applications with the whitelist designation (applications whose file certification has the allow execution option enabled) are learned.

  - **Log only:** Security violations are logged, but not blocked.
  - **Block:** Security violations are blocked, but not logged.
- **Security model devices:** Specifies the HIPS protection mode for a subset of devices that are configured with the same HIPS settings. You can use this feature to observe or learn software and system modifications and which applications are run on a limited group of devices. For example, you could use the same HIPS settings with the protection mode set to Automatic blocking mode, but identify a few target devices that you want to learn from by adding those machines to the security model devices list with their protection mode set to Learn.

About the HIPS: File certifications page

Use this page to view and manage file certifications. File certifications are a set of rights (privileges or authorizations) that allow and deny certain actions that can be performed BY an application on managed devices.

This page contains the following options:

- **Certified files:** Lists the files that have certification rights configured for HIPS.
- **Add:** Opens a file explorer dialog where you can browse and select a file you want to configure with file certifications.
- **Configure:** Lets you edit the selected file's certifications.
- **Delete:** Deletes the selected file and its certifications.

About the HIPS: Configure file certification dialog

Use this dialog to configure certifications for a specific application file.

This dialog contains the following options:

- **File name:** Identifies the application file that is being assigned certifications.
- **Full path:** Specifies the location of the file.
- **File size:** Specifies the size (in KB) of the file.
- **File date:** Indicates the creation date and time of the file.
- **Version:** Indicates the version number of the file, if available.
- **Certified:** Indicates the date and time the file's certifications were created or last modified.
- **MD5 hash:** Shows the file's MD5 hash. A hash file is used to ensure the integrity of the file.
- **Description:** Provides a text box for you to enter a description of the file.
- **Bypass all protection:** Allows the application file complete privileges. The file is completely unfiltered and unmonitored.
- **Bypass buffer overflow protection:** Allows you to bypass buffer overflow protection. You will want to use this option for files (processes) that are certified and that you trust.
- **System security**
  - **Modify executable files:** Allows the application the right to modify other executable files.
  - **Modify protected files:** Allows the application the right to modify protected files. You can generate a list of protected files, such as the LANDesk Management Suite device agents.
  - **Modify protected registry keys:** Allows the application the right to modify protected registry keys. Protected keys prevent malware infections.
- **Network security**

    - **Send emails:** Allows the application to send email messages. (**Note:** HIPS recognizes standard email client applications and automatically certifies them so that they can send emails.)
- **Files on disk**
    - **Add to system startup:** Allows the application the right to add files to the system startup.
    - **Allow execution:** Allows the application (process) to run on the device. Certified files are automatically have allow execution enabled. Also, if a file's certification provides partial rights, then the allow execution option is automatically enabled.
- **Advanced security rules**
    - **Protect application in memory:** Enforces protection for the application as it is running in memory. The application is protected from termination or modification.
    - **Inherit to child processes:** Assigns the same file certifications (rights) to any subordinate processes executed by this application. For example, you can use with a setup or installation executable to pass the same rights to subsequent processes launched by the setup program.
    - **Authorized installer:** Indicates that the application is allowed to perform software installation or deployment. This is the case for the LANDesk Management Suite software distribution tool, and can be applied to other software distribution applications as well.
- **Lock file certification (authorizations will not be updated via learn mode):**
- **OK:** Saves the file certifications and adds it to the list of certified files in the main HIPS settings dialog.
- **Cancel:** Closes the dialog without saving the file certifications.

About the HIPS: File protection rules page

Use this page to view, manage, and prioritize file protection rules. File protection rules are a set of restrictions that prevent specified executable programs from performing certain actions ON specified files. With file protection rules, you can allow or deny access, modification, creation, and execution by any program on any file.

This dialog contains the following options:

- **Protection rules:** Lists all of the predefined (default) file protection rules provided by LANDesk, as well as all of the file protection rules that you've created.
    - **Rule name:** Identifies the file protection rule.
    - **Restrictions:** Displays the specific actions by programs on files that are restricted by the file protection rule.
    - **Apply rule to:** Displays the executable programs that are protected by the protection rule.
- **Move Up \ Down:** Determines the priority of the file protection rule. A file protection rule higher in the list takes precedence over a rule that is lower in the list. For example, you could create a rule that restricts a program from accessing and modifying a certain file or file type, but then create another rule that allows an exception to that restriction for one or more named programs. As long as the second rule is higher in the list of rules, it will take affect.
- **Reset:** Restores the predefine(default) file protection rules that are provided by LANDesk.
- **Add:** Opens the Configure file protection rule dialog where you can add and remove programs and files and specify the restrictions.
- **Configure:** Opens the Configure file protection rule dialog where you can edit an existing file protection rule.

- **Delete:** Removes the file protection rule from the database.

Note: File protection rules are stored in the FILEWALL.XML file, located in: ProgramFiles\Landesk\ManagementSuite\ldlogon\AgentBehaviors\Hips_Behavior.ZIP.

About the HIPS: Configure file protection rule dialog

Use this page to configure file protection rules.

This dialog contains the following options:

- **Rule name:** Identifies the file protection rule with a descriptive name.
- **Apply rule to**
    - **All programs:** Specifies that all executable programs are restricted from performing the actions selected below on the files specified below.
    - **Programs named:** Specifies that only the executable programs in the list have the restrictions selected below applied to them.
    - **Add:** Lets you choose which programs are restricted by the file protection rule. You can use filenames and wildcards.
    - **Edit:** Lets you modify the program name.
    - **Delete:** Removes the program from the list.
- **Restrictions**
    - **Deny access:** Prevents the programs specified above from accessing the protected files.
    - **Deny modification:** Prevents the programs specified above from making any changes to the protected files.
    - **Deny creation:** Prevents the programs specified above from creating the files.
    - **Deny execution:** Prevents the programs specified above from running the protected files.
- **Exceptions**
    - **Allow exceptions for certified programs:** Allows any of the executable programs that currently belong to your list of certified files to bypass the restrictions associated with this file protection rule.
- **Files**
    - **Any files:** Specifies that all files are protected from the programs specified above according to their restrictions.
    - **Files named:** Specifies that only the files in the list are protected.
    - **Add:** Lets you choose which file or files are protected by the rule. You can use filenames or wildcards.
    - **Edit:** Lets you modify the file name.
    - **Delete:** Removes the file from the list.
    - **Apply to sub-directories too:** Enforces the file protection rules to any subdirectories of a named directory.

Understanding the HIPS learn mode

HIPS can run in one of the following protection modes: Automatic, Learn, Log only, or Block.

Using the HIPS learn mode

Below is a description of the HIPS learn mode process:

- In learn mode, HIPS learns what kind of applications are installed on the device, how they behave, and their rights (privileges).

- HIPS monitors activity on the device and records information in an action history file.
- Action history data is sent from the device to the core server.
- Administrators read the action history to see which applications are doing what on the device (The files/applications and associated rights listed in the action history file (XML) are displayed in the File certifications page of the HIPS settings dialog.)
- Then administrators can customize HIPS settings to allow and deny privileges for relevant applications.

Learn mode can be applied to managed devices generally allowing HIPS violations to occur until a new HIPS settings is deployed, or learn mode can be applied initially for a specified period of time in order to discover what applications are run and their behavior and to create a whitelist (applications allowed to execute on devices). If the general protection mode is automatic blocking, you can still use learn mode to discover application behavior and then re-enforce automatic blocking mode once the learning period has expired.

Note that both the core server and the managed device must be operating in learn mode in order for the action history communication to take place.

Merging HIPS certifications

To merge HIPS certified files from one HIPS settings to one of more other HIPS settings. This lets you update and share certified file settings quickly and easily.

1. In the **Security Configurations** tool window, right-click **Host Intrusion Prevention**, and click **Merge certified files**.
2. Select a source configuration from the drop-down list.
3. Select whether you want to merge differences in the certified files or simply replace all certified files.
4. Select the target configuration(s).
5. Click **OK**.

About the Merge certified files dialog

Use this dialog to configure and execute a merger of HIPS certified files between one or more HIPS settings.

This dialog contains the following options:

- **Source configuration:** Specifies the HIPS settings whose certified files you want to merge with the selected target configurations.
- **Merge differences in certified files:** Replaces any common certified files in the target configurations with the ones in the source configuration, and adds unique certified files from the source configuration to the target configurations.
- **Replace certified files:** Forces the certified files in the source configuration to replace all of the files in the target configurations.
- **Target configurations:** Specifies the target configurations you want to be merged with the source configuration. Select targets from the list of available configurations.

LANDesk Firewall

The new LANDesk Firewall tool is an important component of Endpoint Security that lets you protect managed devices from unauthorized application operations and connections.

With LANDesk Firewall settings, you can create and configure trusted programs (applications), trusted network scopes, and connection rules to protect managed devices from unauthorized intrusions.

LANDesk Firewall and Windows Firewall
The LANDesk Firewall complements the Windows Firewall, and both can be enabled and running at the same time on managed devices.

Component of Endpoint Security

LANDesk Firewall is one of the components of the comprehensive Endpoint Security solution, along with the Host Intrusion Prevention (HIPS) and Device Control tools.

Read this section to learn about:

- "Using LANDesk Firewall settings" on page 410
- "LANDesk Firewall settings help" on page 412

Using LANDesk Firewall settings

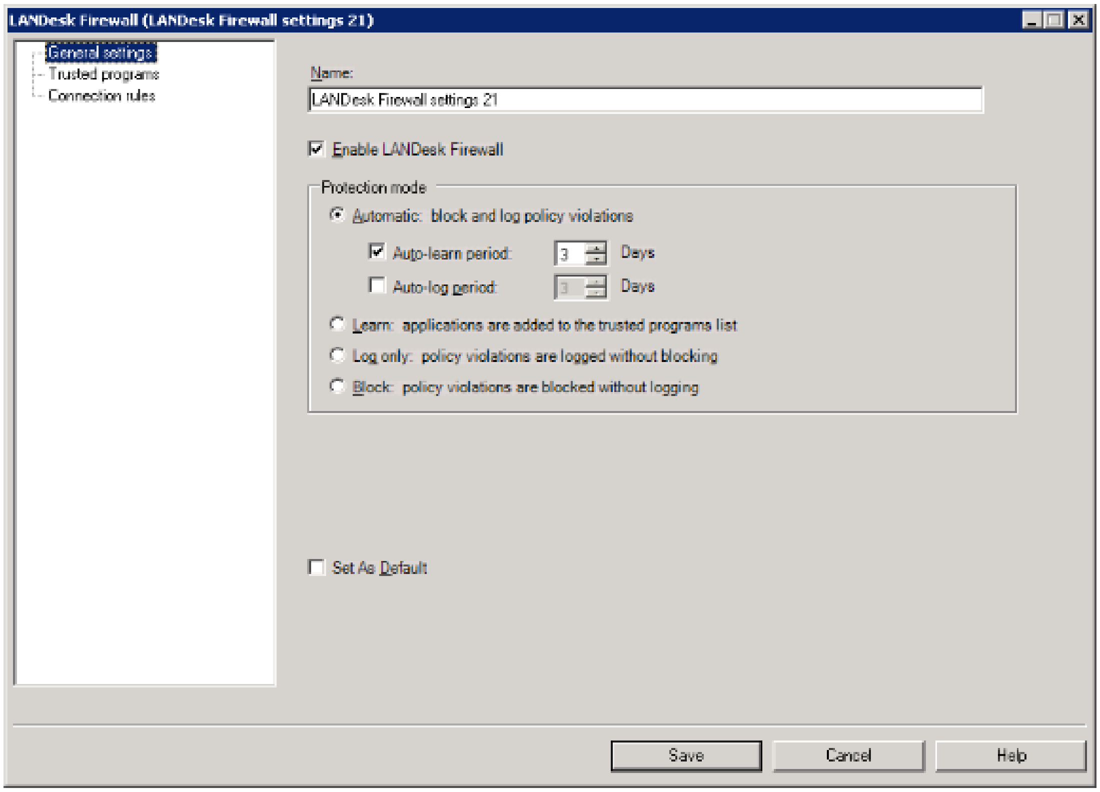
Firewall settings give you complete control over how the LANDesk Firewall operates on target devices.

This section describes how to create and manage Firewall settings.

Creating LANDesk Firewall settings

To create LANDesk Firewall settings

1. In the **Security Configurations** tool window, right-click **LANDesk Firewall**, and then click **New**.



Name: LANDesk Firewall settings 21

☑ Enable LANDesk Firewall

Protection mode

● Automatic: block and log policy violations

☑ Auto-learn period: 3 Days

□ Auto-log period: 3 Days

○ Learn: applications are added to the trusted programs list

○ Log only: policy violations are logged without blocking

○ Block: policy violations are blocked without logging

□ Set As Default

2. At the **General settings** page, enter a name for the settings, enable the LANDesk Firewall service, and then specify the protection mode. For information about an option, click **Help**.
3. At the **Trusted programs** page, add and edit applications you want to be able to connect to and from the network and the Internet. You can also define the trusted scope.
4. At the **Connection rules** page, define the connection rules (incoming or outgoing, and action) by port, protocol, or IP range.
5. Click **Save**.

Once configured, you can deploy settings to target devices with an installation or update task, or a change settings task.

LANDesk Firewall settings help

Use this dialog to create and edit a LANDesk Firewall settings. When creating Firewall settings, you first define the general protection mode, and then add and configure specific trusted programs, trusted scopes, and connection rules. You can create as many settings as you like and edit them at any time.

If you want to modify the device default settings without reinstalling the Endpoint Security agent or redeploying a full agent configuration, make your desired change to any of the options on the settings dialog, assign the new settings to a change settings task, and then deploy the change settings task to target devices.

This dialog contains the following pages.

About the General settings page

Use this page to enable the LANDesk Firewall and configure the protection mode.

This page contains the following options:

- **Name:** Identifies the Firewall settings with a unique name.
- **Enable LANDesk Firewall:** Allows all programs to run except when a program's operation threatens system security as defined by predefined protection rules.
- **Protection mode:** Specifies protection behavior when security violations occur on managed devices.
    - **Automatic:** All policy violations are automatically blocked. In other words, all of the trusted program, trusted scope and connection rules (i.e., permissions) you've created are enforced.
        - **Auto-learn period:** (Note that these two time period options are successive. In other words , if both are selected, the auto-learn period runs first and when it expires, the auto-log period runs.) Allows the administrator to specify a period of time during which the end user can run any of the applications on their machine. During this period, applications that run are observed (or learned).
        - **Auto-log period:** Specifies a period of time during which the applications that run are recorded in an action history file.
    - **Learn:** All applications are allowed to run, but are monitored and recorded in an action history file. Additionally, all of the applications that are run on the device are learned and added to the trusted programs list.
    - **Log only:** Policy violations are logged, but not blocked.
    - **Block:** Policy violations are blocked, but not logged.

About the Trusted programs page

Use this page to create and manage trusted programs and trusted scopes.

This page contains the following options:

- **Trusted applications:** Lists the applications that have connection rules configured for firewall protection.
- **Trusted scope:** Lists the network scopes that have connection rules configured for firewall protection.
- **Add:** Opens a file explorer dialog where you can browse and select an application you want to configure with connection rules.
- **Edit:** Lets you edit the selected application's connection rules.
- **Delete:** Deletes the selected application and its connection rules.

About the Configure trusted application dialog

Use this page to configure connection rules for a specific application.

This page contains the following options:

- **Application details:** Identifies the application file that is being assigned connection rules (i.e., permissions). You can a description of the file.
- **Outbound connection**
  - **Allow application to connect to the trusted scope (network):** Allows the application to connect to locations within the trusted scope you've defined.
  - **Allow application to connect outside the trusted scope (Internet):** Allows the application to connect to locations outside of the trusted scope you've defined.
- **Inbound connection**
  - **Allow application to receive connections from the trusted scope (network):** Allows the application to receive connections from locations within the trusted scope you've defined.
  - **Allow application to receive connections from outside the trusted scope (Internet):** Allows the application to receive connections from locations outside of the trusted scope you've defined.
- **Locked trusted application:** Ensures the application retains the connection rules you assign here, even if the application is allowed other operations during a learn mode.
- **OK:** Saves the connection rules and adds the application to the list of trusted programs.
- **Cancel:** Closes the dialog without saving.

About the Trusted scope dialog

Use this page to configure and manage trusted scopes. A trusted scope is made up of a collection of network addresses, by IP address, IP range, or subnet.

This page contains the following options:

- **Trust client's subnet:** Adds the target device's subnet range to the trusted scope list. Communication across that subnet range is allowed.
- **Trusted scopes:** Lists all of the trusted scopes.
- **Import:** Lets you import subnet ranges from managed devices contained in the core database inventory.
- **Add:** Lets you add a trusted location to the list. Add a trusted location by: IP address, IP range, or subnet.
- **Edit:** Lets you modify the selected existing trusted location.
- **Delete:** Removes the selected trusted location.

About the Connection rules page

Use this page to view, manage, and prioritize connection rules. Connection rules can allow or prevent connections based on port or IP range, whether the program is trusted, and whether the communication is within the trusted network scope.

This page contains the following options:

- **Connection rules:** Lists all of the connection rules.
- **Move up:** Determines the priority of the connection rule. A connection rule higher in the list takes precedence over a rule that is lower in the list.
- **Move down:** Determines the priority of the connection rule.
- **Reset:** Restores the rule order.

- **Add:** Opens a dialog where you can configure a new connection rule.
- **Edit:** Lets you modify the selected connection rule.
- **Delete:** Removes the connection rule from the database.

About the Configure connection rule dialog

Use this page to configure connection rules.

This page contains the following options:

- **Name:** Identifies the connection rule with a descriptive name.
- **Ports:** Lets you define port restrictions for the connection rule.
    - **Apply to these local ports:** Specifies the local ports to which the direction and action (selected below) are applied. For example, if Incoming is selected and Accept is selected, connections to the local ports specified here are allowed.
    - **Apply to these remote ports:** Specifies the remote ports to which the direction and action (selected below) are applied.
- **Protocol:** Specifies the communication protocol for the selected ports.
- **IP range:** Lets you define IP range restrictions for the connection rule.
    - **Apply to these remote addresses:** Specifies the remote IP address range to which the direction and action (selected below) are applied.
- **Direction:** Indicates whether the connection rule restricts inbound or outbound connections.
- **Action:** Indicates whether the connection rule allows (accept) or prevents (drop) connections.
- **Allow trusted programs to bypass:** Lets you give trusted programs the ability to ignore or bypass this connection rule.
    - **Only for trusted scope:** Limits the trusted programs ability to bypass the connection rule only if the communication is within the trusted network scope.
- **OK:** Saves the options and adds the rule to the list of connection rules.
- **Cancel:** Closes the dialog without saving.

Device Control

The new Device Control tool is an important component of Endpoint Security that lets you monitor and restrict access for I/O devices. With Device Control, you can restrict the use of devices that allow data access to the device, such as ports, modems, drives, and wireless connections.

Read this section to learn about:

Device Control overview

To implement Device Control on clients on your network, you create and deploy Device Control settings that manage USB, modem, I/O port, CD/DVD drive, PCMCIA, and other connections.

You can configure USB restrictions by either generically blocking a whole class of USB devices, such as storage devices, or by using exceptions to restrict certain USB devices based on parameters and values you specify.

Component of Endpoint Security

Device Control is one of the components of the comprehensive Endpoint Security solution, along with the Host Intrusion Prevention (HIPS) and LANDesk Firewall tools.

Supported platforms

Device Control supports managed devices running:

- Windows 2000
- Windows Server 2003
- Windows XP
- Windows Vista (32-bit, and 64-bit)

Using Device Control settings to restrict device access

For Device Control to function on a device, you must have the local scheduler agent and the standard agent deployed on that device. Every time the device initiates a device connection or makes changes to a device connection, the agent applies setting rules. These rules include terminating connections that aren't allowed and sending alerts to the core server.

By default, device control settings can restrict the various types of devices. You can use the advanced USB settings to restrict any USB device or class of devices that you specify. Among the devices you can restrict are:

- USB devices such as drives, keyboards and mice, printers, and scanners
- RIM Blackberry*, Pocket PC*, and Palm* handheld devices

- Network volumes
- Bluetooth* Personal Area Networks
- Wireless 802.11x networks
- Modems
- PCMCIA* devices
- Serial, parallel, infrared, and FireWire 1394 ports
- Floppy and CD/DVD drives

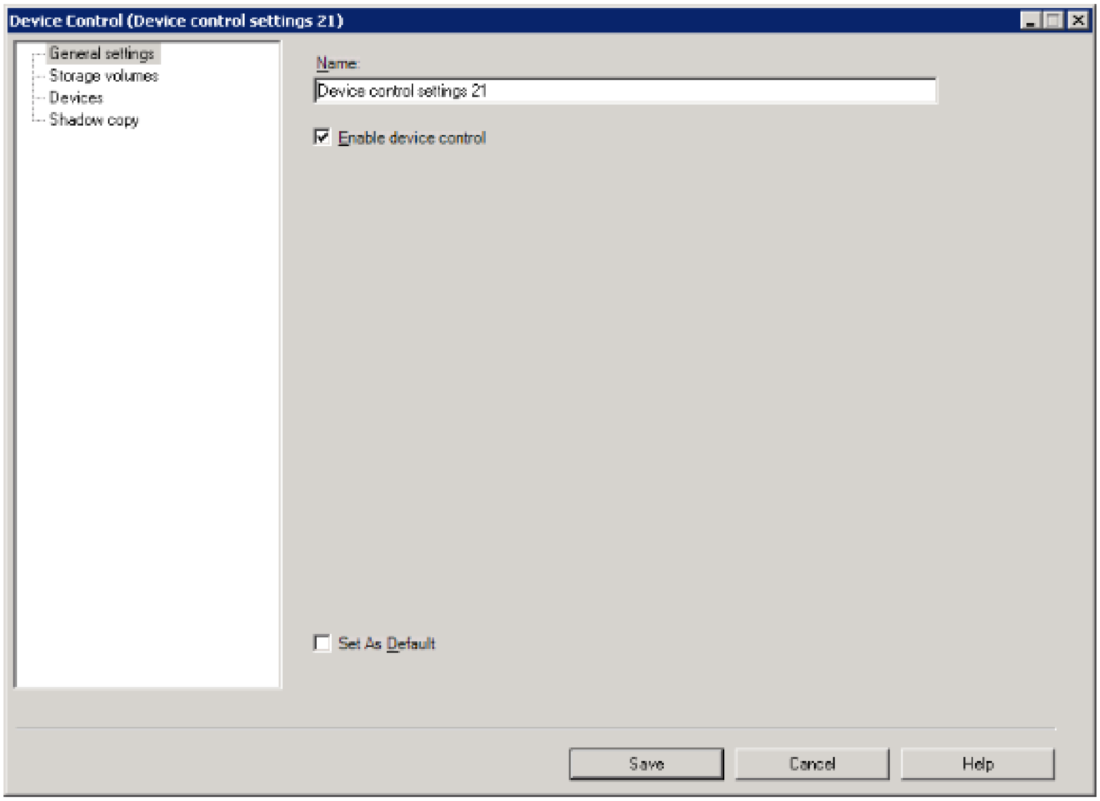
USB device control setting utilizes the usbmon service, which can:

- Prevent the use of unauthorized USB and PCMCIA devices.
- Prevent the use of unauthorized removable storage devices.
- Trigger an external program or script when it detects an unauthorized device.

Creating device control settings

To create device control settings

1. Click **Tools > Security > Security Configurations**.
2. Open Endpoint Security, right-click **Device Control**, and then click **New**.



Device Control (Device control settings 21)

Name: Device control settings 21

☑ Enable device control

□ Set As Default

3. On the General Settings page, enter a **Name**.
4. Check the **Enable device control** checkbox.
5. On the other pages, customize the options you want. For more information about the options on the dialog, see "Device Control settings help" on page 418.

6. Click **Save** to save the settings.

Deploying Device Control settings

Once you've created a Device Control settings, you must deploy it to managed devices before it will be active.

Device Control is deployed via an Endpoint Security settings.

To deploy device control settings

1. Right-click the settings, and then click **Schedule**.
2. The settings is added to the **Scheduled tasks** window. In this window, drag devices onto the settings icon.
3. When all devices have been added, from the task's shortcut menu, click **Properties**. In the tree click **Schedule task**, and configure the scheduling options.

For more information on scheduling tasks, see "Scripts and tasks" on page 120.

When you schedule a device control settings for deployment, Device Control does the following:

- It creates an executable distribution package that's named after the source device control settings. The package's primary file is usbmon.exe. Additional files are usbmon.reg, devactalert.exe, netres.mrl, and <*device control settings name*>.ini.
- If you target users for the device control settings task, Device Control uses a public policy-based delivery method called "Usbmon Pull Delivery." If this delivery method doesn't exist, Device Control creates it. When task targets are users, Device Control has to use a policy-based delivery method to ensure that the correct user gets the settings. When target users log on, the policy-based delivery method activates and installs the settings.
- If you target computers for the device control settings task, Device Control uses a public policy-supported push delivery method called "Usbmon Push Delivery." If this delivery method doesn't exist, Device Control creates it. Since the settings targets a device, any user that logs into that device will get that device control settings; it doesn't matter who is logged in when the settings gets installed. You can use push or policy delivery methods for computers.

Once Device Control creates the usbmon policy or policy-supported push delivery methods, you can customize them. As long as the method name doesn't change, Device Control will use the modified delivery method.

For more information on creating device control settings locally on managed computers and deploying those settings manually, view the usbmon help file, usbmon.chm in the core server's LDMain share.

Device Control settings help

Use this dialog to create and edit Device Control settings.

This dialog contains the following pages.

About the General settings page

Use this page to name the settings and enable device control on a client configured with this settings.

- **Name:** Identifies the settings. This name appears in the main Device Control window.
- **Enable device control:** Turns on Device Control on a client configured with this settings.

About the Storage volumes page

Use this page to specify options for storage volumes that connect to a client configured with this settings.

- **Storage volumes:** Specifies the access level for any storage volume that wasn't present on the client when the settings was installed. (Note that if a device containing a volume was attached when the settings was installed, the usbmon service will allow that device in the future, even though it may be removable.)
  - **Full access:** Allows read and write access to a connecting storage volume.
  - **Read only access:** Allows users to read from but not write to a connecting storage volume.
  - **Force encryption:** Enforces file encryption on a connecting storage volume. An encryption utility is deployed that enables file encryption on a storage device connecting to a client with this settings. Files are encrypted when written to a storage device and decrypted when read from the device. Access is allowed only by providing the correct password that is defined when creating an encrypted folder on the USB storage device.

    IMPORTANT: First create an encrypted folder on the USB device: When a storage device is configured for file encryption, users must initially create an encrypted folder before they can copy files to the device with the encryption utility (go to **Start | LANDesk Management | LANDesk Encryption | Advanced | Create encrypted folder**). Specify a password when creating the encrypted folder. If the Allow password hints option is enabled (see below), the user will have the option of entering a hint that can help them remember the password, although the password hint is not required.

  - **No access:** Prevents the use of storage volumes connecting to a client configured with this device control settings. You can customize which types of devices are still allowed by selecting specific device types on the Device page.
- **Exceptions:** Click to create exceptions to the access level for storage volumes. You can add exceptions based on: hardware ID, media serial, or bus type.
- **Encryption options:**
  - **Storage space allocated for encryption:** Specifies the amount of space on a storage device that can be used for encrypted files. (Note the maximum amount of space that can be used for encrypted files is 128 MB.)
  - **Allow password hints:** Lets the end user enter a hint that can help them remember the encrypted folder password. The password hint cannot be an exact match to the password itself. The password hint cannot exceed 99 characters in

length. (Note that even if the password hint field is available to enter text, the user is not required to enter a hint.)

- **Notify end users:** Displays a message box when a user connects an unauthorized storage device. For more information, see "Creating custom messages when unauthorized devices/volumes are detected" on page 421.

About the Configure exception (for storage volumes) dialog

Use this dialog to create an exception to the access level for storage volumes.

- **Description:** Enter any description you want to identify this exception.
- **Parameter:** Select the parameter type (hardware ID, volume serial, or bus type).
- **Value:** If the hardware ID parameter is selected, enter a value string.
- **Access:** Specifies the access level for this exception (full access, read-only access, encrypted only, no access)

About the Devices page

Use this page to specify options for various device types that connect to a client configured with this settings.

- **Devices / Interfaces:** Use the checkboxes to block devices and interfaces from accessing the client.
- **Block wireless LAN 802.11X:** Blocks a wireless LAN802.11X connection.
- **Exceptions:** Click to create exceptions to blocked devices and interfaces. You can add exceptions based on: hardware_id, class, service, enumerator, vendor_id, device_id, or vendor_device_id.
- **CD / DVD drives:** Specifies the access level for CD / DVD drives.
- **Exceptions:** Click to create exceptions to the access level for CD / DVD drives. You can add exceptions based on: hardware ID, media serial, or bus type.
- **Notify end users:** Displays a message box when a user connects an unauthorized storage device. For more information, see "Creating custom messages when unauthorized devices/volumes are detected" on page 421.

About the Configure exceptions (for devices and interfaces) dialog

Use this dialog to create an exception for blocked devices and interfaces.

- **Description:** Enter any description you want to identify this exception.
- **Parameter:** Select the parameter type (hardware ID, volume serial, or bus type).
- **Value:** If the hardware ID parameter is selected, enter a value string.
- **Access:** Specifies the access level for this exception (full access, read-only access, encrypted only, no access)

About the Shadow copy page

Use this page to enable and configure shadow copy on managed devices configured with this settings.

Shadow copy lets you track what files have been copied to and from the device by making a duplicate (or shadow) copy of those files in a local directory.

- **Enable shadow copy:** Turns on shadow copy on managed devices with this settings.
- **Log events only:** Indicates that only the file copy activity is recorded in a log file, not the actual files that are being copied.

- **Exceptions:** Click to create exceptions. You can add exceptions based on: hardware ID, media serial, or bus type.
- **Local cache:** Specifies the location on the local drive where the shadow copy files and log file are stored.

Device Control management tasks

This section includes information about the following Device Control features and tasks.

- "Creating custom messages when unauthorized devices/volumes are detected" on page 421
- "Unauthorized device handling" on page 421
- "Removable storage device handling" on page 422
- "Configuring advanced USB settings" on page 423
- "Configuring commands that run when an unauthorized device is detected" on page 424
- "Configuring alerts" on page 424
- "Viewing the unauthorized device list" on page 424

Creating custom messages when unauthorized devices/volumes are detected

In the **Device control settings** dialog, you can customize the message text that the user sees when unauthorized devices/volumes are detected. In the message text, you can use these placeholders to show information about the unauthorized volume or device:

- %vol%: volume serial number
- %desc%: description
- %service%: service
- %hwid%: hardware ID
- %mfg%: manufacturer
- %loc%: location
- %class%: class

Unauthorized device handling

Device control settings use the usbmon service on managed devices. When the usbmon service receives notification from the OS that a new USB or PCMCIA device has been inserted, the usbmon service applies a number of custom defined rules to decide whether or not the device is allowed. You can set up simple rules to allow only certain types of devices such as keyboards and mice, printers, and scanners. More complex rules might allow only secure storage devices of a given manufacturer, or exclude devices of a given manufacturer.

When an unauthorized device is detected, the usbmon service will:

- Remove the device from the Windows Device Manager so Windows won't see it any more. Any drivers for the device remain installed.
- In the case of an unauthorized USB device or volume, optionally display a configurable message to the user. For more information, see "Creating custom messages when unauthorized devices/volumes are detected" on page 421.
- Optionally load an external program (For more information, see "Configuring commands that run when an unauthorized device is detected" on page 424). For example, the external program can be a script that sends an alert to a central console.
- Send a "Disabled device activated" AMS alert to the core server. The alert message includes the device name.

Removable storage device handling

Usbmon is the name of the service on managed devices that restricts USB connections. When a new volume is mounted, the usbmon service receives notification from the operating system. The usbmon service then uses the GetDriveType() API call to check the type of drive that was mounted. If the OS describes the drive as "removable" or "fixed drive", the usbmon service will take action. The usbmon service also checks for removable volumes at boot time. If an unauthorized volume is found at boot time, the same actions are taken as when the volume is mounted later.

Drives that are considered removable include (but are not limited to) USB storage devices. CD drives (read-only or read/write) are not considered removable storage.

The OS doesn't consider hard drives as removable. The GetDriveType() call describes them as "fixed drive" even if they are attached via USB or some other external port. To allow removable hard drives to be handled the same as other removable storage devices, the usbmon service records the list of hard drives at the time the service is installed. For example, if a device has two hard drives (C: and D:) at the time the usbmon service is installed, the usbmon service will consider those drives as fixed and will not check them. But if at some later time a hard drive with drive letter E: is found, the usbmon service will consider it a removable device.

The usbmon service keeps the list of "fixed drives" in the registry at HKLM\Software\LANDesk\usbmon\FixedDrives. This list is created at the time the service is installed. The **No access** option blocks access to any volume that wasn't present when the device control settings was installed. Note that if a device containing a volume was attached when the settings was installed, the usbmon service will allow that device in the future, even though it may be removable.

When a removable storage device is detected, the usbmon service will:

- Lock the volume. Users who attempt to access the volume will get an "access denied" error.
- Optionally display a configurable message to the user.
- Optionally load an external program. For example, the external program can be a script that sends an alert to a central console.
- Send a "Disabled device activated" AMS alert to the core server. The alert says a volume was activated, but additional information about the volume isn't available.

Blocking all unknown volumes works for Windows XP or Windows 2003 only
In Windows 2000, the operating system says that the volume is blocked when it really isn't blocked. We recommend that for Windows 2000 you block specific devices in order to prevent the addition of new volumes.

What if a support person needs to use a USB memory stick?

If you're an IT support person and you want to use a USB storage device on a user's computer, there are several things you can do:

- The most convenient method of allowing access to a USB device on a temporary basis is to enable the password override option when defining and deploying a device control settings to your managed devices.

You can try the following methods if the device control isn't configured with the password override feature:

- Log on with admin rights and temporarily disable the usbmon service.
- Log on with admin rights, run the usbmon GUI and add the device to the list of authorized volumes.

Configuring advanced USB settings

Once Device Control is installed on a device, the agent stores information about the last ten USB devices that it blocked access to. The inventory scanner sends this information to the core database. Information about these blocked devices then appears in the **Advanced USB settings** dialog. You can use this information to create advanced rules that allow or block specific USB devices. These advanced rules allow you to control more than just the basic device categories you see in the **Device control settings** dialog.

In the **Advanced USB settings** dialog, you can base a rule on any of the six columns. Right-click on a value in the column and click **Allow** to create a rule that allows devices based on that attribute. The keywords created for each of the columns are the following:

```
DeviceDesc
HardwareID
Service
Mfg
LocationInformation
Class
```

These are the same names that are used in the registry under the HKLM\System\CurrentControlSet\Enum\USB key.

The most useful field to base rules on is usually **Service**. This corresponds to a Windows driver. For example, the driver for USB ActiveSync connections to Windows CE PDAs is called wceusbsh (see HKLM\CurrentControlSet\Services\wceusbsh). Any of the six columns can be used to base a rule on, however, it is up to you to decide which rules make sense for your situation.

Wildcards

You can use wildcards in rules, for example, the following would allow any device that has the string "floppy" in its device description:

```
DeviceDesc=*floppy*
```

Whitelist vs. Blacklist rules

All the rules illustrated so far have been whitelist rules, where devices are forbidden unless they satisfy at least one of the rules. The usbmon service also supports blacklist rules. Rules prefixed by a minus sign are blacklist rules. For example:

```
Service=usbstor
DeviceDesc=*floppy*
```

The first rule allows USB storage devices. The second rule blacklists devices that have the string "floppy" in their device description.

If both whitelist and blacklist rules are defined, the usbmon service first checks devices against the whitelist rules. If there are no whitelist rules that allow the device, the device is forbidden. If there is at least one whitelist rule that allows the device, then the usbmon service checks the device against the blacklist rules. If the device satisfies none of the blacklist rules, it is allowed. Otherwise it is forbidden.

If only whitelist rules exist, a device is forbidden unless it satisfies one of the whitelist rules. If only blacklist rules exist, a device is allowed unless it satisfies one of the blacklist rules.

Composite rules

All the rules illustrated so far have been simple rules, where a single field is tested. Usbmon also supports composite rules, as in the following example:

```
Service=wceusbsh,DeviceDesc=*iPAQ*
```

This rule allows only Windows CE devices that have the string IPAQ in their device description.

Composite blacklist rules are also possible. Example:

```
Service=wceusbsh
Service=wceusbsh,Mfg=*iPAQ*
```

The above two lines allow Windows CE devices, except those that have the string IPAQ in their manufacturer field. The above lines are equivalent to the following single line:

```
Service=wceusbsh,-Mfg=*iPAQ*
```

Configuring commands that run when an unauthorized device is detected

When the usbmon service detects an unauthorized volume or device, it can execute external programs. You can include one or two placeholders in the commands:

- %1: will be replaced with either "volume" or "device", depending on whether an unauthorized volume or an unauthorized USB device was detected.
- %2: will be replaced with either the volume serial number of the unauthorized volume, or with the identification string of an unauthorized USB device.

For example, when a command such as the following is given:

```
wscript myscript.vbs %1 %2
```

This might cause the following command to be launched:

```
wscript myscript.vbs volume "1234ABCD"
wscript myscript.vbs device "Y-E Data USB Floppy: Vid_057b&Pid_0000"
```

Usbmon guarantees that only one instance of the script will be running at the same time.

To configure commands

1. In a device control settings, click **Commands**.
2. Enter the commands you want.
3. Click **OK**.

Configuring alerts

Device Control settings use the alert management system for alerting. Device Control can trigger alerts on these events:

- Configuration error
- Disabled device activated
- Restricted network connection attempted
- Unlisted network connection attempted
- Unlisted network session detected

Viewing the unauthorized device list

On each computer, Device Control stores a list of the ten most recent unauthorized devices that were connected.

You can view this information from the **Network view** by clicking **Inventory** on a device's shortcut menu. Then click **LANDesk Management | Device Control | Usbmon alert**.

Troubleshooting Device Control

This section contains information about some possible situations you might encounter with Device Control, and how to address them.

- Each new Device Control settings is saved as one settings file and one script file in the following folders:
    - ldmain\ccmgr\name.cfg
    - ldmain\scripts\name.ini
- If a script or settings already exists with the same name that you give a settings, you'll be prompted to overwrite the existing script or settings. This can cause an unrelated distribution script of the same name to be overwritten.
- When entering IP ranges for network restrictions, don't restrict access to the network range the core server is on. If clients access a restricted network and Device Control disables network access, only communication with the core server can restore network access. If devices can't communicate with the core server because of a restriction, network access can't be restored.
- When restricting access to I/O devices, don't restrict I/O devices that host network adapters. If you restrict access to I/O devices that host a network adapter, that client will no longer be able to access the network. For example, restricting USB access prevents any USB network adapters from working. Without network access, you won't be able to update restriction settings for that client.
- If you select the following options in Device Control, and the core server isn't available on a listed network, clients will have unrestricted I/O device access while on that network:
    - Limit connections to listed networks
    - Allow unlisted networks if not connected
    - Verify core server existence on the network
- If "Allow unlisted networks if not connected" is checked, and the agent can't find the core on a listed network, it will assume that the network is unlisted. At this point, unintended access may be granted to local I/O devices. This can create a security risk. Make sure the core server is available to prevent this from happening.

Security Activity

The new Security Activity tool provides a convenient single window where you can view status and activity information for several LANDesk Security Suite services running on your managed devices.

Security Activity lets you view status and activity information for:

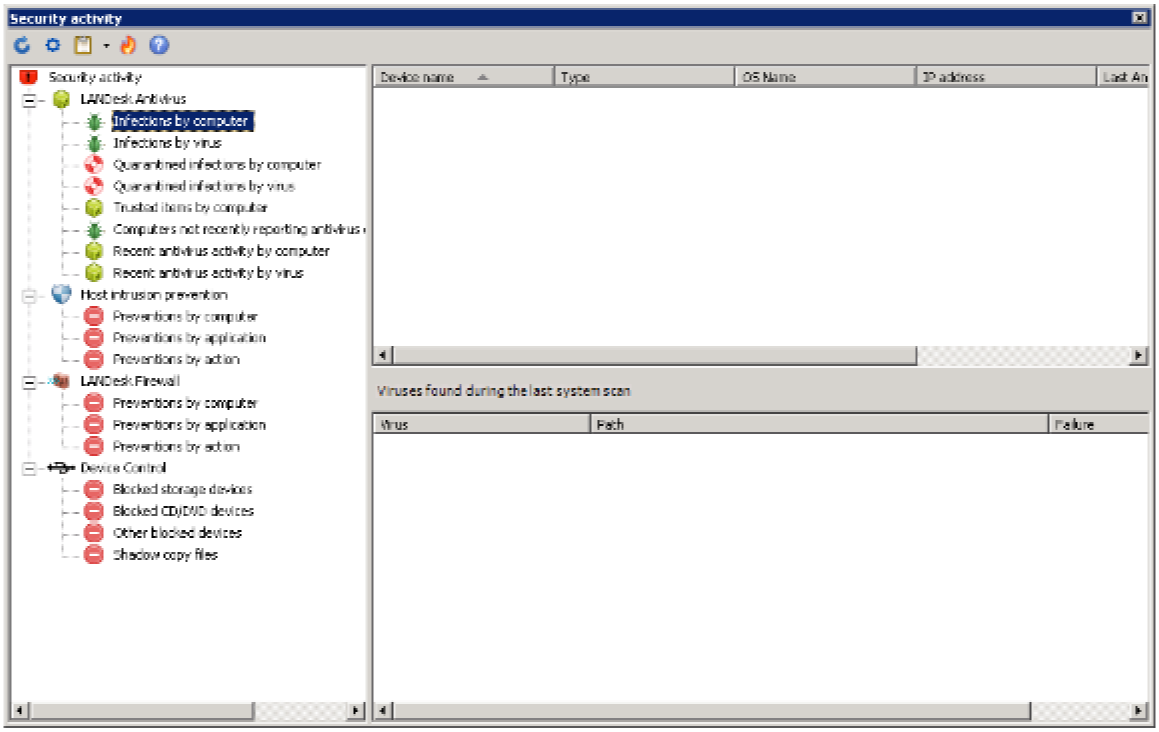
- LANDesk Antivirus
- Host Intrusion Prevention (HIPS)
- LANDesk Firewall
- Device Control

You can also perform these tasks:

- Configure security activity threshold settings
- Purge security activity information

Viewing security status and activity

The Security Activity tool lets you view information about LANDesk Security Suite services.



For example:

Viewing Antivirus activity and status information

If the antivirus scanner discovers any of the selected virus definitions on target devices, this information is reported to the core server. You can use any of the following methods to view detected security data after running a scan.

This window displays antivirus activity and status information by the following categories:

- Infections by computer
- Infections by virus
- Quarantined infections by computer
- Quarantined infections by virus
- Trusted items by computer
- Computers not recently reporting antivirus activity
- Recent antivirus activity by computer
- Recent antivirus activity by virus

Additionally, for a scanned device, right-click the device, select Security and Patch Information, in the Type drop-down list select Antivirus. You can view:

- Missing antivirus updates
- Installed antivirus updates
- Purge repair history

About the Antivirus activity and status information dialog

Use this dialog to view detailed antivirus activity and status information for all of your managed devices with the LANDesk Antivirus agent. This scan result data is used to generate the LANDesk Antivirus reports available in the **Reports** tool.

To customize the scope and focus of data that is displayed, click **Thresholds** and change the time period thresholds for scanned device's recent antivirus activity and devices that haven't recently been scanned.

You can also right-click a device in this view to access its shortcut menu and directly perform available tasks.

This dialog contains the following options:

- **Refresh:** Updates the fields in the dialog with the latest antivirus scan information from the database.
- **Thresholds:** Opens the **Threshold settings** dialog, where you can define the duration (in days) for both recent antivirus activity and "not recent" antivirus scanning. Thresholds determine the time period for which antivirus scan results are gathered and displayed for the two computer-specific display categories.
- **Infections by computer:** Lists devices in the right pane on which virus infections were discovered during the last system scan. Select a device to see the specific viruses infecting the device.
- **Infections by virus:** Lists viruses in the right pane that were discovered on managed devices during the last system scan. Select a virus definition to see the devices it has infected.
- **Computers not recently scanned for antivirus vulnerabilities:** Lists all of the devices with the LANDesk Antivirus agent that have not been scanned for viruses within the time period specified on the **Threshold settings** dialog. If you want to run an immediate antivirus scan, right-click the device, click LANDesk Antivirus scan now, select an antivirus settings, and then click OK.
- **Computers with recent antivirus activity:** Lists all of the devices with the LANDesk Antivirus agent that have been scanned and have returned antivirus activity within the

time period specified on the **Threshold settings** dialog. Select a device to see its specific antivirus activities, including: virus detection, removal, infected object quarantine, backup, and restoration.

Viewing HIPS activity

If HIPS detects violations to its rules and certification rights, this information is reported to the core server. You can use the following methods to view detected HIPS activity.

For information about HIPS activity throughout your network, in the Security Activity tool, open the **Host Intrusion Prevention** group. The window displays HIPS activity by the following categories:

- Preventions by computer
- Preventions by application
- Preventions by action

You can also view specific host intrusion activity at the bottom of the window, including the following details:

- Action Date
- Action
- Description
- Application
- File version
- File size
- File date
- Mode
- MD5 hash

About the HIPS activity dialog

Use this dialog to view detailed HIPS activity for all of your managed devices with the LANDesk HIPS agent. This data is used to generate the LANDesk HIPS reports available in the **Reports** tool.

To customize the scope and focus of data that is displayed, click **Thresholds** and change the time period threshold for storing HIPS activity information in the core database, and for the number of items to display in the HIPS activity window lists.

You can also right-click a device in this view to access its shortcut menu and directly perform available tasks.

This dialog contains the following options:

- **Refresh:** Updates the fields in the dialog with the latest HIPS information from the database.
- **Thresholds:** Opens the **Threshold settings** dialog, where you can define the duration (in days) for storing HIPS data in the core database and the number of items to display in the HIPS activity lists.
- **Purge:** Completely and permanently removes HIPS activity data from both this display window and the core database.
- **Preventions by computer:** Lists devices in the right pane on which HIPS violations were discovered. Select a device to see the specific violations..
- **Preventions by application:** Lists applications in the right pane that were discovered on managed devices. Select an application to see the devices it was discovered on.

- **Preventions by action:** Lists actions in the right pane that were taken on managed devices. Select an action to see the devices on which it was taken.

Viewing LANDesk Firewall activity

The window displays Firewall activity by the following categories:

- Preventions by computer
- Preventions by application
- Preventions by action

Viewing Device Control activity

The window displays Device Control activity by the following categories:

- Blocked storage devices
- Blocked CD/DVD device
- Other blocked devices
- Shadow copy files

Configuring security activity threshold settings

Security activity information can build up quickly. You can use threshold settings to control how much information is collected.

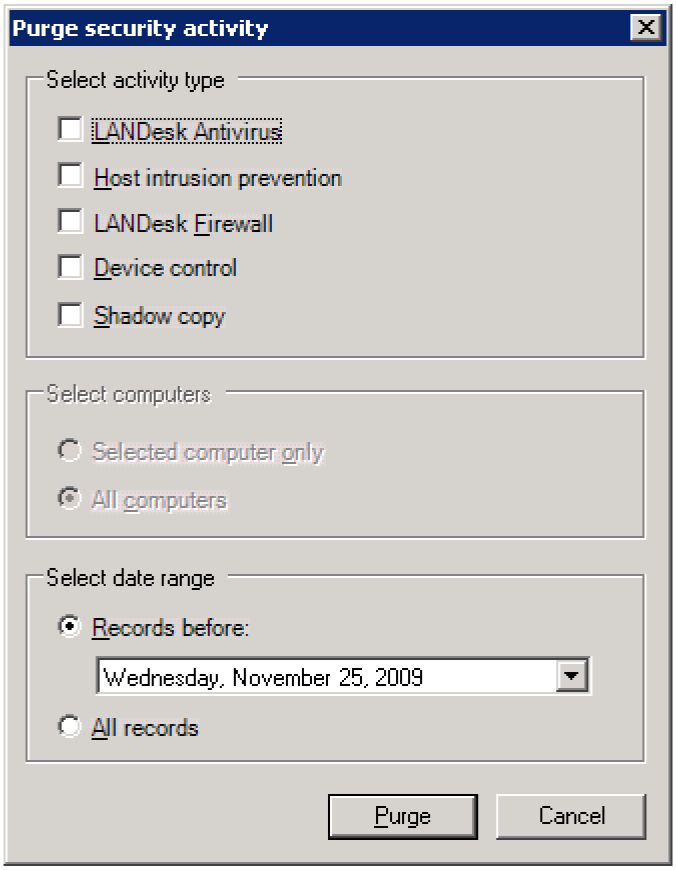
About the Threshold Settings dialog

Use this dialog to define time periods for Antivirus, HIPS, and Firewall activity that appears in Security Activity views.

- **Antivirus:**
  - **Threshold for recent antivirus activity:** Specifies the time period (in days) to collect antivirus activity for devices that have been scanned and have returned antivirus activity.
  - **Threshold for not recently scanned:** Specifies the time period (in days) to collect device information for all devices configured with antivirus that have not been scanned.
- **Truncate lists:** Indicates the maximum number of entries to display in the lists in the activity dialogs. You can specify 1 item to 999,999 items.
- **Automatic purge (HIPS / LANDesk Firewall only):**
  - **Automatically delete activity older than:** Indicates the maximum number of days to keep reported HIPS activity, and LANDesk Firewall activity, for protected devices in the core database. You can specify 1 day to 999 days. However, we recommend that you carefully watch the amount of data being sent to the core and find an optimal number of days so that HIPS data doesn't use too much space or hamper performance.

Purging security activity

From time to time, you may want to purge security activity information for the various security components. You can do this with the **Purge activity** toolbar button in Security Activity.



Purge security activity

Select activity type

□ LANDesk Antivirus

□ Host intrusion prevention

□ LANDesk Firewall

□ Device control

□ Shadow copy

Select computers

○ Selected computer only

● All computers

Select date range

● Records before:

Wednesday, November 25, 2009

○ All records

Security activity purging is a one-time task, not a scheduled task or policy.

About the Purge security activity dialog

Use this dialog to completely remove activity records from the console and core database.

This dialog contains the following options:

- **Select activity type:** Specifies which security component activity information you want to purge.
- **Select computers:** Specifies which managed device(s) about which security activity is purged. (Note: You must be an Administrator users to perform this task.)
- **Select date range:** Specifies the earliest date from which security activity is purged. Or, you can simply purge all of the existing activity information with the **All records** option.
- **Purge:** Completely removes activity records for the security components you've selected.

Network Access Control (NAC)

Network Access Control (NAC) is an important component of a comprehensive security management solution. NAC protects your network from unauthorized access, malicious intrusions, and external security exposures introduced by vulnerable or corrupted devices that can infect and damage your network.

LANDesk Security Suite offers an 802.1X NAC tool designed to support and extend the security of an existing 802.1X Radius server implementation on your network. LANDesk 802.1X NAC support adds authentication and compliance capabilities to basic 802.1X access control functionality.

Technical knowledge and expertise required for setting up Network Access Control
This section describes all the concepts and procedures necessary to install, configure, and use LANDesk 802.1X NAC support. Note that NAC requires additional hardware and software configuration beyond the basic core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with 802.1X Radius server configuration, 802.1X authentication and health posture validation, as well as advanced networking infrastructure design principles and administration. You should recognize that in order to set up NAC you may need to consult with support representatives and/or affiliated system engineers.

The LANDesk User Community has user forums and best known methods for many LANDesk products and technologies. To access this valuable resource, go to: http://community.landesk.com

This introductory section gives a basic overview of NAC technology and services, and describes relevant prerequisites and tools.

Read this section to learn about:

- Network Access Control overview
    - Understanding the basic NAC components
    - Role-based administration with LANDesk 802.1X NAC
- Implementing LANDesk 802.1X NAC support

Network Access Control overview

Network Access Control (NAC) adds an extra layer of protection to your network by letting you prevent vulnerable or corrupted devices from gaining network access, as well as protect critical network resources from connected system that become corrupted.

NAC enforces endpoint perimeter security by using industry standard security technologies and systems. Network Access Control provides flexibility in implementing network access control functionality on your network by supporting common industry standards and methodologies, such as: IEEE 802.1X.

With NAC, you can define custom baseline security policies, scan devices (both managed and unmanaged) for security policy compliance, verify the health status (posture) of connecting devices, and deny or allow access to your critical network resources based on the device's compliance to your security policy. Healthy devices are granted full network access. If a device is determined to be unhealthy, it is blocked from accessing the network and remains in a virtual quarantine area where it can either be repaired with Security Suite remediation capabilities or be allowed limited network access.

With NAC, you can evaluate the security credentials of any device as soon as it attempts to connect to your network by comparing it to custom security policies, monitor the security state of devices that are already connected, allow or deny network access, quarantine devices that fail to meet the security policy requirements, and remediate vulnerable devices so they can be rescanned for security policy compliance and allowed network access once they are deemed healthy.

Network Access Control benefits and features

With NAC, you can:

- Create and enforce customized compliance security policies
- Implement stronger, around-the-clock, enterprise security
- Assess the security credentials (health status) of connecting devices
- Prevent infected or corrupted systems from accessing the network
- Quarantine non-compliant devices in a secure area
- Remediate infected devices to bring them into compliance
- Reduce downtime due to infections from malicious intrusions
- Protect your network, systems, applications, and data from external threats
- Extend existing security technologies and standards

Compliance security policies

Compliance security policies are comprised of rules that verify the health state of a device by checking for: vulnerabilities (in the form of missing or obsolete OS and application patches), software updates, antivirus engine and signature files, firewall presence and settings, and spyware.

For more information on defining a compliance security policy in the Patch and Compliance tool in the console, see Defining compliance security criteria and publishing NAC settings.

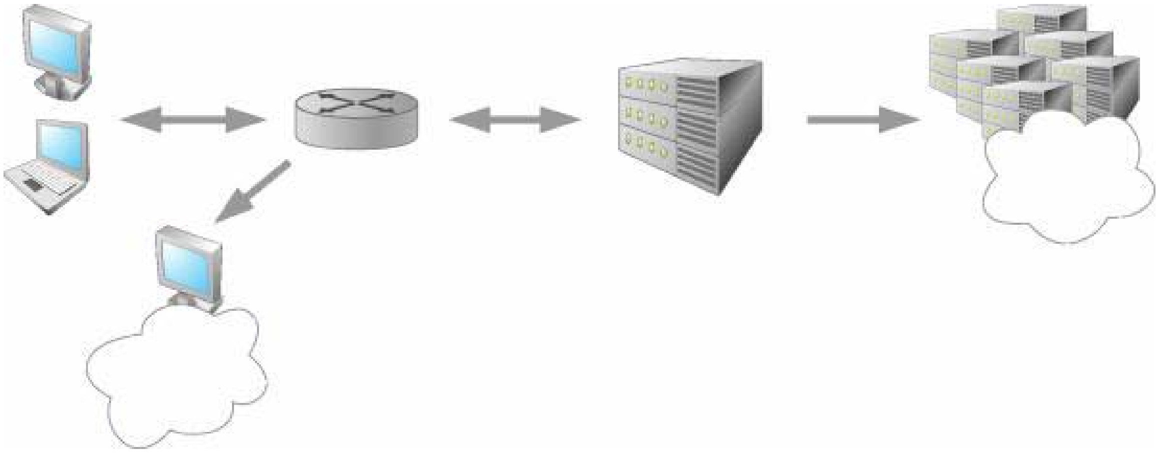
Understanding the basic NAC components

The sections below describe the basic components of a NAC implementation and the function of each component and how they interact.

Basic NAC components descriptions

Component	Description
Devices attempting to access the network	Includes occasionally connecting or mobile laptops, visiting contractors and guest users, as well as regular network users that attempt to access the corporate network. Devices with a trust agent installed can communicate with the policy server or posture validation server in order to send and receive health credential information, and can be repaired by the remediation server if vulnerabilities are detected during the security scan. Without a trust agent, a device can't communicate with the posture validation server and can't be remediated. When a device without a trust agent is scanned for the first time, the device is directed to a Web page with links to install the appropriate trust agent. For more information, see Using the HTML template pages.
Network access control device	The network access control device functions as the "first hop" network device from the supplicant/requesting device perspective and begins the posture validation and authentication process.
Policy server / posture validation server (network access decision point)	A dedicated back-end server also known as the posture validation server that evaluates the posture credentials (state of devices requesting access) based on the compliance rules (security policy published to it from the core server). Sends a validation response (healthy, unhealthy, etc.) via the network access control device.
Corporate network	Critical network area and resources that NAC protects from unhealthy, infected, or otherwise vulnerable devices.
Quarantine VLAN	Virtual safe network area where non-compliant devices can be secured and either remediated, rescanned, and then granted full access to the corporate network, or retained with restricted access to network resources such as the Internet.

Basic NAC components and process flow



Devices attempting network access:	Network access control device:	Network access decision point / policy server:	Corporate network:
(Managed and unmanaged network user devices and/or visitor devices)	(Network router or switch)	(Posture validation service, that evaluates and enforces compliance security policies)	(Network access granted to compliant, healthy devices)

Quarantine VLAN:
(Virtual safe network area to secure and/or remediate non-compliant, unhealthy devices)

Security Suite prerequisites

In order to use the NAC feature, you must have a valid Security Suite license (core server activation).

NAC requires not only the scanning and remediation capabilities of the Patch and Compliance tool, but Security Suite content subscriptions in order to download the vulnerability, system configuration threat, and spyware definitions, and virus pattern files, that are used to create custom compliance security policies.

A group named Compliance has been added to the Patch and Compliance tool's tree view. Users with the Patch and Compliance right can add and remove security type definitions into and from the Compliance group. Security definitions contained in the Compliance group comprise the compliance security policy, and are scanned for on connecting devices in order to determine their health status.

For more information on Security Suite content subscriptions, see Security content types and subscriptions.

Supported device platforms for compliance scanning

NAC services works on the Management Suite supported device platforms, including the following operating systems:

- Windows NT (4.0 SP6a and higher)
- Windows 2000 SP4
- Windows 2003
- Windows XP SP1
- Windows Vista
- Macintosh (10.2 and higher)

Role-based administration with LANDesk 802.1X NAC

Network Access Control relies on the following role-based rights.

Patch and Compliance right

This right is required to see and access the Patch and Compliance tool, and download security content updates need to define compliance rules. This right is required to add or remove security definitions from the Compliance group.

Administrator right

This right is required to configure devices with trust agents for compliance scanning, and to configure NAC services in the console.

The LANDesk Administrator right implies all other rights, including the two security-related rights mentioned above.

Implementing LANDesk 802.1X NAC support

LANDesk 802.1X NAC enhances network access control by requiring the proper authentication credentials as well as an active standard agent on the device. You can also validate device health compliance with your custom security policy, and quarantine and remediate unhealthy devices.

LANDesk 802.1X NAC works with all major switching vendors supporting the 802.1X standard. A 802.1X Radius proxy can participate with an existing AAA (authentication, authorization, and accounting) identity-management architecture authenticating users and endpoints, or act as an independent Radius for environments only requiring endpoint compliance validation. Radius Proxy provisions switch port access dependant upon authentication results for connected endpoints.

To learn how to set up, configure, and use LANDesk 802.1X NAC support, see Using LANDesk 802.1X NAC.

Using LANDesk 802.1X NAC

This section describes how to plan, set up, configure, and enable LANDesk 802.1X NAC support in an existing NAC environment.

The LANDesk 802.1X NAC tool is designed to support and extend the security of an existing 802.1X Radius server implementation on your network. LANDesk 802.1X NAC support adds authentication and compliance capabilities to basic 802.1X access control functionality.

IMPORTANT: Technical knowledge and expertise required for setting up NAC
Note that NAC requires additional hardware and software configuration beyond the basic core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with 802.1X Radius server configuration, 802.1X authentication and health posture validation, as well as advanced networking infrastructure design principles and administration.

Read this section to learn about:

- Using the quickstart task list
- LANDesk 802.1X NAC overview
    - Understanding the 802.1X NAC components and process
    - Network topology and design considerations
- Setting up a remediation server
- Setting up a 802.1X Radius server or proxy
    - Using the IAS Radius server plug-in (for MD5)
    - Using the Radius proxy (for PEAP)
- Deploying the LANDesk 802.1X NAC agent to managed devices
- Configuring a switch and router for LANDesk 802.1X NAC support
- What happens on a managed device configured with LANDesk 802.1X NAC
- Troubleshooting LANDesk 802.1X NAC

What you should do after setting up LANDesk 802.1X NAC

After you've completed the setup tasks listed above, the next step in implementing NAC is to: define your compliance security policy, publish NAC settings to the appropriate servers, and customize the HTML remediation pages as desired. For information on performing these tasks, see Defining compliance security criteria and publishing NAC settings.

Additionally, to learn more about other ongoing NAC management tasks such as: ensuring 802.1X NAC services is enabled, using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing NAC settings, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, and configuring logging, see Managing 802.1X NAC compliance security.

Using the quickstart task list

For your convenience, use this task checklist to help keep track of the steps required to set up LANDesk 802.1X NAC. See the Quickstart task list for LANDesk 802.1X NAC.

LANDesk 802.1X NAC overview

802.1X is a IEEE security protocol used for port-based network access control. 802.1X provides authentication to devices by either establishing a connection or preventing access if authentication fails. 802.1X is based on EAP (Extensible Authentication Protocol), and most recently PEAP (Protected Extensible Authentication Protocol). 802.1X is supported by most network switches, and can be configured to authenticate clients that have agent software installed.

802.1X NAC is a Radius proxy authentication and network access technology that works with all major switching vendors supporting the 802.1X standard. With 802.1X NAC, a Radius server (either a Microsoft IAS server with the EAP IAS plug-in, or a Radius server with the 802.1X proxy) performs posture validation, or in other words checks for security policy compliance.

Standard 802.1X authentication requires a username and password in order to access the network. LANDesk 802.1X NAC extends this basic model by also requiring the standard LANDesk agent (CBA) is installed on managed devices requesting network access, and the supplicant device is determined to be compliant with your custom security policy. NAC verifies the presence of the agent (CBA) by looking for a unique device ID created by the agent itself. (Note: The EAP will not try to authenticate unless it can find the device ID.)

802.1X NAC with the EAP IAS plug-in uses a proprietary NAC EAP agent that resides on both the IAS Radius server and on managed devices. The LTA EAP agent is installed on your managed devices via an agent configuration.

In addition to the specific 802.1X Radius server component, and required switch and router configuration, you must also set up a remediation server in order to implement Network Access Control.

With 802.1X NAC, the Radius server acts as the network access decision point and works in conjunction with the network switch. The switch acts as the network access control device and forwards device authentication requests to the Radius server which performs the actual authentication. Depending on the results that are returned to the switch from the Radius server, the switch allows or denies device access to the network.

Understanding the 802.1X NAC components and process

This section describes the components that comprise 802.1X NAC. Additionally, this section describes what happens when a device attempts to access or connect to the corporate network when NAC is enabled.

The following components are required for LANDesk 802.1X NAC.

Required components

Component	Description
Core server	Provides the Patch and Compliance tool used to: Download security content (such as OS and application vulnerability definitions, spyware definitions, etc.) Define compliance criteria Configure remediation servers Configure Radius proxy installation (MSI) packages Configure and publish NAC settings (including compliance security policies and remediation resources for scanning and repairing devices)
Radius server plug-in, Or Radius proxy	Acts as the network access decision point. Use the 802.1X IAS server plug-in if you want to utilize an existing IAS server (or configure a new IAS server). Use the Radius proxy method if you have a Radius server other than IAS, or if you want to use PEAP as the specified EAP type.
Remediation server	Contains the necessary setup and support files (security type definitions and required patches, as well as the HTML remediation pages used to scan devices for vulnerabilities) identified by your security policy. Remediates any detected vulnerabilities so that the device can be scanned as healthy or compliant and access the network.
Switch	Acts as the network access control device and forwards device authentication requests to the Radius server which performs the actual authentication.
Router	Acts as a network access device that enforces the compliance security policy. Communicates with both the connecting device attempting access and the 802.1X Radius server to evaluate the posture credentials of the endpoint device. In other words, in a 802.1X NAC environment the router is the policy enforcement point on the network and grants or denies access privileges.
Devices	User devices, attempting to access your corporate network. Typical endpoint devices include desktop computers and laptops but may also be clientless devices such as printers, etc. NAC allows you to evaluate the health status of these connecting devices and restrict network access based on their posture credentials.

The steplist below describes the communication flow between the various components in a 802.1X NAC environment when the device attempting to access the network has the LANDesk 802.1X agent installed.

Process workflow

1. A managed device configured with the LANDesk 802.1X agent makes an initial attempt to access the corporate network.
2. The network switch (configured for 802.1X pass-thru forwarding, and acting as the access control point) sends out an EAP-request identity to the supplicant device.
3. A prompt appears on the device asking for a username and password. The end user must type in valid login credentials, which are forwarded by the switch, along with a token added to the EAP-response packet, to the Radius server (configured with either the LTA EAP plug-in or with the LTA Radius proxy, and acting as the access decision point).
4. If the authentication credentials are recognized and the token indicates the device has the standard agent installed, LANDesk 802.1X NAC then runs a compliance security scan that determines the device posture or health status according to the criteria defined by your custom security policy. This scan is performed by a Compliance scan task using a Compliance settings that has the **Enforce 802.1X scan** option enabled on the **Compliance** page.
5. If the device is considered healthy (or compliant), it is granted access to the corporate network
6. However, if the device is considered unhealthy (or non-compliant) it remains in the quarantine VLAN. A message box displays informing the user how to contact the remediation server in order to perform vulnerability assessment scanning and remediation. The Remediation shortcut is created on the device desktop. The end user can choose whether to remain in the quarantine VLAN or take the steps necessary to demonstrate compliance with the security policy and gain full network access.
7. Remediation is performed by the remediation server by scanning for vulnerabilities and other security risks (the compliance rules mentioned above) and installing any required patches. Once the device is repaired, the network access process is repeated and the healthy device is granted access to the corporate network.

Compliance security scans
With the Patch and Compliance tool you can create and configure a compliance-specific security scan, that checks target devices for compliance with your customized security policy. A compliance scan is based on the contents of the Compliance group and can be run as a scheduled task or as a policy. For information on updating compliance security rules and policies and republishing NAC settings, see Managing 802.1X NAC compliance security.

Network topology and design considerations

You should keep the following issues in mind when implementing LANDesk 802.1X NAC support in an existing 802.1X Radius server environment.

- The **remediation server** and **Radius server** can be installed on the same machine, but if performance or scalability issues arise they should be moved to their own server machines.
- The **network switch** must be configured for 802.1X pass-thru forwarding.
- The **router** needs to be configured with two VLAN subnets: the primary subnet is the corporate/production network; the secondary subnet is the quarantine network (i.e., 802.1X guest VLAN).
- The **quarantine network** of the router should use access control lists (ACL) to restrict device access to only the remediation server.
- The **core server** should not be visible to the quarantine network.

Setting up a remediation server

You need to set up and configure a remediation server only if you've selected to use a DHCP quarantine network instead of the TCP/IP self-assigned IP address method to quarantine unhealthy devices. 802.1X NAC with self-assigned IP addressing uses the built-in NIC TCP/IP functionality.

For more information and step-by-step instructions, see Setting up and configuring a remediation server.

Setting up a 802.1X Radius server or proxy

As stated previously, LANDesk 802.1X NAC enhances an existing 802.1X NAC environment by adding authentication and compliance functionality. LANDesk 802.1X NAC requires an 802.1X Radius server or Radius proxy.

Choose one of the following methods to implement LANDesk 802.1X NAC.

- Using the IAS Radius server plug-in (for MD5)
- Using the Radius proxy (for PEAP)

Note: Use the IAS Radius server plug-in if you specify the EAP type MD5. Use the Radius proxy if you specify the EAP type PEAP. (You can also use the Radius proxy if you have a Radius server other than IAS.)

The sections below provide step-by-step instructions for both configurations.

Switch and router configuration
After you set up the Radius server, you must also configure your network switch and router for LANDesk 802.1X NAC. Because switch and router hardware is unique to each network environment, specific instructions for every type of hardware can't be provided here. When configuring your switch and router for 802.1X NAC, follow the basic guidelines for functionality and topology requirements described in the Understanding the 802.1X NAC components and process and Network topology and design considerations sections above. Also, you can go to the LANDesk Support site for switch and router configuration recommendations and sample configuration files.

Using the IAS Radius server plug-in (for MD5)

Use the 802.1X IAS server plug-in if you want to utilize an existing IAS server (or configure a new IAS server) for 802.1X authentication.

The steps below describe how to install (if necessary) and configure an IAS server with the EAP plug-in. Complete all of the steps before enabling 802.1X NAC in the console.

Step 1: Install the Radius server and LTA EAP type

1. Install IAS (Internet Authentication Server) on the server you want to set up as the remote access Radius server. You can install IAS from the Windows 2003 CD. (**Note:** The Radius protocol is supported with Windows 2000 and Windows 2003 only.) Follow the installation prompts.
2. Install the LTA EAP type on the Radius server. LTA EAP is the proprietary authentication protocol. You install LTA EAP from your core server. Map a drive to the core server, and then run the executable file named **LTAEAP.EXE** found in the: \LDMain\Install\Radius directory.
3. Reboot the server to register the LTA EAP on the server.

Note: You can verify this new EAP type in the Remote Server Properties page. To do this, go to **Administrative Tools | Routing and Remote Access**. Right-click the remote server, click **Properties**, click the **Security** tab, click **Authentication Methods**, and then click **EAP Methods**. The LTA EAP type should appear in the methods list. If LTA EAP isn't in the list, you need to install it from the core server.

Step 2: Configure and start the remote access service on the Radius server

1. Click **Control Panel | Administrative Tools | Routing and Remote Access**.
2. Right-click the server, and then click **Configure and Enable Routing and Remote Access**. The Routing and Remote Access Server Setup Wizard displays.
3. Click **Next**.
4. Select **Custom Configuration**, and then click **Next**.
5. Select **Dial-up Access**, and then click **Next**.
6. Click **Finish**.

7. If prompted, click **Yes** to start the service.

Step 3: Customize the remote access service (set EAP as the preferred authentication method for remote devices)

1. In the Routing and Remote Access tool, right-click the server you just configured, and click **Properties**.
2. On the **General** tab, verify that the **Remote access server** option is checked.
3. On the **Security** tab, check the **Extensible Authentication Protocol (EAP)** checkbox. (You may want to click the **EAP Methods** button to make sure the new LTA EAP method is in the list of methods.)
4. Click **OK** to exit the Authentication Methods dialog.
5. Click **OK** again to exit the Properties dialog.

Creating a remote access policy on the Radius server

You need to configure a remote access policy that uses the EAP method for authentication.

You can do this in either the IAS tool, or in the Routing and Remote Access tool.

Step 1: Create the remote access policy

1. Under the remote server node, right-click **Remote Access Policies**, and then click **New**. The Remote Access Policies wizard displays.
2. Click **Next**.
3. Select **Typical** as the policy type, enter a name for the policy, and then click **Next**. (Note: Enter a descriptive name that easily identifies the policy.)
4. Select **Ethernet** as the access method, and then click **Next**.
5. Select **User** for granting access (not Group), and then click **Next**.
6. Select **LTA EAP** as the authentication method, and then click **Next**.
7. Click **Finish** to create the remote access policy.

Step 2: Configure the remote access policy to support both wired and wireless networks

1. Right-click the new remote access policy you just created, and then click **Properties**.
2. Check the **Grant Remote Access Permission** option to enable wireless support.
3. Click **OK**.

Setting up (adding) network switches as Radius clients

Now you need to add the network switches (as Radius clients) that you want to use with 802.1X authentication.

You perform this task in the IAS tool (**IAS | Radius Clients**).

By adding a switch as a Radius client, the Radius server is able to recognize and process authentication requests through that switch.

Creating a common user on the Radius server

You must now create a new user on the Radius server in order to establish login credentials. This user's user name and password will determine the authentication credentials for managed devices configured with 802.1X NAC that attempt to access the network.

Use the server's Computer Management tool to perform this task.

To create a user on the Radius server

1. At the Radius server, click **Start | Programs | Administrative Tools | Computer Management**.
2. Open **Local Users and Groups**, right-click **Users**, and then click **New User**.
3. Enter a user name.
4. Enter and confirm a password.
5. Configure the password with the following settings:
    - Uncheck the **User must change password** checkbox
    - Check the **User cannot change password** checkbox
    - Check the **Password never expires** checkbox
    - Make sure the **Account is disabled** checkbox is clear
6. Click **Create**.

The user name and password entered here are the login credentials that an end user must provide in order to respond successfully to the authentication identify request during the 802.1X authentication process. Then, the credentials are sent to the Radius server, along with the device EAP data, in order to determine whether the device is granted access to the network.

You can also enable 802.1X NAC in the console. (The other method of implementing 802.1X NAC is to configure and install a Radius proxy. For more information, see Using the Radius proxy (for PEAP).)

Enabling LANDesk 802.1X NAC with the IAS Radius server plug-in

After you've completed all of the setup tasks noted above, you can now enable LANDesk 802.1X NAC.

You do this from the console (**Tools > Security > Network Access Control**).

This essentially turns on 802.1X authentication services on your network. However, you must still configure managed devices with the 802.1X agent before their network access can be managed and enforced through 802.1X authentication. See Deploying the LANDesk 802.1X NAC agent to managed devices.

To enable LANDesk 802.1X NAC with the IAS Radius server plug-in

1. In the **Network Access Control** tool, right-click **802.1X**, and then click **Configure 802.1X > Radius server**.
2. Check the **Enable 802.1X Radius Server** checkbox. This turns on 802.1X authentication on your network (for devices with the 802.1X agent) using the IAS Radius server with the EAP plug-in that you've configured.
3. For the **EAP Type**, select MD5.
4. Select **Use LTA EAP IAS plug-in**.
5. Click **Save**.

The next section describes how to configure LANDesk 802.1X NAC using the Radius proxy method.

Using the Radius proxy (for PEAP)

Use the Radius proxy if you want to utilize the EAP type PEAP. (You can also use the Radius proxy if you have a Radius server other than IAS.)

The 802.1X Radius proxy can be installed on the following types of Radius servers:

- Cisco ACS
- A10 Networks
- CAMS (Comprehensive Access Management System)
- IAS (Internet Authentication Service)

Coexisting with Radius server software
The 802.1X Radius proxy can coexist on servers running Radius server software. If your Radius server is hardware-based, you should install the 802.1X Radius proxy on a separate server.

The Radius proxy communicates between the switch and the device with the 802.1X agent installed. The proxy is in the middle and the device authenticates with the Radius proxy and the proxy passes the ID and password on to the Radius server. If the agent is not installed on the device attempting to make a connection, then the Radius proxy denies access.

Enabling LANDesk 802.1X NAC with the Radius proxy

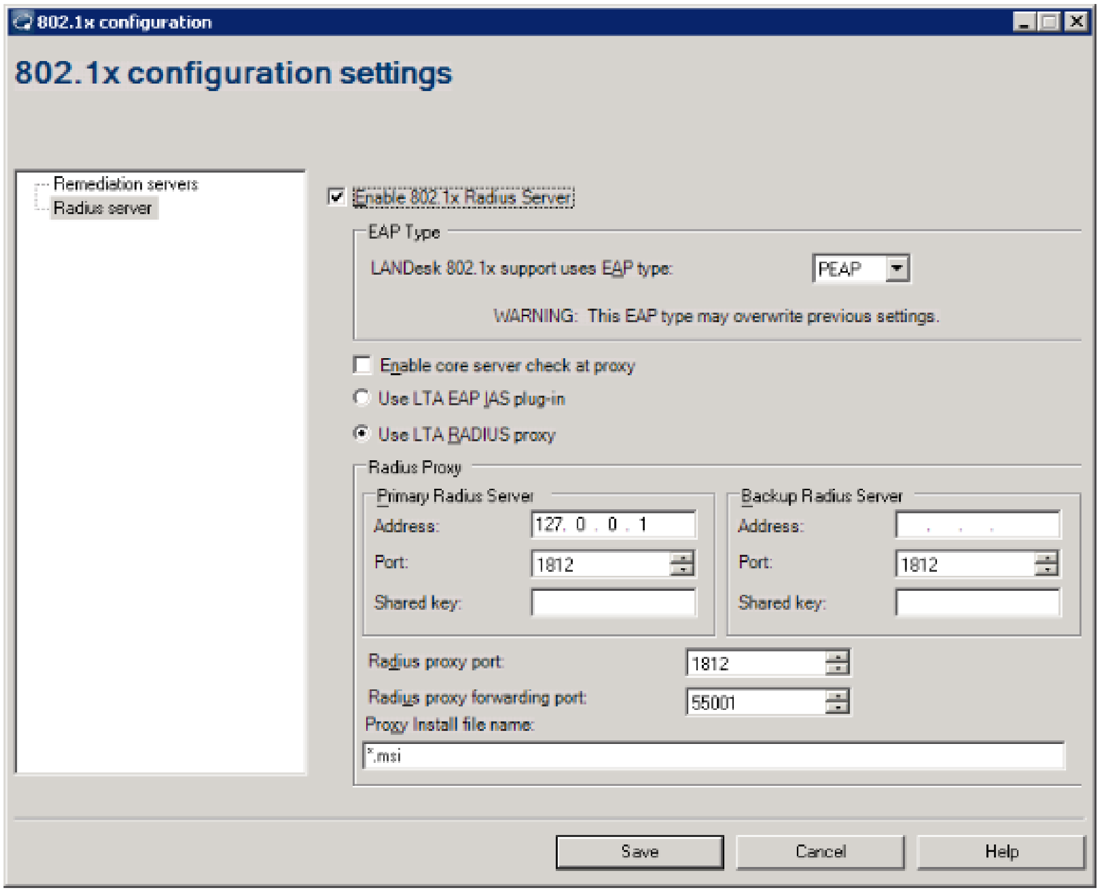
In order to use the Radius proxy, you must enable LANDesk 802.1X NAC, configure the settings for a Radius proxy installation file, and install the Radius proxy on your Radius server.

You do this from the console (**Tools > Security > Network Access Control**).

This essentially turn on 802.1X authentication services on your network. However, you must still configure managed devices with the 802.1X agent before their network access can be managed and enforced through 802.1X authentication. See Deploying the LANDesk 802.1X NAC agent to managed devices.

To enable LANDesk 802.1X NAC, and configure a Radius proxy installation file

1. In the **Network Access Control** tool window, right-click the **802.1X** object, click **Configure 802.1X**, and then click **Radius Server**.



802.1x configuration settings

☑ Enable 802.1x Radius Server

EAP Type

LANDesk 802.1x support uses EAP type: PEAP

WARNING: This EAP type may overwrite previous settings.

□ Enable core server check at proxy

○ Use LTA EAP IAS plug-in

● Use LTA RADIUS proxy

Radius Proxy

Primary Radius Server		Backup Radius Server	
Address:	127. 0 . 0 . 1	Address:	. . .
Port:	1812	Port:	1812
Shared key:		Shared key:	

Radius proxy port: 1812

Radius proxy forwarding port: 55001

Proxy Install file name: *.msi

2. Check the **Enable 802.1X Radius Server** checkbox. This turns on 802.1X authentication on your network (for devices with the 802.1X agent) after you install the Radius proxy that you're configuring here.
3. For the **EAP type**, select PEAP.
4. If you want to verify the core server, check the **Enable core server check at proxy** checkbox.
5. Select **Use LTA Radius proxy**.
6. Enter information for a primary Radius server. (If you want to use a backup Radius server, enter information for a secondary server as well.)
7. Enter a name for the Radius proxy installation file (MSI). The install file is created in the LDMAIN\Install\Radius directory. You can have multiple Radius proxy server installations. (**Note:** The Radius proxy is supported on any Windows 32-bit platform.)
8. Click **Save**.

To install a Radius proxy

1. From the server that you want to configure with the 802.1X Radius proxy, connect to the core server and browse to the folder where you saved the proxy installation file.
2. Double-click the MSI file to execute the installation.
3. Click **Close** when the installation is complete. A system reboot is not required.

The Radius proxy installation adds data (such as address and port information) to the server registry.

Not supported on 64-bit platforms
Do NOT install the Radius proxy on Windows 98, or on any 64-bit platform.

The section below describes the dialogs referenced in the tasks above.

About the 802.1X configuration settings dialog

Use this dialog to select a remediation server and publish network access control settings to the remediation server, and to enable 802.1X NAC on your network.

If you're using the IAS Radius server plug-in, you simply enable the Radius server and specify the EAP type (MD5), and then select the IAS plug-in option.

If you're using the Radius proxy, you must not only enable the Radius server and specify the EAP type (PEAP), but you must also configure a Radius proxy installation file, and then install the Radius proxy to your designated server.

This dialog has two pages:

About the Remediation servers page

- **Add:** Opens a dialog where you can specify the remediation server you want to use to remediate unhealthy devices placed in the quarantine network. Click on a Help button for information about the remediation server. A remediation server contains the necessary setup and support files (security client, security type definitions and required patches), as well as the HTML template pages used to scan devices for vulnerabilities identified by your security policy and remediate (repair any detected vulnerabilities) so that the device can be scanned as healthy or compliant and access the network.
- **Remove:** Deletes the selected remediation server.
- **Modify:** Lets you edit the selected remediation server.
- **Publish:** Opens a dialog where you can publish NAC settings to posture validation and remediation servers.

About the Radius server page

- **Enable 802.1X Radius Server:** Turns on LANDesk 802.1X NAC support (authentication and compliance).

  Note: By default this option is unchecked, which essentially allows network access to every connecting device whether it is healthy or unhealthy. Leave this option unchecked if your want to allow everyone access to the network.

- **EAP Type:** Identifies the EAP type used by 802.1X authentication. Select PEAP for a Radius proxy implementation. Select MD5 for a IAS Radius server plug-in implementation.
- **Use LTA EAP IAS plug-in:** Select this if you want to utilize an existing IAS server.
- **Use LTA Radius proxy:** Select this option if you want to utilize the EAP type PEAP. With this option selected, you can configure a 802.1X Radius proxy installation file.
- **Radius proxy:** Enter information for a primary Radius server. (If you want to use a backup Radius server, enter information for a secondary server as well.)
  - **Radius server address:** Specifies the IP address of your Radius server.
  - **Radius server port:** Specifies the port number of your Radius server. The default port number for Radius authentication is UDP port 1812.
  - **Shared key:** Specifies the shared key (i.e., shared secret) that provides security for communication between the switch and the Radius server. The shared key is a text string. The string you enter here must match the shared key string configured on the switch and on the Radius server.

- **Radius proxy port:** Specifies the port number of your Radius proxy. This port communicates with the switch. Note that this port number must be different than the Radius server port (above) if they're on the same machine.
- **Radius proxy forwarding port:** Specifies the forwarding port number of your Radius proxy. This port forwards data to the Radius server.
- **Proxy install file name:** Identifies the Radius proxy installation file. The installation file is created in the LDMain directory, under Install\Radius\. You can create multiple Radius proxy installation files. A Radius proxy is supported on any Windows 32-bit platform.

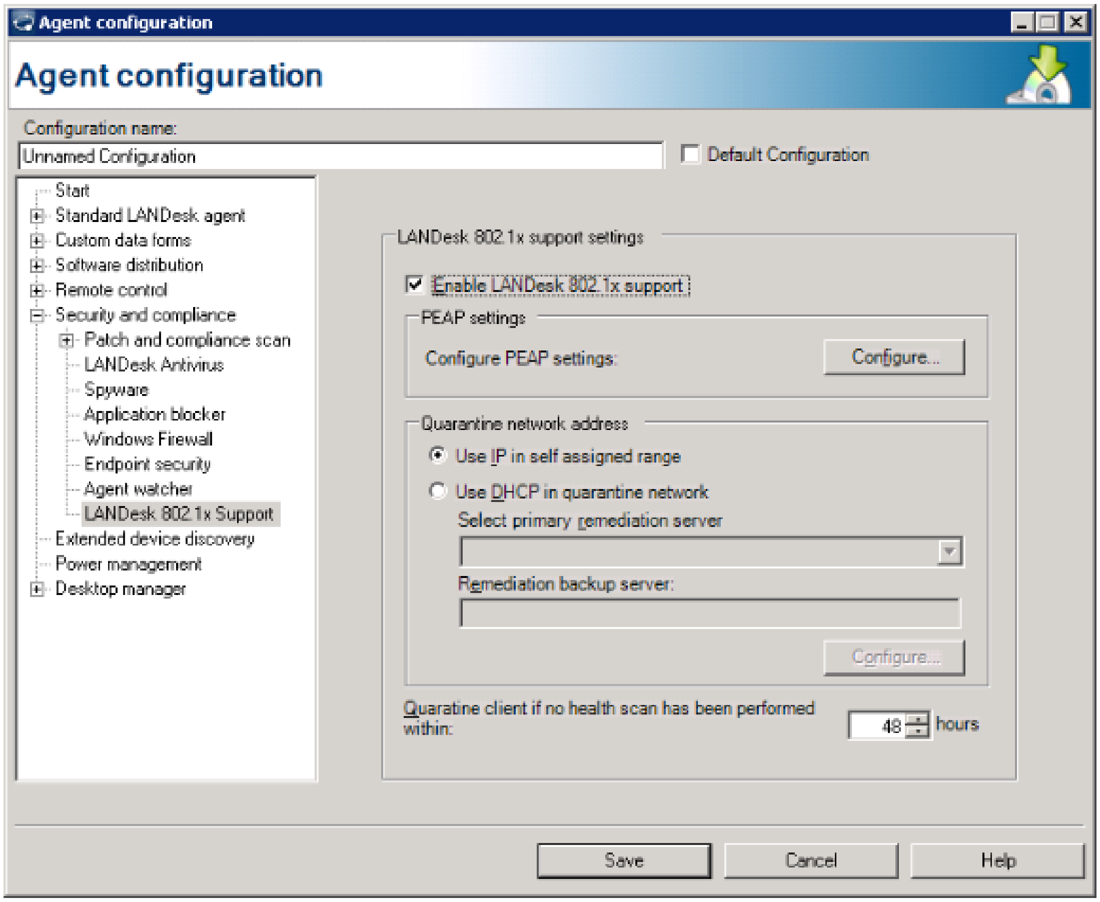
Deploying the LANDesk 802.1X NAC agent to managed devices

As the final step in setting up LANDesk 802.1X NAC support, you must deploy the 802.1X agent to target devices.

This enables compliance scanning and allows the managed devices to be authenticated and either allowed access to the network, or quarantined and remediated.

To deploy the 802.1X agent to managed devices

1. In the **Agent Configuration** tool, click **New Windows Configuration**, open the **Security and Compliance** node, and then click **LANDesk 802.1X support**.



Agent configuration

Configuration name: Unnamed Configuration

☐ Default Configuration

LANDesk 802.1x support settings

☑ Enable LANDesk 802.1x support

PEAP settings

Configure PEAP settings: Configure...

Quarantine network address

● Use IP in self assigned range

○ Use DHCP in quarantine network

Select primary remediation server:

Remediation backup server:

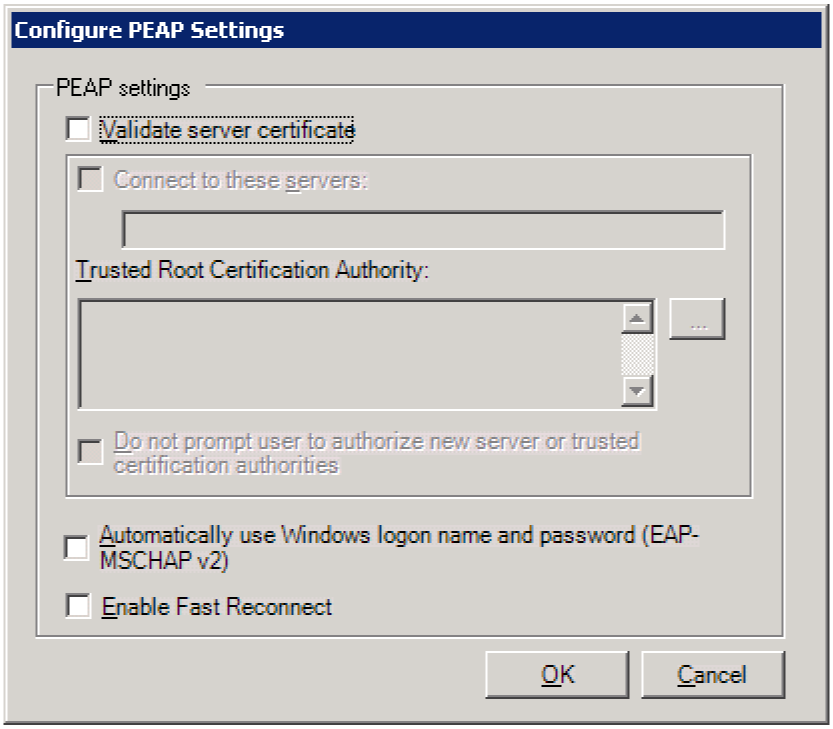
Quaratine client if no health scan has been performed within: 48 hours

2. Check the **Enable LANDesk 802.1X support** checkbox.

   IMPORTANT: This option is unavailable if you haven't already enabled the 802.1X Radius Server in the NAC tool in the console.

   Note: 802.1X NAC uses the EAP type specified in the NAC tool (PEAP or MD5). The EAP type setting is core-wide. In other words, all devices configured with this agent configuration will be configured with the EAP type specified in the console.

3. If you're using the EAP type PEAP, click **Configure**.


Configure PEAP Settings
PEAP settings
□ Validate server certificate
□ Connect to these servers:
Trusted Root Certification Authority:
...
□ Do not prompt user to authorize new server or trusted certification authorities
□ Automatically use Windows logon name and password (EAP-MSCHAP v2)
□ Enable Fast Reconnect
OK
Cancel

4. Specify the following PEAP settings, and then click **OK**.
   - **Validate server certificate:** Indicates the certificate file from the Radius server can be trusted.
   - **Connect to these servers:** Provides another validation check by letting you identify specific servers that can be trusted. Enter server names (fully-qualified DNS names) separated by spaces.
   - **Trusted root certification authority:** Imports the trusted certificate file.
   - **Do not prompt user to authorize new server:** Turns off the authorization prompt on end user devices.
   - **Automatically use Windows logon name and password:** Uses the Windows logon credentials so they don't have to be entered more than once.
   - **Enable Fast Reconnect:** Caches the logon credentials for a quick log in if the device times out.
5. At the Agent Configuration dialog, select the method you want to use to quarantine any devices found to be unhealthy. (Use IP address in self-assigned range, or Use DHCP in quarantine network.)
6. Configure automatic quarantine time by specifying how many hours can transpire since the last health scan has been run on a device before it's considered unhealthy, logged off the corporate network, and placed in the quarantine network.
7. Specify any other device agent configuration settings you want for the target devices being configured.
8. Click **Save**.

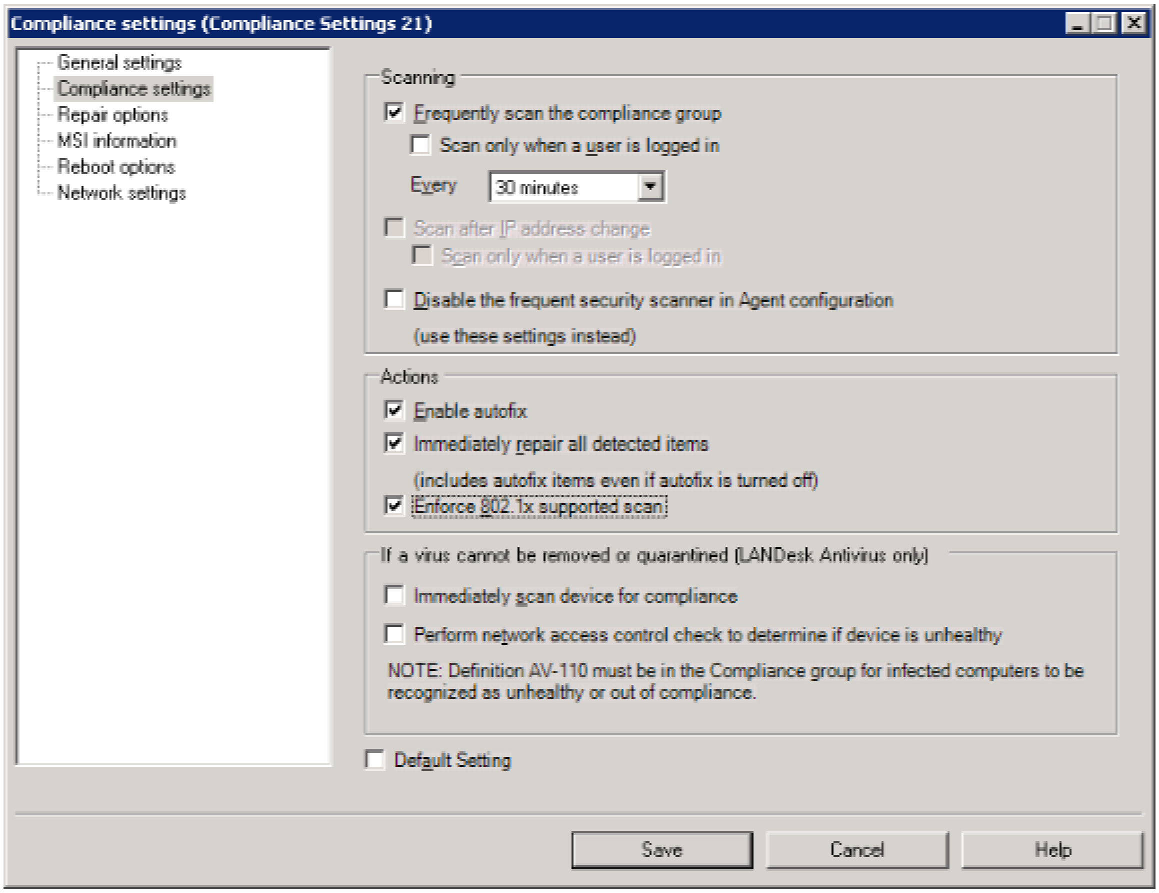
You can now deploy the agent configuration to target devices that you want to use LANDesk 802.1X NAC, and then create compliance scan tasks that scan 802.1X enabled devices for compliance with your security policy.

Creating compliance security scan tasks

Network Access Control runs a compliance security scan that determines the device posture or health status according to the criteria defined by your custom security policy.

Using Compliance settings

The compliance scan is performed by a Compliance scan task using a Compliance settings that has the **Enforce 802.1X supported scan** option enabled on the **Compliance** page.



Scanning

☑ Frequently scan the compliance group

□ Scan only when a user is logged in

Every 30 minutes

□ Scan after IP address change

□ Scan only when a user is logged in

□ Disable the frequent security scanner in Agent configuration (use these settings instead)

Actions

☑ Enable autofix

☑ Immediately repair all detected items (includes autofix items even if autofix is turned off)

☑ Enforce 802.1x supported scan

If a virus cannot be removed or quarantined (LANDesk Antivirus only)

□ Immediately scan device for compliance

□ Perform network access control check to determine if device is unhealthy

NOTE: Definition AV-110 must be in the Compliance group for infected computers to be recognized as unhealthy or out of compliance.

□ Default Setting

Use the Patch and Compliance tool (**Tools > Security > Patch and Compliance**) to create compliance security scans. For step-by-step instructions, see Creating security and compliance scan tasks.

Compliance security scans
With the Patch and Compliance tool you can create and configure a compliance-specific security scan, that checks target devices for compliance with your customized security policy. A compliance scan is based on the contents of the Compliance group and can be run as a scheduled task or as a policy. For information on updating compliance security rules and policies and republishing NAC settings, see Managing 802.1X NAC compliance security.

Configuring a switch and router for LANDesk 802.1X NAC support

LANDesk 802.1X NAC requires a switch and router in order to perform authentication and compliance.

Because switch and router hardware is unique to each network environment, providing specific instructions here for every type of hardware is not practical. However, as a general guideline when configuring your switch and router for LANDesk 802.1X NAC, make sure they meet the functionality and topology requirements described in those sections above. For information, see Understanding the 802.1X NAC components and process and Network topology and design considerations.

Also, you can go to the LANDesk Support site for switch and router configuration recommendations and sample configuration files.

The LANDesk User Community has user forums and best known methods for many LANDesk products and technologies. To access this valuable resource, go to: http://community.landesk.com

What happens on a managed device configured with LANDesk 802.1X NAC

When a managed device configured with LANDesk 802.1X NAC attempts to connect to the network, the following process occurs:

1. A login prompt appears asking for a username and password.
2. The end user must type in the correct authentication credentials.
3. The credentials are sent to the 802.1X Radius server (along with the EAP data) in order to initiate the compliance security scan on the end user device.
4. The compliance security scan determines whether the device is healthy (compliant) or unhealthy (non-compliant) according to your custom security policy.

If the scanned device is healthy it is granted access to the corporate network.

OR

If the scanned device is unhealthy it is placed in the quarantine network where it can be remediated (via the Remediation shortcut on the device desktop) and scanned again in order to gain access to the corporate network.

For a more detailed description of the authentication and compliance process workflow and how the different components interact, see Understanding the 802.1X NAC components and process.

Manually resetting 802.1X authentication at the end user device
If authentication fails even though you're confident the correct login credentials have been entered, you can manually reset the local network card to force another authentication attempt. On the managed device, click **Start | LANDesk | 802.1X reset**.

When you run the 802.1X reset option, make sure you first close any open Windows pop-up dialogs, otherwise the login dialog won't display. If the login dialog goes away too quickly, it is most likely caused by the LINK-3-UPDOWN state timing out, and all you need to do is simply try the 802.1X reset feature again.

Troubleshooting LANDesk 802.1X NAC

This section contains information about some possible problems you might encounter with LANDesk 802.1X NAC, and how to address them.

Scheduled compliance security scan task returns "lost connection" status
If a scheduled 802.1X compliance security scan task returns a status that indicates the target device has "lost connection" or that the "task failed" it might be because the task status was sent to the core server while the machine was being restarted. If you see this status, you can check the target device to verify whether it was quarantined or not.

With a Huawei switch, multiple 802.1X login prompts display

When using a Layer 2 Huawei switch (H3C S3900 Series), if a device displays more than one 802.1X login prompt and the end user cancels or closes one of them without entering the correct credentials, the 802.1X authentication process is canceled. In this case, users must enter the correct credentials in each login prompt. If the authentication is canceled, use the 802.1x reset menu option to restart the authentication process.

With a Windows XP SP2 device, initial authentication fails after remediation

If you remediate an unhealthy end user device that is running Windows XP SP2 and the subsequent authentication attempt fails, you can use the 802.1X reset menu option to restart the authentication process and successfully access the corporate network.

If the Radius server is not available, the device fails to authenticate

In a situation where the 802.1X Radius server is not available to communicate with the LTA EAP agent on an end user device, the device is placed in the quarantine network but it doesn't have the correct configuration, so it can't be remediated and can't authenticate. You must wait until the Radius server is available, and then use the 802.1X reset menu option at the device to restart the authentication process.

802.1X is designed to work on desktop platforms only

802.1X is not supported on server platforms.

Setting up and configuring a remediation server

Network Access Control (NAC) requires a remediation server to repair vulnerable or infected devices. The remediation server is where a device whose posture is determined to be unhealthy is sent to be remediated (repaired) so that it can meet the compliance rules you've configured for a healthy status.

The remediation server is where you publish remediation resources, such as: the security clients that scan for vulnerabilities and other security risks on devices, patch files, and the HTML pages that appear on devices providing options for remediation or limited network access.

Read this section to learn about:

- "Remediation server prerequisites" on page 453
- "Determining server location on the network" on page 453
- "Creating and configuring a Web share on the remediation server" on page 453
- "Configuring (adding) a remediation server in the console" on page 454
- "Next steps: Publishing remediation infrastructure files to remediation servers" on page 456

Remediation server prerequisites

The machine you want to set up as a remediation server must meet the following system requirements:

- The remediation server can be any type of Web server. For example: IIS on Windows, or Apache on Linux.
- You must create a Web share on the remediation server that has anonymous access with read and browse rights enabled. For detailed instructions, see "Creating and configuring a Web share on the remediation server" on page 453.

If you're using an Apache Web server on Linux, the share you create must be a Samba share.

Determining server location on the network

You should comply with the following guidelines when deciding the location of the remediation server on your network.

- The remediation server can be placed on either side of the router.
- If you choose to have it on the client side of the router, then it will be more secure because you don't have to make any exceptions in your router rules, but you will have to manually walk all the remediation files to the machine each time you change them.
- If you put it on the opposite side of the router, then you have a potential security risk since quarantine machines are accessing a machine on your network, but you can push remediation files to the machine without having to walk them there.
- The remediation server must be visible from the remediation VLAN.
- You can have more than one remediation server on your network.

You can see diagrams showing component location and process workflow for LANDesk 802.1X NAC in the overview section.

Creating and configuring a Web share on the remediation server

This procedure has been automated for you with a script located on the core server that you run from the machine you want to set up as a remediation server.

The Web share that is created on the remediation server acts as a storage area for the patch executable files that are used to remediate vulnerabilities on affected devices. When you publish Infrastructure files or remediation resources (i.e., security client, patch files, and HTML files from the core server), those files are copied to this Web share.

Note: The name of the Web share must be LDLogon. You can create this share anywhere on the Web server. A typical path would be: C:\Inetpub\wwwroot\LDLogon. However, you can create the share at any path as long as the URL redirect is configured to go to: http://servername/LDLogon.

After running the script to create and configure the Web share, you must then add the remediation server in the console and specify the path to the share (for detailed instructions, see "Configuring (adding) a remediation server in the console" on page 454). This ensures the core server publishes remediation resources to the correct location on the remediation server.

To run the remediation server configuration script

1. From the machine you want to set up as the remediation server, map a drive to your core server's LDMain\Install\TrustedAccess\RemediationServer folder.
2. Double-click the CONFIGURE.REMEDIATION.SERVER.VBS setup script.

The remediation server configuration script automatically configures the server to perform remediation by:

- Creating a Web share named LDLogon (typically) at: c:\inetpub\wwwroot\LDLogon .
- Enabling anonymous access to the LDLogon share with Read, Write, and Browse rights.
- Adding a new MIME type for .lrd files, and setting it to application/octet-stream (application/binary).

Note: You can also use the Microsoft IIS tool to manually configure the LDLogon share's access permissions and MIME types.

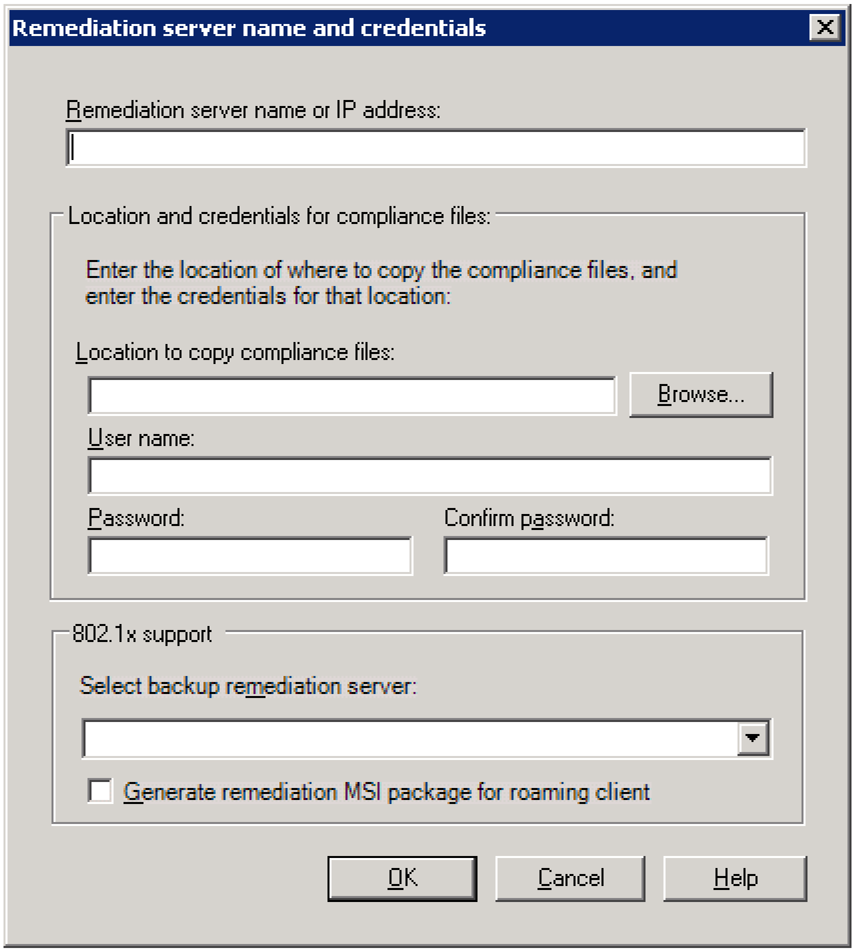
The remediation server is now ready to be added in the console.

Configuring (adding) a remediation server in the console

Once a remediation server is set up, you must configure and add it to the list of valid remediation servers in the **Configure remediation servers** dialog in the console. By doing this, the remediation server is recognized on the network and can communicate properly with the other NAC components.

To configure and add remediation servers in the console

1. In the **Network Access Control** tool window, right-click **802.1X**, and then click **Configure 802.1X**.
2. At the **Remediation servers** page, click **Add**. The **Remediation server name and credentials** dialog displays.


Remediation server name and credentials

Enter the location of where to copy the compliance files, and enter the credentials for that location:

Remediation server name or IP address:
Location and credentials for compliance files:
Location to copy compliance files:
Browse...
User name:
Password:
Confirm password:
802.1x support
Select backup remediation server:
□ Generate remediation MSI package for roaming client
OK
Cancel
Help

3. Enter the server name or IP address of the remediation server.
4. Enter the path to the Web share (on the Web server you're setting up as a remediation server) where you want to publish compliance files. The Web share must be named LDLogon. Compliance files are the security definition files that define your compliance security policy (i.e., the contents of the **Compliance** group in Patch and Compliance, as well as the required patch files that remediate detected vulnerabilities).

   You can enter a UNC path or a mapped drive path. A UNC path is the most reliable method because drive mappings may change (see note below). You can click the Browse button to navigate to the share you want to publish compliance files to on the remediation server.

   Important: If you enter a local path or a mapped drive in the Location to copy compliance files field, the files are published either to the local machine or to the specified mapped drive on the machine where the publish action is initiated. To ensure that compliance files are published to the same location on each remediation server on the network, we recommend using a UNC path to a network share.

5. Enter a valid user name and password to access the remediation server.
6. If you've configured more than one remediation server, you can select a backup remediation server from the drop-down list.
7. If you want to be able to configure a remediation server on another network, for devices that move between trusted networks, generate an installation package (MSI).

8. Click **OK** to add this remediation server to the list.

You can now publish remediation infrastructure files to the server (as long as you've also configured a posture validation server and user credentials).

About the Remediation server name and credentials dialog

Use this dialog to identify the remediation server and the path to Web share on the remediation server where remediation resources (security clients, patch files, and HTML pages are published).

- **Remediation server name or IP address:** Identifies the remediation server by its IP address or hostname.
- **Location to copy compliance files:** Specifies the full path to the Web share located on the remediation server where compliance files are published from the core. The name of the Web share should be LDLogon. The path can be either a UNC path or mapped drive path (or local path). A UNC path is recommended (see the **Important** note above).
- **Browse:** Opens the local Windows Explorer window where you can navigate to the remediation server's LDLogon share.
- **User name:** Identifies a valid user with access credentials to the Web share on the remediation server.
- **Password:** Identifies the user password.
- **Confirm password:** Verifies the user password.
- **OK:** Saves the remediation server settings and adds it to the list in the Configure remediation servers dialog.
- **Select backup remediation server:** If you've configured more than one remediation server, you can select a backup remediation server from the drop-down list.
- **Generate remediation MSI package for roaming client:** Use this option to create an installation package (MSI) that you can use to configure a remediation server on another network, for portable devices that move to other trusted networks.
- **Cancel:** Closes the dialog without saving the settings and without adding it to the list of remediation server.

Next steps: Publishing remediation infrastructure files to remediation servers

The next step in setting up and configuring a remediation server is to publish to the remediation server vital remediation infrastructure resources from the core server. These remediation infrastructure resources include:

- Security client (vulnerability scanner utility)
- Patches associated with the vulnerabilities contained in the Compliance group
- HTML pages that provide links that allow end users to: install trust agents, perform compliance security scanning, and remediate detected vulnerabilities and other security exposures.

You must first define your compliance security criteria in the Patch and Compliance tool before you can publish to servers.

For information about these tasks, see "Defining compliance security criteria and publishing NAC settings" on page 457.

Defining compliance security criteria and publishing NAC settings

After you've set up LANDesk 802.1X NAC support in your environment, you can perform these compliance security management tasks.

Additional servers required for LANDesk 802.1X NAC
For Network Access Control you should have already set up a remediation server and configured (or added) it in the console. For 802.1X NAC, you should also have an 802.1X Radius server. For more information, respectively, see "Setting up and configuring a remediation server" on page 453, and "Setting up a 802.1X Radius server or proxy" on page 441.

Read this section to learn about:

- "Defining compliance security criteria in the Patch and Compliance tool" on page 457
- "Using the Compliance group to define a compliance security policy" on page 458
- "Publishing NAC settings" on page 459
- "Using the remediation pages" on page 461
- "Customizing the remediation pages" on page 462

Other compliance security management tasks

To learn more about compliance scanning and other NAC management tasks such as: updating compliance security rules and policies on posture validation servers, updating remediation resources on remediation servers, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, see "Managing 802.1X NAC compliance security" on page 465.

Defining compliance security criteria in the Patch and Compliance tool

Compliance security criteria is defined by the following factors:

- The security content in the **Compliance group** in the Patch and Compliance tool.

  AND

- The **automatic quarantine time setting** you've specified on the **LANDesk 802.1X support** page in the agent configuration.

See the appropriate steplists below for each of these tasks. See "Using the Compliance group to define a compliance security policy" on page 458, and "Publishing NAC settings" on page 459.

About security content subscriptions

You must have a LANDesk Security Suite content subscription in order to download the various "types" of security content, such as application and operating system vulnerability definitions (and required patches), spyware definitions, blocked application definitions, virus definitions, system configuration security threat definitions, etc.

Without a Security Suite license, you can't access the Security services, and can't define compliance security using those security definitions.

Downloading security type definitions

Use the Patch and Compliance tool to download different security type definitions, such as vulnerability, spyware, antivirus, and security threat definitions. For more information on using the Patch and Compliance download features, see "Downloading security content" on page 315.

Using the Compliance group to define a compliance security policy

As explained above, the contents of the Compliance group determine your baseline compliance security policy. You can have minimal compliance security made up of just a few vulnerability and security threat definitions, or you can create a complex, strict security policy that is comprised of several security definitions. You can also modify the compliance security policy at any time simply by adding and removing definitions from the Compliance group.

Patch and Compliance right required
Only an administrator or a user with the Patch and Compliance right can add or remove definitions to and from the Compliance group.

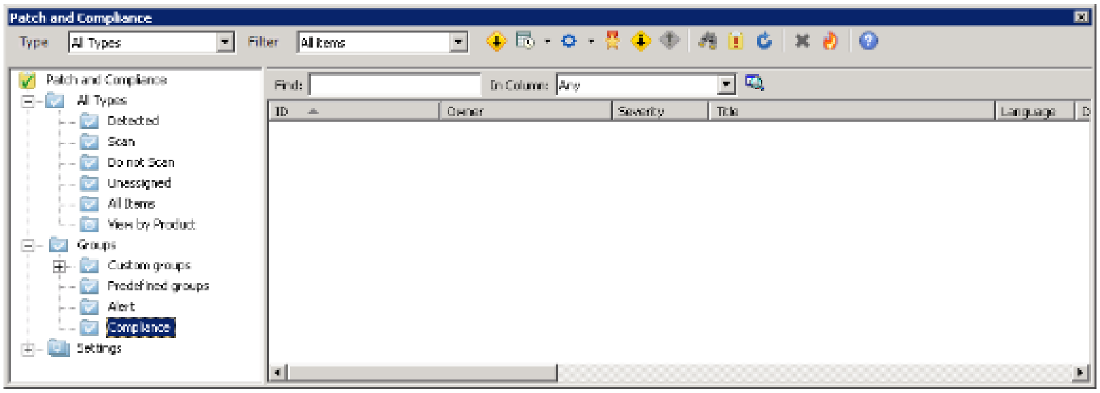
The following security content types can be added to the Compliance group to define a compliance security policy:

- Antivirus definitions
- Custom definitions
- Driver update definitions
- LANDesk software update definitions
- Security threat definitions (includes firewall definitions)
- Software update definitions
- Spyware definitions
- Vulnerabilities (OS and application vulnerability definitions)

Note: You can't add blocked application definitions to the Compliance group to define compliance security policies.

To add security definitions to the Compliance group

1. In the **Patch and Compliance** tool, select the type of security content you want to add to your compliance security policy from the **Type** drop-down list, and then drag and drop definitions from the item list into the **Compliance** group.



2. Or, you can right-click an individual definition or selected group of definitions, and then click **Add to compliance group**.

3. Make sure any necessary associated patches are downloaded before you publish NAC content to posture validation servers and remediation servers. You can right-click a definition, selected group of definitions, or the **Compliance** group itself, and then click **Download associated patches** to download the patches necessary to remediate affected devices.

Publishing NAC settings

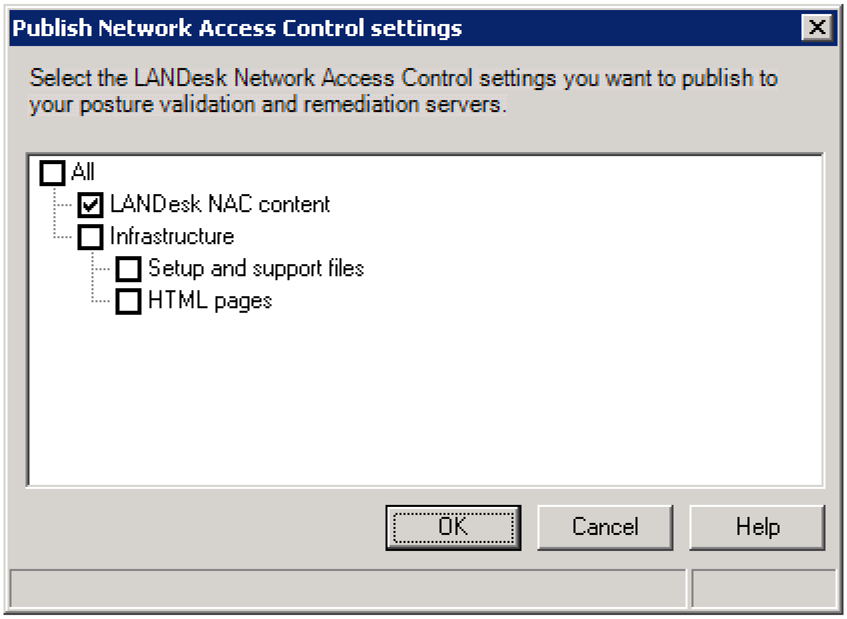
Publishing NAC settings sends information and resources to posture validation servers and remediation servers that is required in order to implement the posture validation process and enforce compliance security.

In order to publish NAC settings from the console, you must have at least one remediation server, and user credentials configured.

The initial publish must include All settings
The first time you publish NAC settings to your posture validation servers and remediation servers, you must include ALL of the NAC settings, including: NAC content and infrastructure files (see below for details about these files). Subsequent publishing can include NAC content or compliance rules only. Typically, the infrastructure files only need to be published once to remediation servers.

To publish NAC settings

1. You can access the **Publish NAC settings** dialog and publish the settings from several locations in the Network Access Control tool. For example, you can right-click the **Network Access Control** object or the **Compliance** group, and then click **Publish**. You can also find the **Publish** button on the **Configure NAC** and **Configure remediation server** dialogs. Additionally, you can click the **Publish NAC settings** toolbar button.


Publish Network Access Control settings

Select the LANDesk Network Access Control settings you want to publish to your posture validation and remediation servers.

- □ All
  - ☑ LANDesk NAC content
  - □ Infrastructure
    - □ Setup and support files
    - □ HTML pages

2. To publish all of the NAC settings, including the NAC content and the Infrastructure files to all of your posture validation servers and remediation servers at once, select the **All** checkbox and click **OK**.
3. If you want to publish only the NAC content (security definitions, NAC settings or compliance rules, and associated patches) to posture validation servers and remediation servers, check the **NAC content** checkbox, and then click **OK**.

4. If you want to publish only the Infrastructure files (security client scanner, trust agent installs, and HTML pages to remediation servers), check the **Infrastructure** checkbox, and then click **OK**. (Typically, you have to publish the Infrastructure files only one time to remediation servers.)

About the Publish NAC settings dialog

Use this dialog to publish NAC settings to posture validation servers, and to publish remediation settings (resources) to remediation servers on your network.

- **All:** Published both NAC content and Infrastructure files to the appropriate servers.
- **NAC content:** Publishes the NAC content and settings you've defined in the Patch and Compliance tool to all of the posture validation servers and remediation servers that have been added to your network.
  Important: You must have at least one posture validation server on your network in order to publish NAC content.
  - NAC content represents the vulnerability and other security content type definitions that currently reside in the **Compliance** group in the Patch and Compliance tool, as well as the NAC settings such as healthy and unhealthy posture settings, logging levels, etc. that are defined in the **Configure NAC settings** dialog. Security definitions, healthy and unhealthy posture settings, and logging levels are published to posture validation servers, while associated patch files are published to remediation servers (based on the contents of the Compliance group at the time you publish).
    (**Note:** If you change the contents of the **Compliance** group or change NAC settings on the **Configure NAC** dialog, you must republish this data to your servers.)
- **Infrastructure:** Publishes the following remediation resources to all of the remediation servers that have been added to your network.
  - **Setup and support files:** Setup and support files represent the security client scanner and trust agent installs. The security client scanner performs security scanning and remediation on devices.
  - **HTML pages:** Represents the template HTML pages that are served by the remediation server to devices with trust agents installed that are trying to access your corporate network. These pages tell the end user what to do in order to gain limited access to the network, or to have their computers remediated in order to become compliant with your security policy and gain full access to the corporate network. These HTML pages are templates that you can modify. (**Note:** Typically, the Infrastructure files only need to be published once to remediation servers. Unlike the NAC content (compliance criteria), you don't need to republish these files every time you change the compliance security policy.)

Using the remediation pages

The NAC remediation pages are HTML files that are published to remediation servers with the Publish NAC settings tool in the console. These remediation pages are part of the remediation infrastructure files. Typically, these files only need to be published once to remediation servers.

The HTML files are located in the following folder on the core server:

ManagementSuite\Install\TrustedAccess\RemediationServer

The HTML pages are merely templates, and you should modify them to suit your own compliance security needs and requirements. For information on how to customize the HTML pages, see "Customizing the remediation pages" on page 462.

The sections below describe the purpose of each HTML page.

Healthy status page

This HTML page is used to inform the corporate end user of a connecting device that the device posture has been evaluated and is determined to be healthy, according to the compliance security credentials, and that it has been granted full access to the corporate network.

The name of this HTML page is: Healthy.html

The healthy status page will ONLY be seen when a device transitions from unhealthy to healthy. It will not display each time a device postures as healthy.

The URL to this page on the remediation server should be entered in the **Healthy URL** field when you configure the remediation server.

First time visitor status page

This HTML page is used to inform a visitor to your corporate network that you have implemented compliance or network access control security on your network and that they can choose to either browse the Web (Internet access only) or have their computer scanned for vulnerabilities or other security risks, and remediated if necessary, before being allowed access to the corporate network. Links are provided on this HTML page that allow Internet access only or that allow the visitor to download and install the necessary software for compliance scanning and remediation so that their device can be have full access to the network.

The name of this page is: Visitor.html

This page provides links that lets the user either be granted Internet access only, or lets them download and install the trust agent and necessary software for remediation so that their device can be repaired, rescanned, and allowed full access to the network.

The URL to this page on the remediation server should be entered in the **First time visitor's URL** field when you configure the remediation server.

Unhealthy employee status page

This HTML page is used to inform the end user of the connecting device that their device has been scanned and does not meet one or more of the compliance security credentials, is considered unhealthy, and has been denied access to the network. The network administrator should customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the end user must log into the network again to be allowed access.

The name of this page is: FailedEmployee.html

The URL to this page on the remediation server should be entered in the **Employee's failed to connect URL** field when you configure the remediation server.

Unhealthy visitor status page

This page is used to inform a visitor to your corporate network that their device has been scanned and does not meet one or more of the compliance security credentials, and has been denied access to the network. As with the unhealthy employee status page, network administrators can customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the visitor should click the Security scan for network access icon that now appears on their desktop.

The name of this page is: FailedVisitor.html

The URL to this page on the remediation server should be entered in the **Visitor's failed to connect URL** field when you configure the remediation server.

Customizing the remediation pages

As mentioned previously, the HTML remediation pages are merely templates that you can manually edit and modify to suit your specific compliance security requirements and policies.

You can use your HTML editor of choice to modify the HTML files. You can modify the existing text to provide additional helpful information specific to your corporate network, and add HTML DIV sections for the security definitions that are included in your compliance security policy (i.e., the definitions contained in the **Compliance** group in the Patch and Compliance tool).

Keep in mind that if you change an HTML file on the core server after it has been published to remediation servers, you must republish the files to the remediation servers before they can be presented to connecting devices (select **HTML pages** under the **Infrastructure** group on the **Publish NAC Settings** dialog).

Adding DIV sections to dynamically show security definitions whose remediation failed

It can be especially useful for corporate end users as well as visitors to your network if you customize the "failed" (or unhealthy) pages so that they can see exactly what the security problems are with their computer and what specific steps need to be taken in order to remediate the problem so their device can be rescanned, evaluated as healthy, and allowed full access to the network.

These pages are designed to dynamically display content when a detected vulnerability can't be repaired by the security scanner's remediation tool. In other words, if the end user device is scanned and vulnerabilities or other security exposures are detected (such as system configuration security threats, spyware, etc.), and the repair job fails, the failed (or unhealthy) HTML page can show those specific security definitions identified by their unique ID number along with other additional information that instruct the end user how to remediate the problem AS LONG AS the system administrator has added a DIV section for that security definition (see a DIV section example below). If remediation fails for a security definition, and that definition does not have a corresponding DIV section in the HTML file, no information specific to that definition will display in the end user device's browser.

To customize an HTML page

1. Open the HTML file in your HTML editor.

2. Edit any of the existing boilerplate text in order to provide as much detailed information as you want your end users (corporate employees and visitors) to see when they log into your corporate network.
3. For the failed HTML pages, add new DIV sections in the HTML code (using the example DIV sections as a model) for the security content definitions you've placed in the Compliance group that defines your compliance security policy.
   Adding DIV sections for every security definition is not required, but only those definitions with DIV sections in the HTML file can appear if that security exposure is detected AND wasn't repaired by the security scan. See the sample DIV entry below. You can add steps needed to repair the security problem, links to software download sites, and any other information you think will assist the end user in resolving the issue.
4. Save your changes.
5. Republish modified HTML pages to your remediation servers.

Sample DIV entry in a failed (unhealthy) HTML file

Below is an example of text that would appear in the browser if a device failed the compliance security scan and was determined to be unhealthy. This example is based on the boilerplate text already in the failed HTML files, and describes two security definitions that could not be remediated:

Automatic Windows Update (ST000003):

Step 1: Click on Start
Step 2: Click on Control Panel
Step 3: Open Automatic Updates
Step 4: Click on Automatic
Step 5: Click OK

No Antivirus Software (AV-100): Click here to install the Symantec Anti-Virus Client

And here is the actual HTML code for that example:

```
<div style="display:block;clear:both;">&nbsp;</div>
<div id="ttip">
<p>
<ul>
<li>Step 1: Click on Start</li>
<li>Step 2: Click on Control Panel</li>
<li>Step 3: Open Automatic Updates</li>
<li>Step 4: Click on Automatic</li>
<li>Step 5: Click OK</li>
</ul>
</p>
</div>
<div id="ttip">
<p>
<strong>No Antivirus Software (AV-100):</strong>&nbsp;<a
href="symantec.exe"><strong>Click here</strong></a> to install the Symantec Anti-Virus
Client
</p>
</div>
```

Finding and inserting definition IDs

The security definition is identified by the following code in the HTML file:

<div id="ttip">

Where "ttip" is the actual ID of the security definition. You can find a definition's ID on its properties page in Patch and Compliance. Type the ID exactly as it appears in the definition's properties.

If that particular security definition's remediation fails, the contents of the DIV section will dynamically appear in the end user browser and provide the end user with useful information to remediate the problem (to the extent that you've entered that information).

Managing 802.1X NAC compliance security

Once you've set up LANDesk 802.1X NAC support and defined your compliance security policy, you can use the subsequent ongoing compliance security management tasks described in this section.

Read this section to learn about:

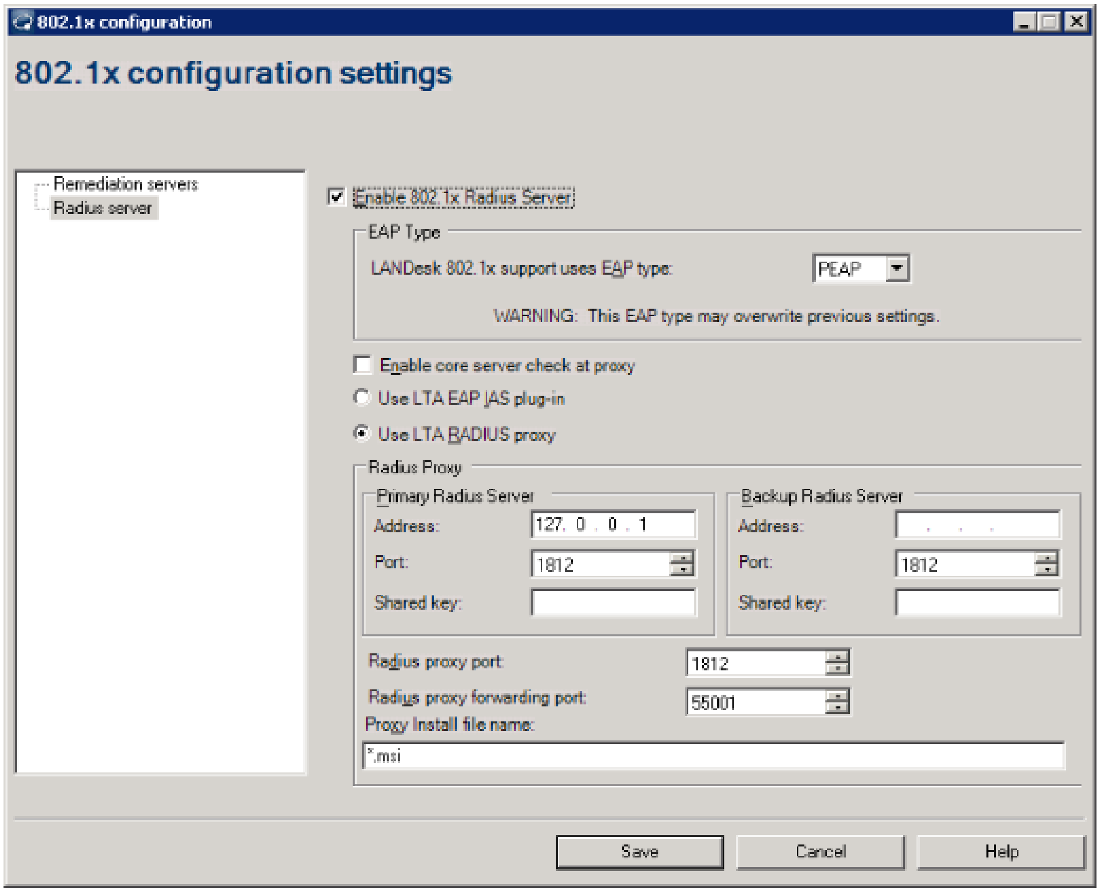
Making sure LANDesk 802.1X NAC support is enabled on your network

LANDesk 802.1X NAC support is enabled when ALL of the following conditions exist:

- A **network control device** is set up and configured properly with the necessary services running. (For 802.1X NAC, this is your network switch and the 802.1X Radius server.)
- The **Patch and Compliance tool** can be accessed in the console by a user with the necessary rights. (You must also have a valid Security Suite content subscription that allows you to download security content.)
- The **Compliance group** contains at least one security content definition. The contents of the Compliance group is the primary factor that defines your compliance security policy, and can include OS and application vulnerabilities, spyware, antivirus, software updates, custom definitions, and system configuration security threats. If the Compliance group is empty, there are no security credentials to check for, posture validation can't take place, and NAC isn't operational.
- At least one **remediation server** is set up and configured properly, with remediation resources published to it from the core server. (Remediation resources include: the security client or vulnerability scanner utility, patches associated with the vulnerabilities contained in the Compliance group, and the HTML pages that provide links to: install trust agents, perform compliance security scanning, and remediate detected vulnerabilities and other exposures.)

  AND

- The **Enable 802.1X Radius server option** on the **802.1X Configuration** dialog must be checked.



☑ Enable 802.1x Radius Server

EAP Type

LANDesk 802.1x support uses EAP type: PEAP

WARNING: This EAP type may overwrite previous settings.

□ Enable core server check at proxy

○ Use LTA EAP IAS plug-in

● Use LTA RADIUS proxy

Radius Proxy

Primary Radius Server
Address: 127 . 0 . 0 . 1
Port: 1812
Shared key:

Backup Radius Server
Address: . . .
Port: 1812
Shared key:

Radius proxy port: 1812

Radius proxy forwarding port: 55001

Proxy Install file name: *.msi

Defining your own desired level of compliance security

If all of the conditions listed above are met, LANDesk 802.1X NAC support IS running on your network.

Note: Remember that the LANDesk 802.1X NAC tool is designed to support and extend the security of an existing 802.1X Radius server implementation on your network. LANDesk 802.1X NAC support adds authentication and compliance capabilities to basic 802.1X access control functionality.

Of course, there is flexibility built in to the service and you can customize how NAC handles devices with options such as the Exclusion List and Allow Everyone On. You can also control the level of security by how many and exactly which security content definitions you place in the Compliance group, as well as the number of hours you specify before a compliance security scan runs automatically on connected devices.

By adjusting these options and policy criteria, you can define very strict, complex security policies or simple, lenient security policies, or any level in between. In other words, you have the ability to customize the degree of difficulty, or ease, with which a connecting device can comply with the security criteria you specify.

Most importantly, you can change the nature of your compliance security policy at any time in order to meet constantly changing circumstances and requirements. Just remember that any time you change your compliance security criteria (for example, the contents of the **Compliance** group in Patch and Compliance, you need to republish NAC settings to your posture validation servers and remediation servers. For information, see "Publishing NAC settings" on page 459.

Modifying and updating compliance security policies

You can modify and update your compliance security policy at any time.

You do this by changing the content of the **Compliance** group in the Patch and Compliance tool.

You then must republish the NAC content to posture validation servers and remediation servers. Remember that publishing NAC content sends NAC settings and compliance rules to posture validation servers AND any associated patches to remediation servers; while publishing Infrastructure files sends setup and support files (including the security client scanner, trust agent installs, and HTML template pages to remediation servers). (**Note:** Typically, the Infrastructure files only need to be published once to remediation servers. Unlike the NAC content, you don't need to republish these files every time you change the compliance security policy.)

For information, see "Defining compliance security criteria in the Patch and Compliance tool" on page 457.

Viewing non-compliant devices

When you want to see which devices have been postured and are found to be unhealthy or non-compliant,

1. In the Patch and Compliance tool, click the **Computers out of compliance** toolbar button.
2. Or, right-click the **Compliance** group, and then click **Affected computers**.
3. A dialog displays that lists non-compliant devices.
4. You can select a device in the list to view the security definitions with which the device is vulnerable or out of compliance.

Quickstart task list for LANDesk 802.1X NAC

Use this task list to complete the planning, setup, and configuration tasks required to implement 802.1X NAC support on your network.

You can print this task list and refer to it to track each step during the implementation process. If you're viewing this task list online, click the **For more information** link to view detailed information for a particular task.

Done	Task	For more information, go to
	Prerequisite: A core server must be installed and running on your network, activated with a Security Suite license and security content subscriptions: • Install the core server • Activate the core with a Security Suite license • Log in as an Administrator user or as a user with the Security right (allows downloading security content and copying it to the Compliance group)	For information on using the Patch and Compliance tool, see Patch and Compliance For information on the 802.1X NAC components and process workflow, see Understanding the 802.1X NAC components and process. For information on network topology and design considerations for a 802.1X NAC implementation, see Network topology and design considerations.
	Set up a remediation server: • On a separate server machine, • Run the CONFIGURE.REMEDIATION.SERVER.VBS setup script located in: <coreserver>\LDMain\Install\TrustedAccess\RemediationServer • **Note:** This script automatically configures the server to perform remediation by: • creating a Web share named LDLogon (typically) at: c:\inetpub\wwwroot\LDLogon • enabling anonymous access to the LDLogon share with Read and Browse rights • adding a new MIME type for .lrd files, and setting it to application/octet-stream	Setting up and configuring a remediation server

Done	Task	For more information, go to
	Configure (add) the remediation server in the console: • In **Network Access Control**, right-click **802.1X**, click **Configure 802.1X**, click **Remediation servers**, and then click **Add** • Enter the remediation server IP address, the UNC path to the LDLogon Web share you've created on the remediation server where files are published, and user access credentials, and then click **OK**	Setting up and configuring a remediation server
	Publish NAC settings to remediation servers: • In **Network Access Control**, right-click **802.1X**, click **Publish NAC settings**, select **All**, and then click **OK** • **Note:** The initial publishing process must include ALL of the NAC settings; subsequent publishing can include compliance content only	Publishing NAC settings
	Define compliance security criteria with the Patch and Compliance tool: • In the console's **Patch and Compliance** tool, • Download security content definitions and patches • Add security definitions to the **Compliance** group in order to define your compliance security policy • Make sure associated patches are downloaded and available for deployment • Create a compliance settings that enforces 802.1X supported scans • (The 802.1X NAC compliance security policy is also defined by the automatic quarantine time setting on the device agent configuration.)	Defining compliance security criteria in the Patch and Compliance tool
	Enable 802.1X NAC support, and configure the 802.1X Radius server or proxy in the console: • In **Network Access Control**, right-click **802.1X**, click **Configure 802.1X**, click **Radius server**, first make sure the **Enable 802.1X Radius server** option is checked, select the EAP type, and then select to use the LTA EAP IAS plug-in or the LTA Radius proxy (requires proxy settings configuration)	Setting up a 802.1X Radius server or proxy
	Install the 802.1X agent on managed devices to enable compliance scanning: (**Note:** When deploying the 802.1X agent, you must specify the quarantine network addressing method for unhealthy devices. Quarantine addressing can be handled by a self-assigned IP address range or by DHCP in the quarantine network. You configure this addressing scheme on the router.) • **For managed employee devices:** If they already have the standard LANDesk agent, enable	Deploying the LANDesk 802.1X NAC agent to managed devices

Done	Task	For more information, go to
	802.1X support with a new device agent configuration Or, if they don't have the standard agent, enable 802.1X support with the initial agent configuration Or, enable 802.1X support with an agent configuration to devices in UDD • **For unmanaged employee devices:** Enable 802.1X support by pulling with the standard agent (wscfg32.exe) Or, by using a self-contained Agent Configuration	
	Configure your network switch for 802.1X authentication, quarantine, and remediation: • Go to the Support site for recommendations and sample configurations	Configuring a switch and router for LANDesk 802.1X NAC support
	Configure your network router to provide security between the production network and the 802.1X quarantine network: • Go to the Support site for recommendations and sample configurations	Configuring a switch and router for LANDesk 802.1X NAC support
	Ensure the authentication and posture validation process is working properly: • Try a simple test of 802.1X NAC by connecting a device configured with LANDesk 802.1X NAC support to the network.	
	Perform ongoing compliance security management tasks: • Making sure 802.1X NAC support is enabled • Understanding what happens when connecting devices are postured • Viewing non-compliant devices • Modifying and updating compliance security policies • Adding unmanaged devices • Configuring and viewing compliance logging	Managing 802.1X NAC compliance security

To return to the main section for LANDesk 802.1X NAC, see Using LANDesk 802.1X NAC.

Agent Watcher

Agent Watcher allows you to proactively monitor the status of selected LANDesk Management Suite agent services and files in order to ensure their integrity and preserve proper functioning on managed devices. Agent Watcher can be enabled and associated settings deployed with an initial device agent configuration. It can also be updated at anytime without having to perform a full agent configuration.

Agent Watcher not only monitors critical services and files, but can also restart terminated services, reset services set to automatic startup, restore files that are pending delete on reboot, and report evidence of file tampering back to the core server.

Read this section to learn about:

Agent Watcher overview

Agent Watcher monitors LANDesk Management Suite agent services and files specified by a device's Agent Watcher settings.

Agent Watcher settings also determines how often to check the status of agent services and files, whether Agent Watcher remains resident on devices, and whether to check for changes to the applied settings itself.

By default, Agent Watcher is turned off. You can enable Agent Watcher with an agent configuration or, at a later time, with a separate Update Agent Watcher settings task. In other words, you don't have to enable Agent Watcher during a device's initial configuration. It can be done at any time directly from the console for one or more managed devices.

When monitoring services and files, Agent Watcher performs the recuperative actions listed below.

Monitoring services

The following agent services can be monitored:

- Local scheduler
- Antivirus
- Remote Control
- Software Monitoring
- Targeted Multicast
- USB Monitor

Services you're not deploying should not be selected for Agent Watcher monitoring
When configuring Agent Watcher settings, don't select services you don't intend to install on target devices. Otherwise, the core server will receive alerts for services not being installed that weren't installed on purpose. However, note that even if a service that isn't installed is selected to be monitored, alerts are not sent saying that the service can't be restarted or that its startup type can't be changed.

When monitoring agent services, Agent Watcher:

- Restarts services when they shut down (one time)
- Changes the service's startup type back to automatic when the startup type is changed
- Sends alerts to the core server when services are not installed
- Sends alerts to the core server when services cannot be restarted
- Sends alerts to the core server when a service's startup type cannot be changed back to automatic

Monitoring files

The following files can be monitored:

- Ldiscn32.exe
- Vulscan.dll
- Vulscan.exe
- Sdclient.exe
- Usbmon.exe
- Usbmon.ini

When monitoring files, Agent Watcher:

- Removes files from the registry that are scheduled for deletion upon reboot
- Sends alerts to the core server when the files are scheduled for deletion upon reboot
- Sends alerts to the core server when the files have been deleted

Supported device platforms and system requirements

Agent Watcher supports most of the same platforms supported by Management Suite. Including the following operating systems, listed with minimum software and hardware requirements:

- **Microsoft Windows XP 64 Bit Professional**
  (Intel Pentium 64 Bit processor or compatible; 128 MB of RAM recommended; 72 MB available on HDD to install)
- **Windows 2000 Professional**
  (SP2 and higher; 133 MHz Intel Pentium processor or compatible; 96 MB of RAM recommended; 50 MB available on HDD to install)
- **Microsoft Windows XP Professional**
  (Microsoft Internet Service Pack 2.0 or higher; 300 MHz Intel Pentium processor or compatible; 128 MB of RAM recommended; 72 MB available on HDD to install)

Enabling and configuring Agent Watcher

The Agent Watcher utility is installed with the standard Management Suite agent, but it is turned off by default.

Agent Watcher can be activated through the initial device agent configuration, or at a later time via an Update Agent Watcher settings task.

Enabling Agent Watcher on devices

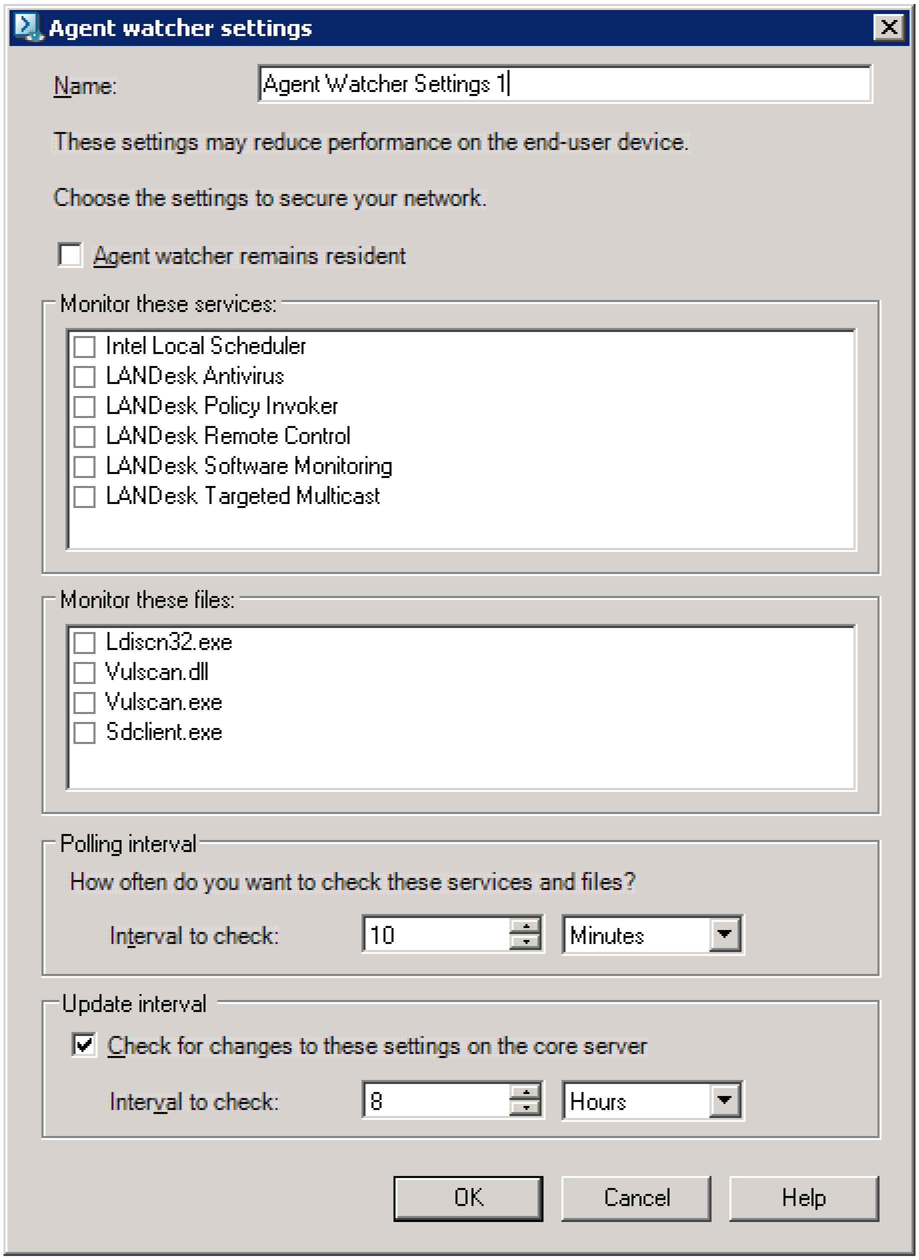
To enable Agent Watcher during agent configuration

1. In the console, click **Tools > Configuration > Agent Configuration**.
2. Click the **New Windows** toolbar button.
3. After specifying your desired settings for the agent configuration, click the **Security and Compliance** group, and then click **Agent Watcher** to open that page on the dialog.
4. Check **Use Agent Watcher**.
5. Select one of the settings from the available list to apply it to the agent configuration you're creating. You can create a new settings or edit an existing settings. The applied settings determines which services and files are monitored and how often, and whether the Agent Watcher executable remains resident in memory on monitored devices.
6. Finish specifying settings for the agent configuration and then click **Save**.

If you want to activate Agent Watcher (or update Agent Watcher settings) at a later time, you can do so for one or more managed devices directly from the console.

Using Agent Watcher settings

Use Agent Watcher settings to determine which services and files are monitored, how often to check the status of services and files, whether Agent Watcher remains resident on devices, and whether to check for changes to the applied settings itself.



Agent watcher settings

Name: Agent Watcher Settings 1

These settings may reduce performance on the end-user device.

Choose the settings to secure your network.

□ Agent watcher remains resident

Monitor these services:

□ Intel Local Scheduler
□ LANDesk Antivirus
□ LANDesk Policy Invoker
□ LANDesk Remote Control
□ LANDesk Software Monitoring
□ LANDesk Targeted Multicast

Monitor these files:

□ Ldiscn32.exe
□ Vulscan.dll
□ Vulscan.exe
□ Sdclient.exe

Polling interval

How often do you want to check these services and files?

Interval to check: 10 Minutes

Update interval

☑ Check for changes to these settings on the core server

Interval to check: 8 Hours

To enable Agent Watcher (or update settings) as a separate task

1. In the console, right-click one or more devices, and then click **Update Agent Watcher settings**.
2. Check **Use Agent Watcher**.
3. Select one of the settings from the available list to apply it to the agent configuration you're creating. You can create a new settings or edit an existing settings. The applied

settings determines which services and files are monitored and how often, and whether the Agent Watcher executable remains resident in memory on monitored devices.

4. Click **OK**.

Once the **OK** button is selected, all the selected target devices are updated with the new settings, and a status message appears.

Disabling Agent Watcher on devices

You can also disable Agent Watcher for one or more devices with the Update Agent Watcher task.

To disable Agent Watcher

1. In the console, right-click one or more devices, and then click **Update Agent Watcher settings**.
2. Make sure the **Use Agent Watcher** checkbox is cleared
3. Click **OK**.

Agent Watcher settings help

This section contains the following online help that describes Agent Watcher dialogs.

About the Configure Agent Watcher settings dialog

Use this dialog to manage your settings. Once configured, you can apply settings to managed devices through an agent configuration or a change settings task.

Agent Watcher allows you to create multiple settings that can be applied to devices or device groups.

This dialog contains the following options:

- **New:** Opens the settings dialog where you can configure the options.
- **Edit:** Opens the settings dialog where you can modify the selected settings.
- **Copy:** Opens a copy of the selected settings as a template, which you can then modify and rename.
- **Delete:** Removes the selected settings from the database.
- **Close:** Closes the dialog, without applying any settings to the task.

About the Agent Watcher settings dialog

Use this dialog to create and edit an Agent Watcher settings.

Agent watcher settings determine which services and files are monitored and how often, as well as whether the utility remains resident on the device.

This dialog contains the following options:

- **Name:** Identifies the settings with a unique name.
- **Agent Watcher remains resident:** Indicates whether the LDRegwatch.exe (Agent Watcher executable) remains resident in memory all of the time. If you don't check this option, LDRegwatch.exe remains in memory only long enough to check the selected services and files at the scheduled time.
- **Monitor these services:** Specifies which critical services will be monitored with this Agent Watcher settings.
- **Monitor these files:** Specifies which critical files will be monitored with this Agent Watcher settings.
- **Polling interval:** Specifies how often you want Agent Watcher to monitor the selected services and files. The minimum settings for this interval is 30 seconds.
- **Check for changes to these settings on the core server:** Automatically compares the current version of the selected Agent watcher settings with the one deployed to target devices (at the interval specified below). If the settings has been modified during that time span, the new settings is deployed and Agent Watcher is restarted with the new settings.
    - **Interval to check:** Specifies the time period of the recurring comparison of Agent Watcher settings.

Services you're not deploying should not be selected for Agent Watcher monitoring
When configuring Agent Watcher settings, don't select services you don't intend to install on target devices. Otherwise, the core server will receive alerts for services not being installed that weren't installed on purpose. However, note that even if a service that isn't installed is selected to be monitored, alerts are not sent saying that the service can't be restarted or that its startup type can't be changed

About the Update Agent Watcher settings dialog

Use this dialog to update Agent Watcher settings on target devices, and to enable or disable the Agent Watcher utility on target devices.

If Agent Watcher is not active on the selected workstations, check the **Use Agent Watcher checkbox**, configure the Agent Watcher settings, and then click **OK**. Agent Watcher will be activated after the configuration is pushed down to the selected devices. To change which files or services are monitored, click the **Configure** button to display the **Agent Watcher Settings** dialog.

With the Update Agent Watcher Settings dialog you can also deactivate the Agent Watcher by unchecking the **Use Agent Watcher** checkbox and clicking **OK**.

This dialog contains the following options:

- **Use Agent watcher: Enables the Agent watcher service on target devices.**
- **Choose an Agent Watcher setting:** Specifies which settings is used for the task. Select one of the settings from the drop-down list, or click **Configure** to create a new settings.

Once the **OK** button is selected, all the selected devices are updated with the new settings, and a status message appears.

Using Agent Watcher reports

Agent Watcher monitoring and alerting information is represented by several reports in the Reports tool.

All the Agent Watcher reports include the hostname of the workstation, the monitored service or file, the status of the alert (either found or resolved), and the date the event was discovered.

Agent Watcher saves the state of the alerts so that the core will only get one alert when the condition is found and one alert when the condition is resolved. Multiple alerts may occur when Agent Watcher is restarted in order to reboot the system, or when a new configuration is pushed or pulled down to the workstation.

Reports can also be generated for a given category based on different time intervals, such as: today, last week, last 30 days, or another specified interval.

Agent Watcher alert data automatically removed after 90 days
All Agent Watcher alerts over 90 days old are automatically removed from the database. Alert data is used to generate Agent Watcher reports.

In order to access the Reports tool, and generate and view reports, a user must have the LANDesk Administrator right (implying full rights) and the specific Reporting roles.

For more information about using the Reports tool, see "Reports" on page 113.

Agent watcher reports

The Agent Watcher reports are listed below:

Failed to change the service type

This report lists all the Agent Watcher alerts from workstations that are unable to change the startup type of a monitored service.

Required services not install

This report lists all the Agent Watcher alerts from workstations where a monitored service has been uninstalled.

Required services not started

This report lists all the Agent Watcher alerts from workstations where a monitored service cannot be restarted by the Agent Watcher.

Files not found on clients

This report lists all the Agent Watcher alerts from workstations were monitored agent files have been deleted.

Pending delete files found on client

This report lists all the Agent Watcher alerts from workstations where the monitored agent files have been scheduled to be deleted upon reboot. Agent Watcher also automatically removes these files from the Windows registry so they will not be deleted.

LaunchPad

LANDesk LaunchPad provides a known location for users to find their physical and virtual applications and URLs. It reduces calls to the help desk that involve application installation or icons missing from the desktop. LaunchPad supplies a list of known applications to a known group of users (or devices). It keeps you from having to go from system-to-system (manually or using remote control) to fix application-specific issues.

LaunchPad keeps users from deleting icons or breaking installed applications. It updates end-user desktops automatically with new applications for designated groups. Users will be able to log into any machine and have their links pulled down into the LaunchPad on that machine.

You can create a distribution package link that seamlessly ties together the installation of an application with its execution (also known as a Just In Time link). A JIT link definition is created in the console by selecting Distribution Package as the link type, and associating a software distribution package with the link.

When a JIT link appears in LaunchPad, and is opened by a user, LANDesk client software will attempt to deploy the associated software distribution package before the target application is executed. Please note that unlike targets of "executable"-type links, targets of JIT links must be themselves executable files; LaunchPad does not resolve file associations for JIT links as it does for ordinary links.

If the package deployment is successful, the target executable will be launched and the link will be marked so that thereafter the deployment will be skipped and the executable will be launched directly.

Because JIT links are designed to hide the installation process from an end user, software deployment packages which will disrupt an end user's normal work flow, such as those requiring a reboot, significant user input, or an unusually long time to install should not be associated with JIT links. These types of software distribution packages should be deployed using either the LANDesk Software Distribution Portal (which allows the user to control the time and manner of deploying the package) or a standard push distribution during off-hours.

Non-JIT LaunchPad links will not be displayed in the LaunchPad window if the target is not found, so you can create an ordinary link to an executable or file which will be installed later, and the link icon will not appear in the LaunchPad window until the target has been created by one of these alternative methods.

To open LaunchPad in Management Suite

1. Click **Tools > Distribution > LaunchPad Link Manager**.

Columns

- **Name:** The name of the link, as defined in **Link Properties**.
- **Description:** The description of the link, as defined in **Link Properties**.
- **Location:** Where the link is located (LaunchPad, desktop, or Start menu).
- **Category:** The classification of the link. Examples include applications, utilities, or web links. You can create categories to best fit your organizational needs. End users will see an interface displaying each category in its own row.
- **Path:** The location of the executable of the link.

Adding links to LaunchPad

Items are added to LaunchPad as links. The links (displayed as icons in LaunchPad) can represent applications, utilities, links to web pages, and so forth. Before the links can display, the following instructions must be completed.

When deploying LaunchPad links to a client computer, the links will not appear on the computer (Desktop, Start menu or LaunchPad window) until the LANDesk software distribution policy synchronization program is executed on the computer. When invoked, the policy synchronization program will contact the LANDesk core, and request and download any updates, including new LaunchPad links.

Normally, the Policy Synchronization program is scheduled to run periodically on the client computers. Administrators may also run policy synchronization at will using the procedures below. Another alternative is to allow users to invoke the policy synchronization program for themselves, using a LaunchPad link, as described in “To set up a policy synchronization program link on client machines” below.

To run policy synchronization (policy.sync.exe) one time on a client machine

1. Execute the following command:

```
"%ProgramFiles%\LANDesk\Shared Files\httpclient.exe"
"http://localhost:9595/policy.cgi.exe?action=start"
```

To force a synchronization on a client from the core

1. Open the Management Suite console on the core.
2. Click **Tools > Distribution > Manage Scripts**.
3. In the left pane, click **All Scripts**.
4. Right-click the "Package Sync" script and click **Schedule**.
5. From the Distribution/Scheduled Task pane, and drag the client you want to synchronize onto the Package Sync task.
6. Right-click the Package Sync task and click **Properties**.
7. Click the Schedule task pane, select **Start now** and **All devices** in the **Schedule these devices** box.
8. Click **Save**. A script will run invoking policy sync on the targeted client. Because you selected all devices, simply click Start now to re-run the script.

Note: Remember that each machine targeted with this script will attempt to contact the core and update its policies. If sent to a large number of machines, this may burden the core server.

To set up a policy synchronization program link on client machines

1. In the LANDesk console, create a LaunchPad executable link labeled “Refresh” that targets “"%ProgramFiles%\LANDesk\Shared Files\httpclient.exe" "http://localhost:9595/policy.cgi.exe?action=start".
2. Right-click the link and click **Schedule**.
3. From the Distribution/Scheduled Task pane, and drag the client(s) you want to deploy to onto the link’s task.
4. Right-click the task and click **Properties**.
5. Click the **Schedule task** pane and click **Start now**. The link will appear on the client machine the next time policy synchronization occurs.

To add links to LaunchPad

1. If LaunchPad is not open, click **Tools > Distribution > LaunchPad Link Manager**.

2. In the LaunchPad toolbar, click **Add new link**.
3. Click the pages in the left pane, and fill out the fields in the right pane. See the additional information below for the fields in these pages. When finished, click **Save**.

Link Info page

Provide basic information for the link, like its type, location to install it to, and so forth.

- **Name:** Type the name of the link. End users see this name under the icon on the client.
- **Description:** Type details of the link. Possible additional information may be service pack numbers or date of an application build or URL.
- **Type:** Select a type of link. There are four types to choose from: executable (including virtual applications), Distribution package, URL link, or Process Manager link.
    - **Executable:** An application, batch file, or script (executable files already installed on the client). You set specific parameters in the Target page.
    - **Distribution package:** A software distribution package. You set specific parameters in the Distribution Package page.
    - **URL link:** A link to a web page on the Internet.
    - **Process Manager link:** A link to a Process Manager process that displays on the LaunchPad window. A process can be something like ordering a new computer.
- **Deploy package when user clicks link in local device's LaunchPad:** Deploys the package automatically when the user clicks the link without user intervention. When the installation is complete, the application will run.
- **Deploy package when link appears in local device's LaunchPad:** Deploys the package automatically when the link appears in the user's LaunchPad on the client.
- **Install link to LaunchPad:** Install the link to the LaunchPad application on the client machine.
    - **Category:** Select a category, or create a category by clicking **Edit**. Categories are the tabs or lines organizing the LaunchPad. For example, Applications, Web Links, or Utilities could be categories.
    - **Edit:** Type the name of the category in the Item box, click **Add**, and click **OK**. The Category will be displayed as a tab or a line in the client-side LaunchPad.
- **Desktop:** Installs the link to the end-user's desktop.
- **Start menu:** Installs the link to the end user's Start menu.
    - **Folder:** Select the folder you want to install the link to on the Start menu. To create a folder, click **Edit**. Folders are stored in Documents and Settings > All Users > Application Data > LANDesk > ManagementSuite > LaunchPad. Any folder created below the LaunchPad folder will not be displayed; folders must be created at root of the LaunchPad folder to be displayed.
    - **Edit:** Type the folder name in the Item box and click **Add**. Click **OK**. The folder will be displayed in the Start menu.

Target page

Select the application the link will run, any command-line arguments, including current working directory

- **Target:** Type the location of the application after it is installed. To run batch files, the command is "cmd.exe /c <"path of batch file to execute">.
- **Command-line arguments:** Type any command-line arguments associated with the application.
- **Start in:** The current working directory

Icon page

Use this page to customize the icon in LaunchPad that represents the link.

- **Use target default:** Select to use the icon associated with the application.
- **Custom (.ico file only):** Select to use a different icon. Custom icons must be accessible over the network.

Distribution package page

- **Type:** Select the type of package you want to use for this scheduled task. The Available distribution packages list will display only the packages of the type you specify.
- **Available distribution packages:** Lists the packages you have created using the Distribution package window in Management Suite.
- **Set:** Makes the package selected from the Available distribution packages list the Current package.
- **Order:** The package selected to be installed.

LANDesk Process Manager

LANDesk Process Manager creates a shortcut to start and schedule a process.

- **Web service address:** The web service URL of the installed core. The Process Manager web service receives the information from the client and initiates an Process Manager workflow. This may culminate in one or more calls into the MBSDK including calls to LaunchPad-specific API's.
- **Process workflow to start:** The identifier of the workflow.

  Examples of possible macros

  - %client - expanded on the client
  - %user - expanded on the client
  - %deviceid - expanded on the client
- **Process context:** LPM context (xml file that can and probably will have macros requiring expansion in it)

To set up Process Manager

1. On the Link Management toolbar, click **Setup Process Manager > Configure Process Manager**.
2. Specify the database username and password.
3. Specify the database server and the database name.
4. Click **Test connection**. Check the results to verify you were successfully connected to the server.
5. Click **Configure and restart services**.

Process management relies on the exchange of data between the server and the database. The Database utility enables you to connect the server to the intended database by providing the proper authentication information, configuring the settings, testing the connection, and restarting the services. By using the Database utility to establish the connection to the database, you are provided with status information, such as verification that the server is in fact connected to the database, validation of the user credentials, the server and database name, version, and so on.

Simply by connecting to a database it becomes the active database. If you want to connect your server to a different database, you follow the same process of connecting to that database. Once you have authenticated to the database, tested the connection, and restarted the services, it becomes the active database that the Process Manager server interfaces with.

Note: Process Manager currently requires Microsoft SQL as the native database. However, you can use any ODBC-compliant database with your workflows and database listeners.

Scheduling tasks

Use the Scheduled tasks window to configure and schedule tasks for LaunchPad. The Scheduled tasks window is divided into two halves. The left half shows task tree and tasks, and the right half shows information specific to what you've selected in the tree.

To schedule a task

1. Select the link you want to schedule.
2. In the Link management toolbar, click **Schedule**.
3. Select the link and click **Properties**.
4. On the Schedule task page, set the task start time and click **Save**. Click Help on the individual Schedule task pages for more information.

LANDesk Power Management Overview

The LANDesk Power Management tool allows you to monitor power usage on your managed computers from a central location. You can easily create and deploy power management policies and generate reports to evaluate financial and power savings. You control the conditions under which computers and monitors stand by, hibernate, or power down.

Power Management includes a feature that lets users avoid specific power management actions (such as a hard shut down) using a client-side user interface. The avoided action will take place the next time the policy runs or is updated on that computer.

The Power Management tool is divided into two panes. The left pane displays power management policies in a tree view. The right pane displays the content and parameters of a power management policy that is selected in the left pane.

Power Management Tool Buttons

The Power Management tool includes a set of tool buttons that allow you to complete various power management tasks.

- **New** (⊕) — Click to create a new power management policy, or right-click **Power management > Power policies** in the left pane and select **Add**.
- **Delete** (✖) — Deletes the power management policy selected in the left pane of the Power Management tool. You can also right-click a power management policy name and select **Delete**.
- **Refresh** (↻) — Refreshes the items displayed in the left pane.
- **Properties** (✎) — Displays the properties of the selected power management policy. You can also right-click a power management policy name and select **Properties**.
- **Schedule** () — Click to schedule the deployment of the selected power management policy. You can also right-click a power management policy and select **Schedule**.
- **Reporting** () — Click to run a report that estimates the power and cost savings you can get by deploying the selected power management policy to a specified group of devices, or to run a report that shows the power and cost savings across a specified time interval. You can also right-click a power management policy and select **View Report**.
- **Historical data** () — Click to run reports on client usage information. You can also right-click a power management policy and select **View report**.
- **Customize** (⚡) — Lets you customize the settings that define overall power usage for specific manufacturers and computer models.
- Application management () — Lets you manage the running of processes as they relate to power policies.
- **Help** (?) — Displays this help file.

Creating a New Power Management Policy

Power Management uses policy-based management to send stand by, hibernate, shut down, and turn on instructions to your managed computers. Create power management policies to control specific computers and groups of computers.

The **New policy** dialog lets you enter a name and a description for a new power management policy. Click **OK** to accept the name and description.

After you click **OK** to close the **New policy** dialog, options and parameters for adding power schemes to the new policy are displayed in the right pane of the Power Management tool. These options and parameters include:

- **Action** — Select the action to take on the managed computer (hibernate*, standby, turn on**, turn off).
- **Device** — Select the device on which to perform the action (for example, computer).
- **Inactivity trigger** — Select the time interval that needs to pass before the action is triggered (1 minute to 5 hours, or never). Note: If you select **Turn off** from the **Action** drop-down list, the title of this drop-down changes from **Inactivity trigger** to **Shutdown type** (hard or soft).
- **Source** — Select the power source the device is using (plugged in, battery, either).
- **Day** — Select the day or days of the week to perform the action.
- **Time** — Select the time or times of the day to perform the action.
- **Add power scheme** — Click to add the selected options and parameters to the current power management policy.
- **Save power scheme** — Click to save the current power scheme after you have edited the options to suit your needs.
- **Save** — Click to save the currently selected power management policy.
- **Delete** — Removes the power policy from the **Power policies** tree in the left pane. (To remove a power scheme from a policy without deleting the policy itself, click the **Delete** button (✖) next to scheme you want to remove.)

Power Management Policy options

Process-sensitive trigger

Use this dialog to delay the power policy if any of the listed processes are detected. Click **Enable process sensitive trigger**. The policy will continue if no policies are detected after the number of minutes specified.

The list of processes is created through the **Process sensitive trigger list** toolbar button. For more information, see Process Sensitive Trigger List below (under Application Management).

Usage monitor

Enforce the power policy if the conditions specified in the dialog are met. Conditions that can be specified are CPU usage and Network traffic. If either or both reach a specified percentage lower than the maximum, the power policy will be enforced. Click **Enable usage monitor**.

End process

End the processes in the list. Click **Enable end process list**.

The list of processes is created through the **End process list** toolbar button. For more information, see End process list below (under Application Management).

*Using Hibernate on Windows 2000 and Windows XP SP2

Power Management cannot automatically enable the Hibernate function on Windows 2000 and Windows XP SP2 computers. Users on your managed computers must manually enable the Hibernate function through the Control Panel.

1. In the Control Panel, double-click **Power Options**.
2. In the **Power Options Properties** dialog, click the **Hibernate** tab.
3. Mark the **Enable hibernation** check box and click **OK**.

**Using the Turn On Action (Wake on LAN)

Power Management uses Wake on LAN (WOL) technology to remotely power on a computer to run scheduled tasks. For Power Management to use WOL functionality, your managed computers must have properly configured network adaptors that support WOL.

Power Management cannot set up or configure a network adaptor's WOL functionality for you. If the WOL functionality on a computer's network adaptor is not enabled, a power management policy that includes a "turn on" action in its power scheme will fail on that computer. Power Management currently does not include any way to monitor whether a network adaptor's WOL functionality is enabled.

Viewing Reports

The Power Management tool allows you to generate and view power, cost savings, and historical reports.

Note: Reports require that a group with at least one device or a query is created first, otherwise the report cannot be run.

- **Policy properties** — Displays the name and description of the currently selected power management policy. This field displays information only and cannot be edited.
- **Select targets** — Click the browse button to the right of this field to select the group(s) that contains the devices on which you want to run the savings report. After you select the group, the total number of machines in the group is displayed below this field.
- **Select the estimated graph type** — You can run a report that estimates how much wattage or money you can save with the current policy.
- **Cost per kWh** — Adjust the associated cost per kilowatt hour to determine how the cost would affect the selected targets.
- **Select currency symbol** — From the drop-down list, select the currency you want to use.
- **Estimated savings** — Click the timeline you want to display (1 Day, 1 Week, 1 Month, or 1 Year). The graph is displayed in this field.
- **Export** — Click if you want a export the savings report in .htm format.

Historical Data

Use this toolbar button to modify client usage info settings.

Start collecting the client usage info: Click this option to turn on the collection of client usage info. This button opens the **Start collecting client usage information** task in the Scheduled task window, from which you can target specific clients and schedule the task to run. For more information, see Scheduled tasks.

Stop collecting the client usage info: Click this option to turn off the collection of client usage info. This button opens the **Stop collecting client usage information** task in the Scheduled task window, from which you can target specific clients and schedule the task to run. For more information, see Scheduled tasks.

Delete old client usage data: Use this dialog to delete all historical power consumption and usage information prior to a specified date.

Custom Wattage Settings

The Power Management tool includes a utility that lets you customize the wattage settings for similar computers for more accurate power management.

To open the **Custom wattage settings** dialog, click the **Custom wattage settings** button (⚡) in the Power Management tool.

Default Settings

The default settings displayed in the **Custom wattage settings** dialog are based on the type of computer running the Power Management tool.

For example, if you are running a desktop computer, Power Management displays default wattage settings based on the average settings of a typical desktop computer. If Power Management is running on a laptop computer, the default settings are lower because laptops typically use less power.

Custom Settings

You can use pre-configured custom power settings to match the type of equipment you are using. Many power settings for popular desktop and laptop computer manufacturers have been added for your convenience.

For example, if you are monitoring the power usage on a Dell Inspiron 531s desktop computer, select **Dell Inc.** from the **Manufacturer** drop-down list and **Inspiron 531s** from the **Model** drop-down list. The wattage settings for the computer and its monitor have been added based on the data returned from a LANDesk inventory of an Inspiron 531s computer.

Wattage Settings

When the **Default settings** check box is marked, these fields display the average power usage of a typical desktop or laptop computer (depending on the type of computer on which the Power Management tool is running). When the **Default settings** check box is cleared, use these fields to enter power usage settings for specific computer brands and models.

Creating Custom Wattage Settings

If the type of equipment you want to manage does not appear in the pre-configured **System Information** drop-down lists, you can enter the information you need manually.

Generate the XML file for default usage table

The Generate the XML file for default usage table toolbar button opens the Default usage table generator dialog, which allows administrators to select the group or groups of devices from predefined queries and timeframe to generate an XML file. This XML file contains data that populates the Savings report window. If client information is collected, the XML file created at installation is updated with the actual usage information from the client machines. This reflects the power usage in an organization and provides more accurate Savings reports.

All groups that are created from queries are displayed in the left pane and the time frame can be selected from the right pane.

The Default usage table generator window contains the following options:

- **Time:** Select a time frame from the XML file usage table
    - **Latest week:** Select the most recent week of use from client usage info.
    - **Specific Period:** Select a specific time range by selecting the month, day, and year.
- **Generate Default usage table:** Create the XML table.

Application Management

Identify process-sensitive triggers

Use the **Identify process-sensitive triggers** toolbar button to observe the process of any program of importance and wait for it to be completed before enforcing the power policies. In some environments programs need to run for an extended period of time. For example, the Management Suite Patch process can be a short or a long process to install the patches. The time frame needed for the managed device to be powered up is unknown when dealing with patch deployment. Other programs can have similar parameters that need to be uninterrupted in an environment.

The Process sensitive trigger list window contains the following buttons:

- **Add:** Adds a process that is a known .exe that needs to delay power policies.
- **Import:** Adds a process from information gathered from the client machines using collect client usage information.
- **Delete:** Removes the selected process from this list.
- **Modify:** Changes the name of the .exe file.
- **All:** Checks all the process in the list to be added to the default list of processes when creating the power policy.
- **None:** Removes the checks from all the process in the list to be added to the default list of processes when creating the power policy.

Identify processes to terminate at shutdown

Use the **Identify processes to terminate at shutdown** toolbar button to allow the administrators to stop processes. Some processes cause a machine to not follow the configured power policies parameters. This same process affects a few or many machines following the policy. Power management terminates the processes preventing the machine from going into standby or to shut down.

The End process list window contains the following buttons:

- **Add:** Adds a process that is a known .exe that needs to be terminated.
- **Import:** Adds a process from information gathered from the client machines using collect client usage info.
- **Delete:** Removes a process from this list.
- **Modify:** Select this button to change the name of the .exe file.
- **All:** Checks all the process in the list to be added to the default list of processes when creating the power policy.
- **None:** Removes the checks from all the process in the list to be added to the default list of processes when creating the power policy

Identify processes to ignore in exception bugs

Use the **Set the list of processes to ignore** toolbar button to designate processes that do not need attention from the power policy. Processes are added to the Import list from Client usage. This list can be large and hard to sort through. Power management has created a way to organize the list of process for management. The [Import] button is used to select a process as sensitive or to terminate the list.

The Processes to ignore window contains the following buttons:

- **Add:** Adds a process that is a known .exe that is to be ignored.
- **Import:** Adds a process from information gathered from the client machines using collect client usage info.
- **Delete:** Removes a process from this list.
- **Modify:** Select this button to change the name of the .exe file.
- **All:** Checks all the process in the list to be added to the default list of processes when creating the power policy.
- **None:** Removes the checks from all the process in the list to be added to the default list of processes when creating the power policy

Monitoring with alerts

Using alerts

LANDesk Management Suite alerting and monitoring features make your work more efficient by giving you immediate notice of hardware, software, and application events on the devices you manage. When events occur that indicate a need for action or a potential problem, alerts can initiate the process of solving the problem in different ways, such as logging the event, sending an e-mail or pager message, running an application, or powering off the device.

An *alert* is a unique ID that represents an event. You can specify an *alert action* that is performed automatically when the event occurs, such as automated e-mail, applications, or power options. An alert combined with an action is referred to in this product as an *alert rule*. Some alerts can be combined with specific *performance monitoring rules* that specify the condition that triggers an event. For example, you can define a monitoring rule for available free space on disk drives, so that when a drive is 90% full a warning alert is generated.

By defining *alert rulesets* you decide which events require immediate action or need to be logged for your attention. A ruleset contains a collection of alert rules, each of which has a corresponding alert action. When you define an alert ruleset you can deploy it to one or more devices to monitor the items that are important for that kind of device.

This chapter includes information about:

- Understanding alerts, actions, and performance monitoring
- Events that can generate alerts
- Severity levels for events
- Using alert actions to receive notifications
- Process for deploying alert rulesets
- Process for configuring custom alert rulesets
- Alert storm control
- Migrating alerts from previous versions of LANDesk Management Suite

Related topics include:

- Configuring alert rulesets
- Deploying alert rulesets
- Viewing alert rulesets for a device
- Viewing the alert log
- Performance monitoring
- Turning off the ModemView service
- Monitoring the contents of log files

Understanding alerts, actions, and performance monitoring

To generate alerts for a managed device, the alerting agent must be deployed to that device. A default alerting agent is deployed to every managed device when you add the device to your list of managed devices. That agent follows the rules defined in the alert rulesets for that device.

By default every managed device has a standard alert ruleset. When you have defined a custom ruleset you can deploy it to devices to monitor items specific to that type of device. You can deploy multiple rulesets to devices, although you should be aware that conflicts could occur between similar rules in different rulesets.

Note: When you install an additional Win32 console on a device, no agent is installed on that device. Even though you can manage other devices from that console, the console device itself can't generate alerts, either as a core or as a managed device, unless you also install management agents on it.

Some alerting events are based on specific performance monitoring rules. "Performance monitoring" refers to an event based on performance counters that are defined for specific devices. Counters can be defined for hardware components and sensors, operating system performance, application components and usage levels.

To add performance monitoring to the ruleset for a device, you select the "Performance monitoring" alert rule in the ruleset, but the details of what to monitor are defined for each individual device. This is done in the server information console on each device. You can select different hardware and software components and define counters for the items to be polled, then view the monitoring data in real time or historically. For more information, see Performance monitoring.

Events that can generate alerts

This product has an extensive list of events that can generate alerts. Some events are problems that need immediate attention, such as component failure or system shutdown. Other events are configuration changes that provide useful information to a system administrator, such as changes that affect a device's performance and stability or cause problems with a standard installation.

Examples of the types of events you can monitor include the following:

- **Hardware changes:** A component such as a processor, memory, a disk drive, or a network card has been added or removed.
- **Application added or removed:** A user has installed or uninstalled an application on a device. This can be useful in tracking licenses or employee productivity. Applications registered in Windows Add or Remove Programs are monitored, and the application name used in Add or Remove Programs is the name that appears in the alert notification.
- **Service event:** A service has started or stopped on the device.
- **Performance:** A performance threshold has been crossed, such as for drive capacity, available memory, etc.
- **IPMI event:** An event detectable on IPMI devices has occurred, including changes to controllers, sensors, logs, etc.
- **Modem usage:** The system modem has been used, or a modem has been added or removed.
- **Physical security:** Chassis intrusion detection, power cycling, or another physical change has occurred.
- **Package installation**: A package has been installed on the target computer.
- **Remote control activity:** Remote control session activity has occurred, including starting, stopping, or failures.

To view a record of alerts for configuration changes, review the alert log on the device's server information console (see "Viewing the alert log" on page 507).

Alerts can only be generated when devices are equipped with the appropriate hardware. For example, alerts generated from sensor readings only apply to devices equipped with the correct sensors.

Hardware monitoring is also dependent on the correct configuration of the hardware. For example, if a hard drive with S.M.A.R.T. monitoring capabilities is installed on a device but S.M.A.R.T. detection is not enabled in the device's BIOS settings, or if the device's BIOS does not support S.M.A.R.T. drives, alerts will not be generated from S.M.A.R.T. drive monitoring.

Severity levels for events

Device problems or events can be associated with some or all of the severity levels shown below. In some parts of the product interface, these states are noted with a numeric value as well as an associated icon. Numeric values are in parentheses.

- **Informational (1)**: Supports configuration changes or events that manufacturers may include with their systems. This severity level does not affect device health.
- **OK (2)**: Indicates that the status is at an acceptable level.
- **Warning (3)**: Provides some advance warning of a problem before it reaches a critical point.
- **Critical (4)**: Indicates that the problem needs immediate attention.
- **Unknown:** The alert status can't be determined or the monitoring agent has not been installed on the device.

Depending on the nature of the event, some severity levels don't apply and aren't available. For example, with the Intrusion detection event, the device's chassis is either open or closed. If it is open, an alert action can be triggered, but only with a severity of Warning. Other events, such as Disk space and Virtual memory, include three severity levels (OK, Warning, and Critical) because different states can indicate different levels of concern to the administrator.

You can choose the severity level or threshold that will trigger some alerts. For example, you can select one action for a Warning status and a different action for a Critical status for an alert. The Unknown status can't be selected as an alert trigger but simply indicates that the status can't be determined.

Using alert actions to receive notifications

This product can notify you when monitored events occur by doing any of the following:

- Adding information to the log
- E-mailing a notice or sending a message to a pager
- Running a program on the core or an individual device
- Sending an SNMP trap to an SNMP management console on the network
- Rebooting or shutting down a device

For detailed information about configuring alert actions, see "Configuring alert rulesets" on page 495.

Process for deploying alert rulesets

This product includes predefined alert rulesets that can be deployed to managed devices. Note that each managed device must have a management agent installed before you can deploy an alert ruleset to the device and before it can send alerts to the core server.

When the monitoring agent is installed to a managed device, a default ruleset of alerts is included by default to provide health status feedback to the health dashboard and console. This default ruleset includes alerts such as:

- Disk added or removed

- Drive space
- Memory usage
- Temperature, fans, and voltages
- Remote control activities
- Performance monitoring
- IPMI events (on applicable hardware)
- Inventory scanner alerts
- Connection control manager actions
- LANDesk Antivirus status
- Network access control status
- Client database utility
- Security and Patch Manager alerts

You can modify these standard alert rulesets to include the alerts you want to monitor. For detailed information, see "Configuring alert rulesets" on page 495.

The general process for deploying alert rulesets to managed devices is as follows:

1. Create or edit the ruleset
2. Target the devices you want to deploy the ruleset to
3. Schedule a deployment task to the targeted devices
4. If a ruleset includes performance monitor alerts, open the server information console for each device with that ruleset and define the performance monitor counters for the device

For complete instructions on deploying rulesets to devices, see "Deploying alert rulesets" on page 505. For information about defining performance monitor counters on individual devices, see Performance monitoring.

Notes

You can deploy multiple rulesets to a device, and you can select devices in other ways than by targeting them. For more information about scheduling tasks such as deploying an alert ruleset, see Scheduling tasks.

You can remove all rulesets from one or more devices in the same way that you deploy rulesets: target the devices and, in the list of alert rulesets, right-click and select **Remove all rulesets**.

Process for configuring custom alert rulesets

In addition to the default rulesets, you can configure and deploy custom alert rulesets. You can include custom alert actions to respond any combination of events. For example, you may want to define one set of actions for events on managed desktop devices (such as sending an e-mail to the hardware support team) and a different set of actions for managed servers (such as sending a pager message to the admin).

The overall process for creating and deploying an alert ruleset is as follows:

1. Create your custom alert ruleset. This includes selecting alerts to include and associating alert actions with them. (For more information, see "Configuring alert rulesets" on page 495).
2. Select the devices to which you will deploy the ruleset and click **Target** to add them to the **Targeted devices** list.
3. Deploy the ruleset to the targeted devices. (See "Deploying alert rulesets" on page 505 for more information).

The following is a simple example of the first step in this process, in which a single alert rule is added to a ruleset.

Example: Configuring an alert ruleset for disk space problems

1. In the core server console, click **Configuration > Alerting**.
2. On the toolbar, click **New**. Type a name for the ruleset and a description (such as "Disk space 90% full"), and click **OK**.
3. In the **Alert rulesets** list, click the name of the new ruleset and click **Edit** on the toolbar.
4. In the **Ruleset configuration** window, click **Alerts** in the left column.
   A tree view of alerts is displayed, with a grid containing alerts and their descriptions. You can click **All alerts** to view all available alerts, or click a category in the tree to view a specific group of alerts.
5. In the tree view, under the **Monitor** group, click the **Drive space** alert.
6. In the grid, select **Default disk usage**, then click **Edit** in the right column.
7. In the **Drive space monitoring** dialog, you can set the **Polling interval** frequency to change how often the drive space usage will be monitored. To change the thresholds at which alerts are triggered, click **Drive space** and set percentages for warning and critical alerts. (These are percentages of total available drive space that are full.) Click **OK** to save the settings.
8. On the **Alerts** page, in the right column, click **Rules > Add**.
   Three "wells" are displayed at the bottom of the page. Use these wells to combine alert, action, and time items to create an alert rule.
9. Drag the **Default disk usage** alert to the **Alerts** well.
10. In the left column, click **Actions**. Click the **Standard** folder. Drag **Log alert to local NT event log** to the **Actions** well.
    For every alert rule you create, a default **Log handler configuration** action is already included in the **Actions** well. If you want to add other actions, such as sending an e-mail, you need to define an action and then drag it to the Actions well.
11. In the left column, click **Time**. In the Time list, drag **Always** to the **Time** well.
12. Click **OK** next to the wells to save the rule, and click **OK** again at the success message.
    You have now created an alert rule that is part of the ruleset. To save your changes, you need to publish the ruleset.
13. In the right column click the **Publish** button.
    You can go back to the **Rules summary** page to view the rule and, if you want, edit it.
14. In the left column, click **Rules summary**.
    Note that there are two rules listed. One is for the rule you created (with a **Log alert to local NT event log** action), and the other is a default rule that sends the alert notifications to the core server (with a **Log handler configuration action**). This is automatically created for every rule you define so that all alerts are logged at the core server. You can't delete this rule unless you delete all rules for an alert.
15. Select the **Default disk usage** rule with **Log event in alert log** as the action, then in the right column click **Rules > Edit**. Use this dialog to change settings for the rule.
16. To change the action associated with the rule, select a different item from the **Action** drop-down list.
17. To change the time during the which the alert rule is active, select a different item in the **Time** drop-down list.
18. To change the severity levels for alert notifications, click the **State** icons. A dimmed icon will not be used, so to receive alerts only for critical status alerts, click the Warning (State 2) icon, a yellow triangle, to turn it off.
19. Select the **Health** check box to include disk space usage as an alert that contributes to the device's health status.

20. Click **OK**. You can now see the changes you made reflected in the **Rules summary** list. To save the changes to this ruleset, you need to publish it again. It will then be saved and will be available for deployment in your list of rulesets.
21. In the right column, click **Publish**.

When you return to the management console, the new ruleset you created is listed under **Alert rulesets**.

Alert storm control

Some alert rules assigned to groups of devices can simultaneously generate a large number of responses. For example, you can include an alert rule for computer configuration changes and associate it with an e-mail action. If a software distribution patch is applied to many devices with this alert rule, it would generate a number of e-mails from the core server equal to the number of devices to which the patch was applied, potentially flooding your e-mail server with a "storm" of alert notifications.

This product's alert storm control feature automatically limits the number of times an alert action occurs for an alert. If an alert triggers an action 5 times in 5 minutes, the alert action is discontinued but alerts are still written to the core log file. The administrator is notified of the alert storm with an automated e-mail. When the alert stops occurring and does not occur again for one hour, the alert storm control is reset for that alert. Alert actions will again be triggered if that alert occurs again later.

Migrating alerts from previous versions of LANDesk Management Suite

Previous versions of LANDesk Management Suite included alerting functionality with the Alert Management System (AMS) feature. Beginning with version 8.8, alerting is based on a new set of alert handlers, even though some alerts are based on AMS alerts. Your alert rulesets for managed devices will need to be created using the new alerting feature.

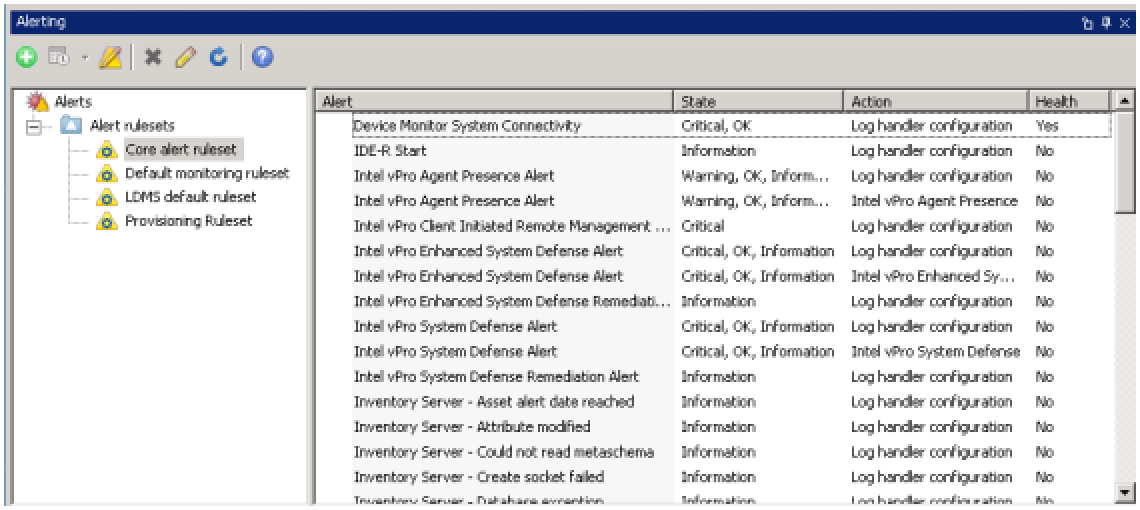
To help you migrate alerts from previous versions, this product includes a utility that extracts information about your AMS alerts and writes the data to a text file, which you can refer to as you create new rulesets. To use this utility:

1. In the \utilities directory of the LDMAIN share, run alertexp.exe.
   To show help information about using the utility, type `alertexp.exe /?` at the command line. You can optionally specify the path to the iaobind.dat file and a path and filename for the output file.
2. Open the iaobind.txt file to view a summary of existing AMS alerts.

You can use the information about your existing alerts to create new alert rulesets. The text file lists the name of each alert with the associated action and severity, along with the application that triggers the alert and parameters associated with it.

Configuring alert rulesets

The **Alert rulesets** page displays all the alert rulesets that you can deploy to managed devices. There are four rulesets that appear by default, and you can create custom rulesets to apply specific types of monitoring to different kinds of devices.



Alert	State	Action	Health
Device Monitor System Connectivity	Critical, OK	Log handler configuration	Yes
IDE-R Start	Information	Log handler configuration	No
Intel vPro Agent Presence Alert	Warning, OK, Inform...	Log handler configuration	No
Intel vPro Agent Presence Alert	Warning, OK, Inform...	Intel vPro Agent Presence	No
Intel vPro Client Initiated Remote Management ...	Critical	Log handler configuration	No
Intel vPro Enhanced System Defense Alert	Critical, OK, Information	Log handler configuration	No
Intel vPro Enhanced System Defense Alert	Critical, OK, Information	Intel vPro Enhanced Sy...	No
Intel vPro Enhanced System Defense Remediati...	Information	Log handler configuration	No
Intel vPro System Defense Alert	Critical, OK, Information	Log handler configuration	No
Intel vPro System Defense Alert	Critical, OK, Information	Intel vPro System Defense	No
Intel vPro System Defense Remediation Alert	Information	Log handler configuration	No
Inventory Server - Asset alert date reached	Information	Log handler configuration	No
Inventory Server - Attribute modified	Information	Log handler configuration	No
Inventory Server - Could not read metaschema	Information	Log handler configuration	No
Inventory Server - Create socket failed	Information	Log handler configuration	No
Inventory Server - Database exception	Information	Log handler configuration	No

The four alert rulesets that appear by default on the **Alert rulesets** page are:

- **Core alert ruleset**: This ruleset ensures that alerts originating on the core server are handled. This ruleset is installed on the core server but can't be installed on other devices, and you can only have one core alert ruleset. You can edit the ruleset but can't delete it from the core server. This ruleset contains a predefined group of alert types, including Device Monitor, Intel vPro (Intel AMT) alerts, and Serial Over LAN Session alert types.
- **Default monitoring ruleset**: This ruleset is deployed by default to all managed devices and contains a number of alert types for real-time inventory and monitoring. You can edit this ruleset to add other alert types and change the settings for the default alert types.
- **LDMS default ruleset**: This ruleset is deployed by default to all LANDesk Management Suite managed devices. It includes alerts for security features included in Management Suite, such as access control, connection control manager, inventory scanner, and Security and Patch Manager alerts.
- **Provisioning ruleset**: This ruleset contains alerts related to provisioning tasks, such as task begin and end, section completed, and wrong OS pre-boot environment. When a device is provisioned, this ruleset is used to send alerts related to the progress of the provisioning task. (The ruleset is included in the provisioning agent and does not need to be manually deployed.) You can edit this ruleset to change the actions associated with the provisioning alerts (for example, to be notified by e-mail when a provisioning task is complete).

In addition to these rulesets you can create custom rulesets to apply to targeted groups of managed devices. You can deploy rulesets by scheduling a deployment task, or you can include rulesets when you deploy agents to devices using agent configuration. While the default rulesets are available to be deployed with agents, you can choose not to deploy the rulesets when you define the agent configuration.

Notes

- When you create a custom ruleset for a device, be aware that if a default ruleset has already been deployed to the device you may have overlapping or conflicting alerting rules. If you deploy the default ruleset when you configure the managed device, and then deploy a custom ruleset, both rulesets will be executed on the device. For example, if both rulesets generate alerts for the same alert type but take different actions, you may have duplicate or unpredictable alert actions as a result.
- Every alert that you create rules for automatically has a "Log handler configuration" rule so that every alert is logged at the core server. When you create a new alert rule, a

second rule with the Log handler configuration action is created by default. This default rule must always be in the ruleset: you can't delete it unless you delete all rules for that particular alert. In other words, if you have three rules for an alert, you can't delete the default rule unless you delete all three rules, but you can delete either of the other two rules for that alert.

Process for configuring a ruleset

Rulesets contain a collection of associated alerts, actions, and time filters. As you configure a ruleset, you'll define multiple action tasks and time filters that can be reused. The general procedure for configuring a ruleset includes the following steps:

1. Create a ruleset
2. Add new alert rules to a ruleset
3. Define alert actions to use in rules
4. Define time filters to use in alert rules
5. Edit alert rules in a ruleset
6. Include rulesets within other rulesets
7. Publish a ruleset

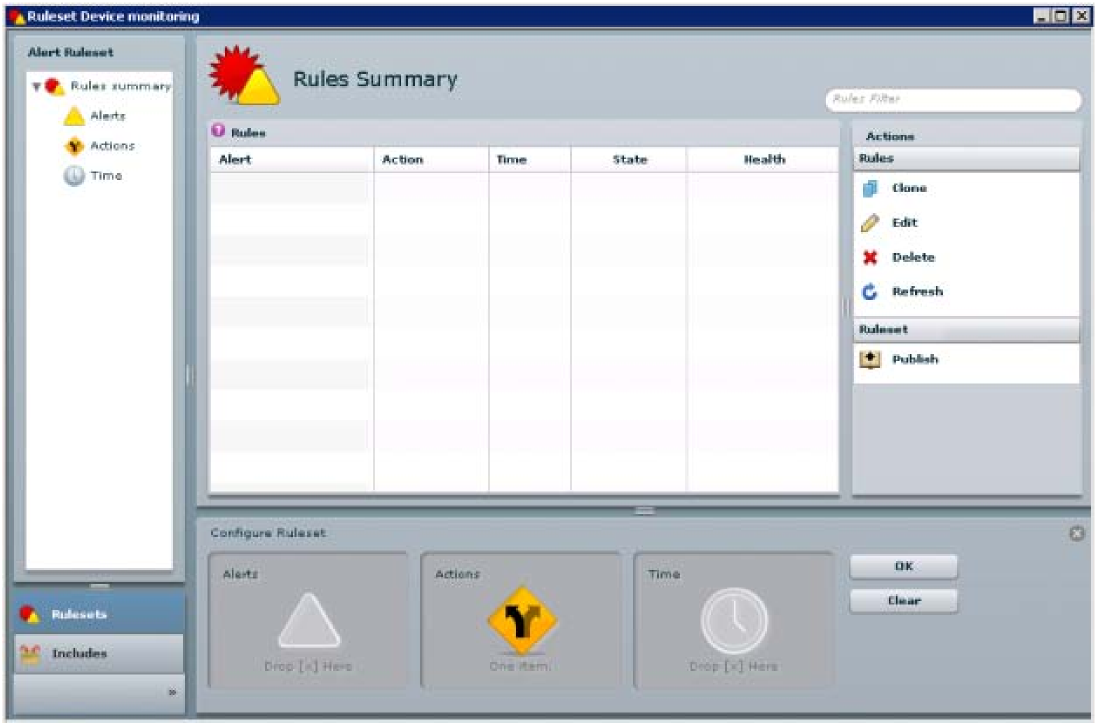
To create an alert ruleset

1. Click **Tools > Configuration > Alerting**.
2. Click the **New alert ruleset** button on the toolbar. Type a name in the **Name** field, type a description of the alert in the **Description** field, then click **OK**.
3. To change the ruleset's name or description, select it in the **Alert rulesets** list and click the **Edit an alert ruleset** button on the toolbar.
4. To make a copy of a ruleset that you can make minor changes to, right-click the ruleset in the list and select **Copy**. Type a new name and description and click **OK**.

To add new alert rules to a ruleset

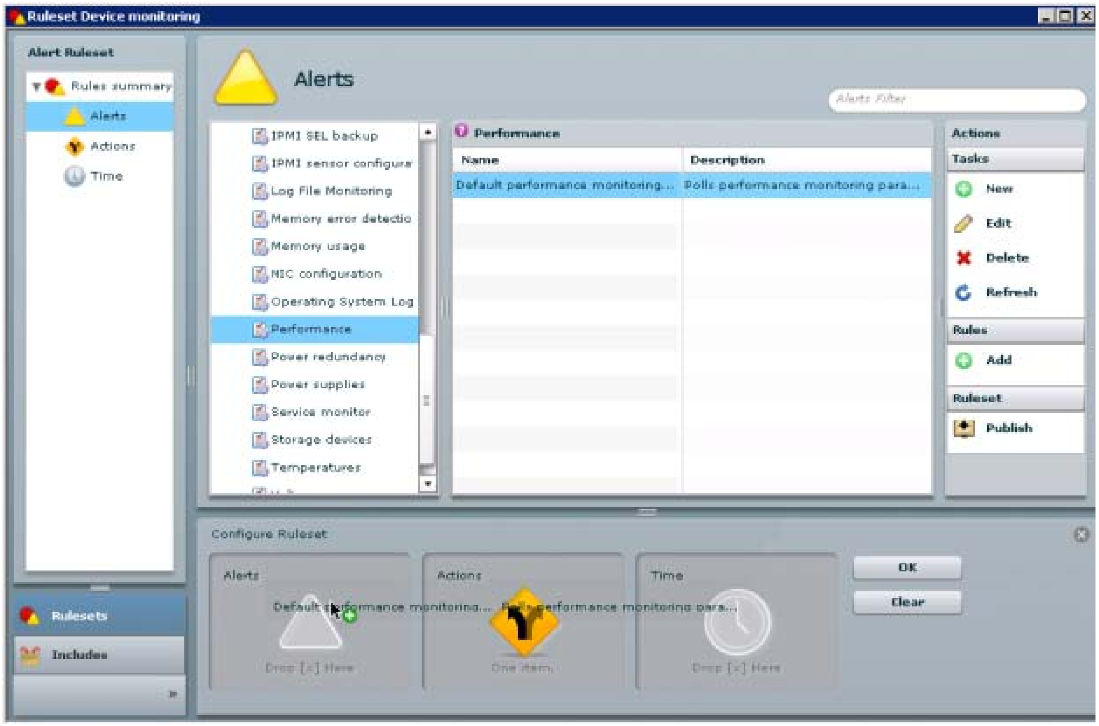
1. In the **Alert rulesets** list, select the ruleset and click **Edit** on the toolbar.

   The **Rules summary** page lists each alert in the ruleset with its associated actions and time. Each combination of an alert, action, and time is listed as a separate item on the rules summary.



2. Click **Alerts** in the left column to add an alert rule to the ruleset.

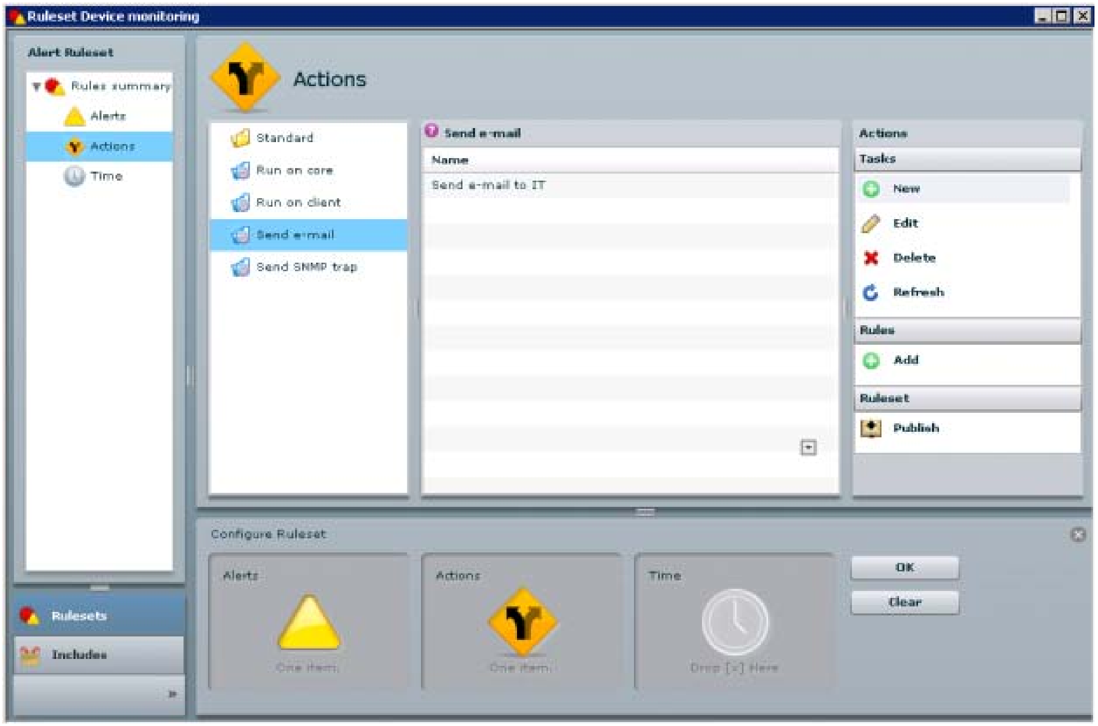
3. In the right column, click **Rules > Add**. Three "wells" are displayed at the bottom of the page to associate alerts, actions, and time rules. Locate an alert in the list and drag it to the **Alerts** well at the bottom of the page.



Name	Description
Default performance monitoring...	Polls performance monitoring para...

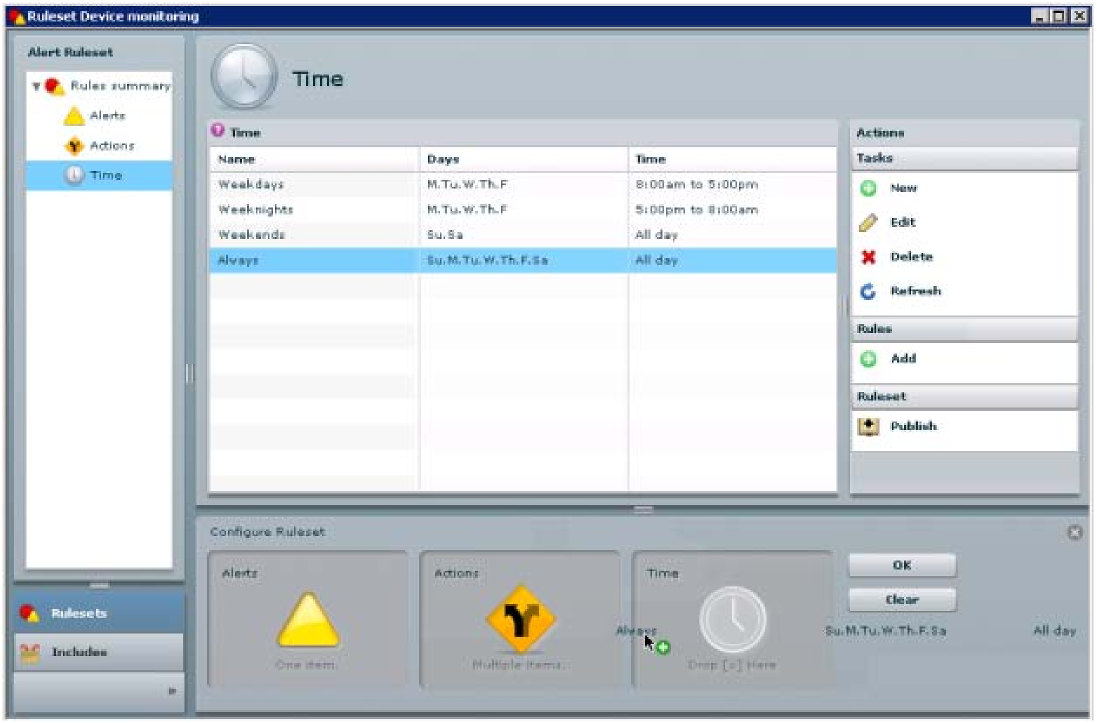
Alerts are listed in two groups, **Standard** and **Monitor**. Click an item under one of those groups to view a group of associated alerts. If you click the **All alerts** folder, all alerts are listed alphabetically.

4. To find a particular alert, type a search string in the **Alerts filter** text box at the top right of the page. All alerts containing the string you type are displayed in the list.
5. Click **Actions** to associate an alert action with the alert you added. By default, every alert has a **Log handler configuration** action associated with it, which logs the alert at the core server. To add another action, drag it to the **Actions** well at the bottom of the page.



The **Standard** folder contains predefined actions. To use another type of action, you need to define the action first (see steps below).

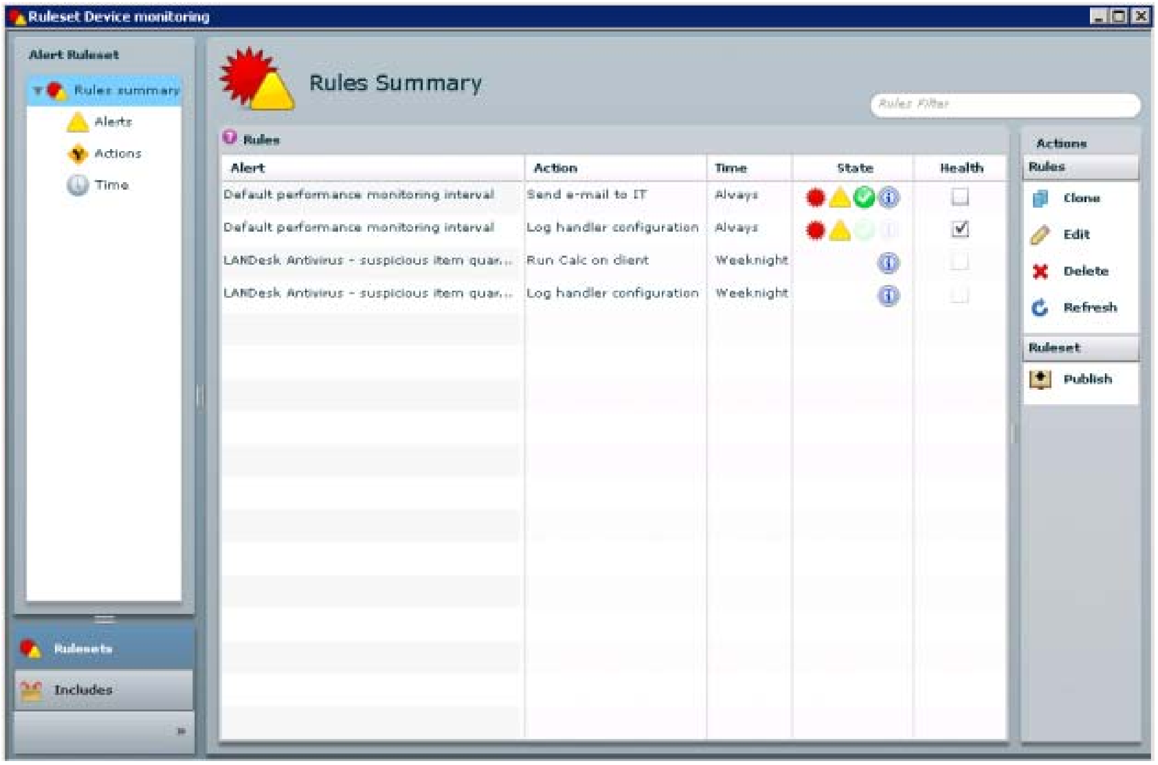
6. Click **Time** to specify how frequently the alert should be monitored. Drag a time rule (for example, **Always**) to the **Time** well at the bottom of the page.



Name	Days	Time
Weekdays	M.Tu.W.Th.F	8:00am to 5:00pm
Weeknights	M.Tu.W.Th.F	5:00pm to 8:00am
Weekends	Su.Sa	All day
Always	Su.M.Tu.W.Th.F.Sa	All day

Three time rules are available by default. To use a different time rule, you need to define it first (see steps below).

7. When you have at least one alert with associated action and time tasks, click the **OK** button at the bottom of the page to add the alert rule to the ruleset. Click **OK** again.
8. In the right column, click the **Publish** button.
9. In the left column, click **Rules summary** to view the updated ruleset with the new alerts.

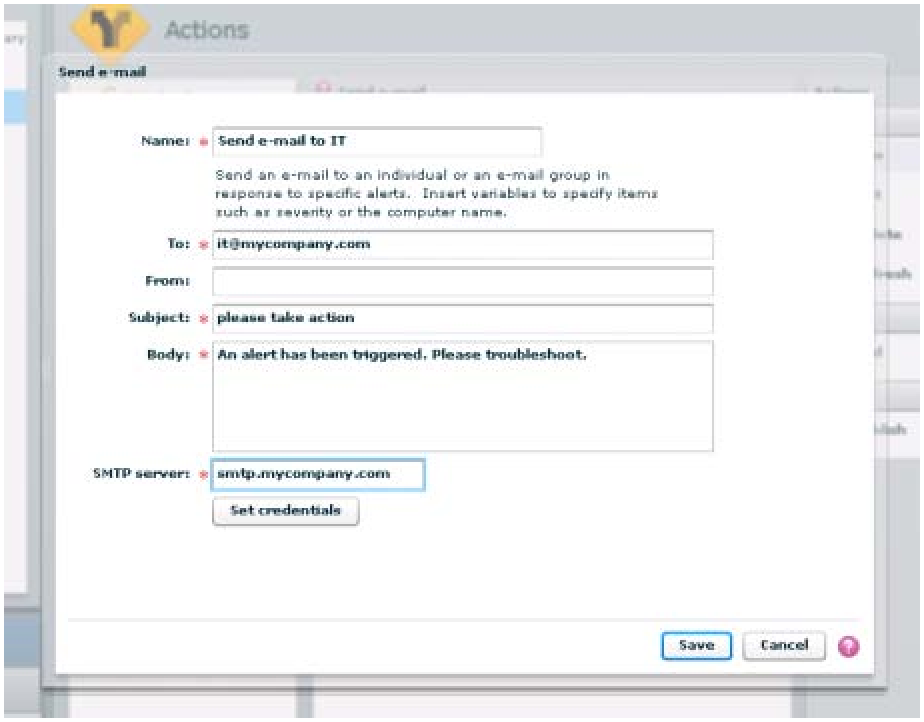


Alert	Action	Time	State	Health
Default performance monitoring interval	Send e-mail to IT	Always	● ▲ ✓ ⓘ	□
Default performance monitoring interval	Log handler configuration	Always	● ▲	☑
LANDesk Antivirus - suspicious item quar...	Run Calc on client	Weeknight	ⓘ	□
LANDesk Antivirus - suspicious item quar...	Log handler configuration	Weeknight	ⓘ	□

With a list of alerts in the ruleset, you can edit each item to change the associated action and time. You can also choose which severity levels to apply to the alert and you can specify whether that alert should contribute to the device health. See the steps below for more information about editing a rule.

To define alert actions to use in rules

1. In the left column of the **Alert ruleset** page, click **Actions**.
2. Select an action group (for example, **Send e-mail**), then click **Tasks > New** in the right column.
3. Add information in the fields as needed, then click **Save**.



Name: * Send e-mail to IT

Send an e-mail to an individual or an e-mail group in response to specific alerts. Insert variables to specify items such as severity or the computer name.

To: * it@mycompany.com

From:

Subject: * please take action

Body: * An alert has been triggered. Please troubleshoot.

SMTP server: * smtp.mycompany.com

Set credentials

The action is listed under the group you selected and is available to associate with alerts. Details about the fields in the different actions types are explained below.

Run on core/Run on client

This action starts an executable file on either the core server or the managed device.

- **Name**: the identifying name for the action. Be specific so you can easily distinguish between actions.
- **Path and filename**: the full path and filename for the executable to be run on the core server or the managed device. When the alert is triggered, the alerting agent will issue a command to run this file.

When you select either action, note that programs may not display as expected on the desktop. When the program is run, it is started as a service in Windows and so is not displayed as a regular application would be. Programs that are run in this way should not contain a user interface that requires interaction. To definitively determine if the program executed, check the processes in the Windows Task Manager.

Send e-mail

This action sends an e-mail message using the SMTP server you specify.

- **Name**: the identifying name for the action. Be specific so you can easily distinguish between actions.
- **To**: the full e-mail address of the person you want to the receive the e-mail notification.
- **From**: any valid e-mail address, preferably one that indicates that the e-mail is an alert notification. If this is not a valid e-mail address the message will not be sent.
- **Subject**: a descriptive subject for the e-mail notification.
- **Body**: a message to accompany the alert notification.
- **SMTP server**: the location of an SMTP server from which the e-mail can be sent.

- **Set credentials**: click to specify a username and password that can be used to log on to the SMTP server.

The e-mail will be sent from the core server.

You can send e-mail messages to multiple recipients, and you can use the following variables in the Body field:

- %% = %
- %D = Description
- %N = Computer name
- %S = Severity
- %T = Time (UTC)

Send SNMP trap

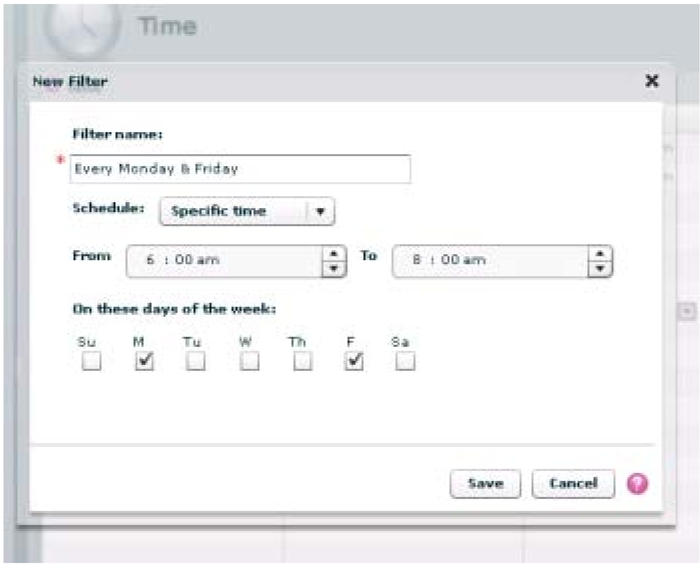
This action sends an SNMP v1 trap when the alert is triggered.

- **Name**: the identifying name for the action. Be specific so you can easily distinguish between actions.
- **Host name**: the name of the SNMP host that will receive the trap.
- **Community string**: a v1 community string that is used by the host to receive traps.

Severity levels for alerts are reported in the Specific Trap Type field of the trap. Values are 1 = Unknown, 2 = Informational, 3 = OK, 4 = Warning, and 5 = Critical.

To define time filters to use in alert rules

1. In the left column of the **Alert ruleset** page, click **Time**.
2. Click **Tasks > New** in the right column.
3. In the **New filter** dialog, enter data in the fields (described below).
4. Click **Save**.



Filter name: Every Monday & Friday

Schedule: Specific time

From 6 : 00 am To 8 : 00 am

On these days of the week:

Su □ M ☑ Tu □ W □ Th □ F ☑ Sa □

The time filter appears in the list and is available to associate with alerts. Details about the fields in the **New filter** dialog are explained below.

- **Filter name**: the identifying name for the filter.
- **Schedule**: select **Specific time** for a filter that limits the time and days when the alert is monitored. Select **Anytime** to monitor the alert continually.

- **From** and **To**: select a beginning and ending time during the day when the alert is monitored.
- **On these days of the week**: select the days that you want the alert monitored.

To edit an alert rule

You can edit individual alert rules in the **Rules summary** page. Changes you can make include selecting a different action or time filter, selecting which severity levels are in effect, and specifying whether the rule contributes to the device's health status.

1. Click **Rules summary** to view the alert rules in the current ruleset.
2. Click the alert rule you want to edit and click **Rules > Edit** in the right column.
3. To change the associated action or time, select a new option from the drop-down lists.
4. To receive an alert notification only for particular severity levels, click the **State** icons. A dimmed icon indicates that alerts for that severity level will be ignored.
5. To include the alert rule as an indicator of device health, check the **Health** check box.
6. Click **OK** to save your changes.

Each alert rule can have only one associated action and one time filter. If you want to create additional rules for an alert, click **Clone** in the right column to create a duplicate of the rule, then edit the duplicate.

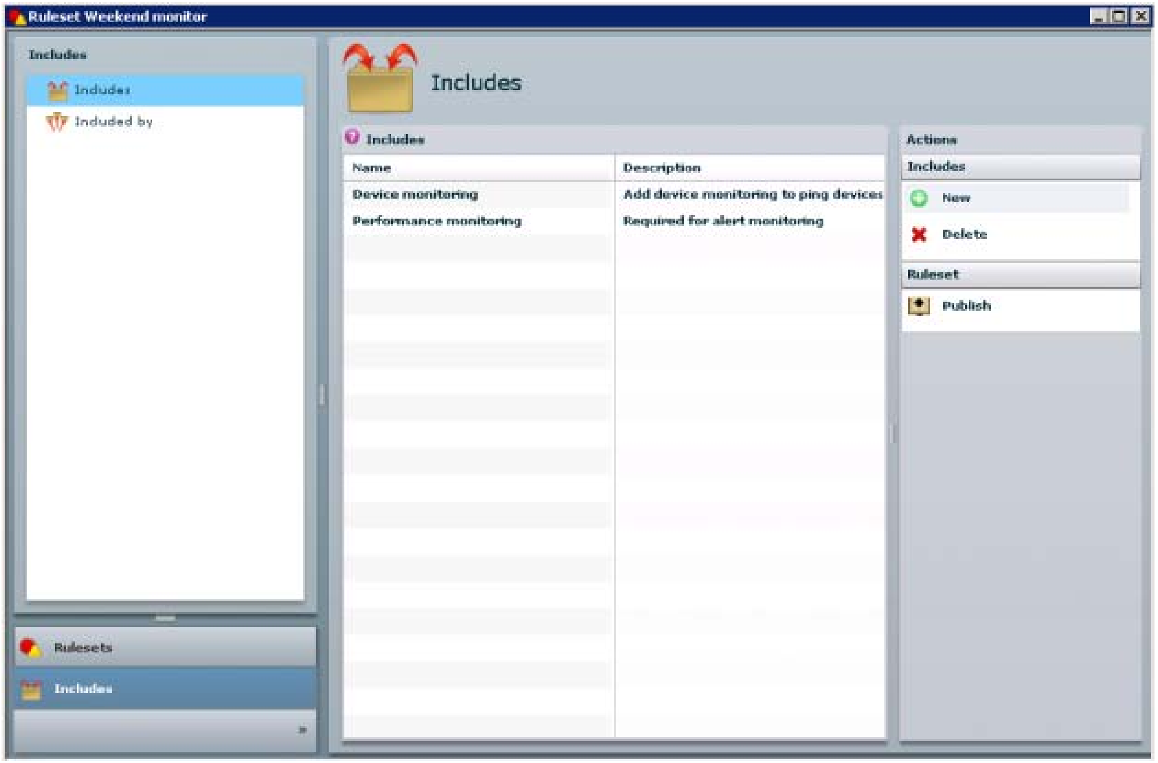
To include rulesets within other rulesets

One way to make ruleset creation more flexible is to create smaller rulesets that you then combine for different uses. To do this, you can include rulesets within other rulesets.

1. At the bottom left of the **Alert ruleset** page, click **Includes**.
2. In the left column, click **Includes**.
3. In the right column, click **Includes > New**.
4. In the **Available rulesets** dialog, select one or more rulesets to include in the current ruleset, then click **Save**. Use Ctrl+click or Shift+click to select multiple rulesets.

   The rulesets are added to the **Includes** list.

5. If you want to remove a ruleset from the **Includes** list, select it and click **Includes > Delete** in the right column.
6. To see which other rulesets include the current ruleset, click **Included by** in the left column.



Name	Description
Device monitoring	Add device monitoring to ping devices
Performance monitoring	Required for alert monitoring

When you include rulesets, each individual ruleset is maintained as an individual XML file. The XML files are not combined, but they reference each other

To publish an alert ruleset

After you have added and edited rules in a ruleset you need to publish the ruleset. This creates an XML file with the ruleset data that is referenced by the alerting agent as it works.

1. On the **Rules summary** page, click **Publish** in the right column.

A success message will indicate that the ruleset has been published.

The XML files with published ruleset data are stored in the ldlogon share on the core server, in the alertrules folder.

When you publish a ruleset, the alerting service is notified to reload the updated rulesets. When you have updated a ruleset that you have already deployed to managed devices, each of those devices will automatically update their rulesets with the modified rules the next time the alerting agent runs on those devices.

If you don't publish a ruleset, there will be no signal to the alerting service to reload the ruleset, so there will be no automatic update of the ruleset on devices that already have the ruleset. It is strongly recommended that you publish rulesets every time you make any changes to them.

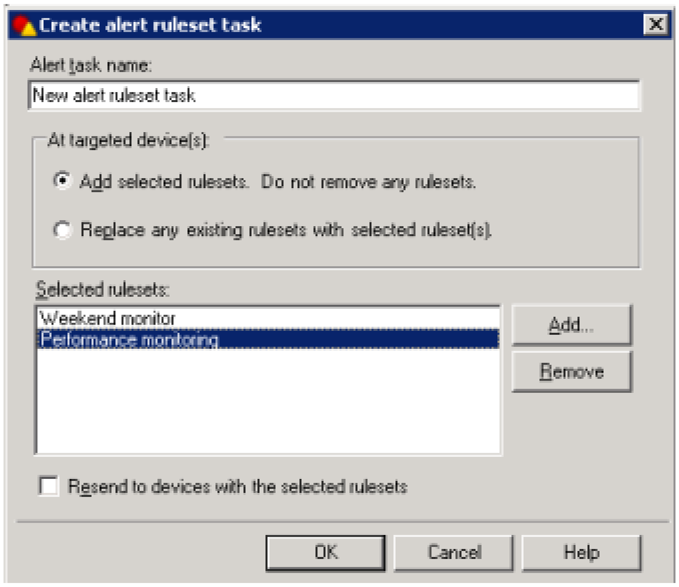
Deploying alert rulesets

To install an alert ruleset on one or more devices, you can schedule a deployment task for the ruleset.

In order to deploy a ruleset to a managed device, you must first have a management agent installed on that device. When you deploy the standard management agent, the default ruleset is installed on the device by default, but you can select this or any other available rulesets to be installed on the device with the management agent. After the agent setup is complete you can update the default ruleset or deploy new rulesets by scheduling an alerting task.

To deploy an alert ruleset

1. Click **Tools > Configuration > Alerting**.
2. In the **Alert rulesets** list, click the ruleset you want to deploy.
3. On the toolbar, click the **Create a task** icon and select **Distribute rulesets**.



Create alert ruleset task

Alert task name: New alert ruleset task

At targeted device(s):

● Add selected rulesets. Do not remove any rulesets.

○ Replace any existing rulesets with selected ruleset(s).

Selected rulesets:

Weekend monitor
Performance monitoring

□ Resend to devices with the selected rulesets

4. Type a task name for the alerting task.
5. To add the ruleset to devices and keep any existing rulesets on those devices, click **Add selected rulesets**.

   To add the ruleset to devices and remove any existing rulesets on those devices, click **Replace any existing rulesets**.

   If you have previously deployed the ruleset and want to update it on the same devices, select the **Resend to devices with the selected rulesets** check box.
6. To deploy other rulesets in the same task, click the **Add** button and select the rulesets.
7. Click **OK**.

To remove all existing rulesets

You can remove all existing rulesets from targeted devices without deploying any new rulesets.

1. Click **Tools > Configuration > Alerting**.
2. On the toolbar, click the **Create a task** icon and select **Remove all rulesets**.
3. Click **OK**.

You can deploy rulesets to devices as part of an agent configuration. When you define an agent configuration you can select the rulesets you want to deploy.

If the ruleset you deploy includes a Performance monitoring rule, the details of what to monitor are defined on each individual device. This is done in the server information console on each device. You can select different hardware and software components and define counters for the items to be polled, then view the monitoring data in real time or historically. See Performance monitoring for detailed information.

Viewing alert rulesets for a device

To view the alert rulesets that have been assigned to a managed device, open the full inventory view for the device. This displays the name of the ruleset and the date it was last installed or updated on the device.

To view the alert rulesets installed on a device

1. In the **All devices** view, right-click the device and select **Inventory**.
2. In the tree view, expand **LANDesk Management** and click **Alert Ruleset Installed**.
3. If there is more than one ruleset, select a ruleset in the tree view to display its details.

You can also create a query that returns all devices that have a particular alert ruleset installed. In the query components list, follow the same path as described in the inventory list above.

Viewing the alert log

Use the **Alert log** page to view alerts sent to the core (the global alert log) or to managed devices. The log is sorted by time (GMT), the most recent alert being at the top of the log.

The alert log contains the following columns:

- **Alert name:** The name associated with the alert, as defined in the **Alert configurations** page.
- **GMT Time:** The date and time the alert was generated (GMT).
- **Status**: The severity state of the alert, which can be one of the following:
  - **Unknown:** The status cannot be determined.
  - **Informational:** Supports configuration changes or events that manufacturers may include with their systems.
  - **OK:** Indicates that the status is at an acceptable level.
  - **Warning:** Provides some advance warning of a problem before it reaches a critical point.
  - **Critical:** Indicates that the problem needs your immediate attention.
- **Device name:** The name of the device on which the alert was generated. This should be a fully qualified domain name. (Global alert log only).
- **IP address:** The IP address of the device on which the alert was generated (Global alert log only).
- **Instance:** Provides more detailed information as to the situation in which the alert was generated.

If the device name does not appear as a fully qualified domain name, it is because this product was unable to resolve the fully qualified domain name for the device.

To view the global alert log

1. Click **Tools > Reporting/Monitoring > Logs**.
2. To sort entries by column, click a column heading.
3. To view a more detailed description of an alert, double-click the entry in the **Alert name** column.
4. To list log entries by name, status, or instance, select the filter criteria in the **In column** drop-down list. For example, select **Alert name** and type a complete name

(such as Performance) or a partial name with the * wildcard (such as Remote*) in the **Find** box. To search by date, select **Enable date filtering**, enter a range with a start date and end date. When you have added filter criteria, click the **Search** button.

5. To clear the health status of an alert, select the alert in the **Alert name** column and click the **Acknowledge** button on the toolbar, and then click **OK**.
6. To delete a log entry, right-click the alert and select **Delete**.

To view the alert log for a specific device

1. Click **Tools > Reporting / Monitoring > Health dashboard**.
2. In the list of devices, double-click the device.
3. In the left navigation pane, click **System information**.
3. Click **Logs > Alert log**.
4. To sort entries by time, name, or state, click a column heading.
5. To view a more detailed description of an alert, double-click the entry in the **Alert name** column.
6. To list log entries by name or state, click the **Filter** button on the toolbar and select the filter criteria. For example, select **Alert name** and type a complete name (such as Performance) or a partial name with the * wildcard (such as Remote*). To search by date, select **Enable date filtering**, enter a range with a start date and end date. When you have added filter criteria, click **Find.**
7. To clear the health status of an alert, select the alert in the **Alert name** column, click **Acknowledge alert** on the toolbar, and click **OK**.
8. To delete a log entry, click the alert in the **Alert name** column and click **Delete entry** on the toolbar.

You can also view the device's alert log by clicking the **Alert log** button on the **Rulesets** page of the server information console.

Rollup cores

If you've installed more than one core server, you can:

- Install a rollup core
- Use the database Rollup Utility

Installing a rollup core

You can use a rollup core to combine the data from multiple core servers. You must schedule rollup core updates to synchronize the rollup core database with each core server's core database. Using the Management Suite Web console, you can then manage devices in the rollup core using queries, software distribution, remote control, and the other features the Web console supports.

Before installing a rollup core, you need to have configured an additional Oracle or SQL Server rollup database server. Management Suite setup's rollup option will prompt you for information about the database you've set up.

You can rollup data from cores using Management Suite version 8.7 SP2 or later. The rollup core must be installed from the latest Management Suite version. All cores must be using the same database type, such as all SQL or all Oracle. If you're rolling up data from Management Suite versions earlier than 9.0 and you're also using a double-byte version of Management Suite (Japanese, Chinese, or Russian), all cores must be using the same language.

To install a rollup core

1. Set up a server to host the rollup core and database.
2. Install the database the same way you would for a normal Management Suite installation. For information on installing the database, see the LANDesk community at http://community.landesk.com.
3. Log in to the rollup core server with an account that has administrator rights.
4. Install the rollup core through the autorun on your Management Suite installation media. Finish setup.

Configuring rollup database links

This section describes how to configure database links on the rollup core. You'll need to do this before you can start rolling up data.

- Oracle rolling to Oracle
- SQL Server rolling to SQL Server

The person doing this configuration must also have access to all DBMSs used by LANDesk, and they must have security permissions to create database links and perform configuration steps at a DBMS server level.

Oracle rolling to Oracle

Configure the Oracle database

The TNSNames.ora file on the database server in which your rollup database exists must contain an entry for your core server database.

1. For an Oracle database, within the Enterprise Manager Console, log in to your database. Expand **Distributed**.
2. From the **Database Links** item's shortcut menu, click **Create**.
3. In the **Name** field, enter a name for your database link.
   Note: If the AR database is using Oracle9i, the link name can be any name that is not already in use or reserved. The installation will prompt you for this information.
4. Choose **Fixed User** and enter the username and password for the core server's database.
5. In the **Service Name** field, enter the TNSNames.ora (i.e., Net Alias) entry that refers to your core server database.
6. Click **Create**.
7. Double-click your newly-created link and click **Test**. You should get a message that says your link is active. You can also test your link by logging into the rollup database and issuing the following command:

   Select count(*) from computer@linkname;

   If the return is a count of devices in the core server's production database, then the link is configured properly.

SQL Server rolling to SQL Server

Configure the SQL Server database

Creating links with SQL

1. Open SQL Server Management Studio.
2. Expand your server and expand **Server Objects**.
3. From the **Linked Servers** item's shortcut menu, click **New Linked Server**.
4. On the **General** page, do steps 5-11:
5. **Linked Server**: enter a unique name for this database link (for example, LDMS core server1 Link).
6. Choose **Other data source.**
7. Select **Microsoft OLE DB Provider for SQL Server**.
8. **Product name**: Enter LDMS.
9. **Data source**: enter the name of the database server containing the core database.
10. **Provider string**: enter the provider string. For instance:

    SQL Server
    provider=SQLOLEDB.1;user id=<User for the core server's database>
    *** The user id portion of the provider string is required on the connection string to another SQL Server database. ***

11. **Catalog**: enter the physical name of your core server's database (for example, lddb).
12. On the **Security** page, select **Be made using this security context** and enter the username and password for the core server's database, then click **OK**.
13. Click **New Query** and issue the following command:

    Select count(*) from [Link name].[database name].[table-owner name].Computer

    Using the values above, this query would appear as:

```
Select count(*) from [LDMS Core Server1 Link].[lddb].[dbo].Computer
```

If the correct count comes back, your link is set up correctly.

Using the database Rollup Utility

The database Rollup Utility (DBROLLUP.EXE) enables you to take multiple source core databases and combine them into a single destination core rollup database. The rollup core device limit depends on your hardware and acceptable performance levels. The source database can be either a core server or a rollup core server.

The system requirements for a destination database may be substantially greater than the system requirements for a standard database. These requirements can vary considerably depending on your network environment. If you need more information about hardware and software requirements for your destination database, contact your LANDesk Software support representative.

Setup installs the database Rollup Utility automatically with the rollup core. The Rollup Utility uses a pull mechanism to access data from cores you select. For database rollups to work, you must already have a drive mapped to each core you want the Rollup Utility to get data from. The account you connect with must have rights to read the core server's registry.

The Rollup Utility checks with a registry key on the core server for database and connection information (HKLM\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\local) and uses that key's information to access the database associated with each core you add to the Rollup Utility. For Oracle databases, the TNS definition on the server you're running the Rollup Utility from must match the TNS definition on the core server the utility is accessing.

You can use the Rollup Utility to select the attributes you want rolled up from the cores. The attribute selections you make apply to all cores. Limiting the number of attributes shortens the rollup time and reduces the amount of data transferred during rollups. If you know you won't be querying on certain attributes, you can remove them.

The Rollup Utility always rolls up the selected attribute data. Rollup also doesn't include any queries or scopes you've defined. Any console users with rights to the rollup database have access to all data within that database. You can use feature-level security to limit access to Web console features.

Once you've added the core servers that you want to roll up and the attribute list for those servers, you can click **Schedule** to add a scheduled rollup script for each core server. From a Web console, you can then schedule these rollup scripts to run at the time and interval you want. Rollup scripts are only visible from the Web console and reside on the rollup core.

To launch the Rollup Utility

1. On a rollup core, run the Rollup Utility (\Program Files\LANDesk\ManagementSuite\dbrollup.exe).
2. Select an existing rollup core server to manage from the list, or click **New** to enter the name of a new rollup core server. Note that you must enter the core server name, and not the database name.
3. Once you select a rollup core, the Source cores list shows cores you've configured to roll up to the selected rollup core.

To configure the attributes that you want to roll up

1. From the Rollup Utility, select the rollup core you want to configure.
2. Click **Attributes**.
3. By default, all database attributes are rolled up. Move attributes from the **Selected Attributes** column to the **Available Attributes** column that you don't want to roll up.

4. Click **OK** when you're done. Moving attributes to the Available Attributes column deletes associated data from the rollup database.

To configure the source core servers for a rollup core

1. From the Rollup Utility, select the rollup core you want to configure.
2. Once you select a rollup core, the Source cores list shows cores you've configured to roll up to the selected rollup core. Click **Add** to add more cores or select a core and click **Delete** to remove one.

WARNING: Clicking delete immediately removes the selected core and all of that core's data from the rollup core database. Also, if you supply an invalid link name when adding a core server to the rollup database, you will have to remove the core from the rollup and re-add it in order to modify the link name.

To schedule database rollup jobs from the Web console

1. From the Rollup Utility, select the **Rollup core** you want to configure.
2. In the **Source cores** list, select the cores you want to schedule for rollup and click **Schedule**. If you don't select any cores, by default all cores in the list will be scheduled when you click **Schedule**. Clicking **Schedule** adds a rollup script for the selected core to the selected rollup core. If you select multiple cores, they will be scheduled as one job and will be processed one at a time.
3. From a Web console, connect to the rollup core server.
4. In the left navigation pane, click **Schedule rollup jobs**.
5. Click the rollup script you want to schedule. The script names begin with the source core name followed by the destination rollup core name in parentheses. Click **Schedule roll up**.
6. Select when you want the roll up to happen and whether it should automatically reschedule or not. Make sure there isn't more than one core being rolled up at a time. Click **Continue to next step**.
7. Verify the script schedule and click **Finish**.

WARNING: Don't schedule rollups from cores during times when they'll be downloading patch information. The patch information download puts a heavy load on the database which will slow down the rollup.

Only one rollup can be processed at a time. A scheduled rollup will fail if another rollup is already in progress. When scheduling rollups, allow enough time between rollups that there won't be any overlap. If the rollup times are hard to predict, it's best to schedule all the rollups in a single job. Do this by selecting multiple cores before clicking **Schedule**. This way, the rollups are handled one at a time automatically.

Note: After rolling up data from core servers running a version of Management Suite earlier than 9.0, DBRollup.exe's **Rollup status** dialog will show that the "Job completed with one or more errors." This is normal. Also, if you schedule a rollup task to a pre-9.0 core, the scheduled task status will show "Failed - Task handler encountered an error" even if the job completed successfully. This also is normal, but you should check the DBRollup and database logs if you suspect the failure is for another reason, such as a database lock.

Replicating rollup core data to source cores

If you have a rollup core in your LANDesk environment, you can replicate these items to source core servers:

- Queries
- Distribution package configurations
- Delivery method configurations

You can create standard configurations for these items on the rollup core and then use replication to make them available on source cores for your Management Suite users.

The **Replicate to cores** tool is visible when the Web console is connected to a rollup core. The account you use to connect must be a LANDesk administrator. When you click this tool, a dialog appears where you can name the replication task and choose what you want replicated. When you configure this information and click **OK**, a task with the name you chose is available in the rollup core's **Scheduled tasks** view.

Replication won't happen until you configure the replication task to run. You can manually start the task with the **Start now** option or you can create a recurring schedule for the task. When the task runs, the rollup core creates an XML document containing the information to be replicated. Replication tasks aren't large or demanding, so you can use whatever replication schedule is necessary for your management environment.

Replication tasks don't use manually-selected targets. Source cores with a rollup core certificate receive the XML file and then show the replicated data. You can use the Database Rollup Utility (DBROLLUP.EXE) to attach rollup core certificates.

Only data with a "Public" owner is replicated. If you have data you don't want replicated, assign it to an owner other than "Public." You can edit replicated data on source cores, but unless you change the item's name, your changes will be overwritten the next time replication happens for an item with the same name. If replicated items are in custom groups on the rollup core, the group structure also gets replicated on source cores.

Replication only adds the replicated data to source cores. If you delete an item on the rollup core that was replicated at one point, that deletion won't be made on source cores. If you want to delete a replicated item on source cores, you must do it manually.

To use replication on a rollup core

1. On the rollup core, configure the public queries, distribution packages, and delivery methods that you want to replicate.
2. While connected to the rollup core's Web console with an account that's a LANDesk administrator, click the **Replicate to cores** tool.
3. Enter a task name and check the items you want to replicate.
4. Click **OK**.
5. Click the **Scheduled tasks** tool.
6. Start the replication task now or configure a schedule for it. When the task runs, source core servers with a rollup core certificate receive the replicated data.

Increasing the rollup database timeout

With large rollup databases, the Web console's query editor may time out when it tries to display a large list, such as the Software Package Name list. When this happens, the list you are trying to display won't show any data. If you experience timeouts you need to increase the database timeout value. This needs to be done wherever the IIS service or the Web console server is being installed. At the following registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core

Add a new DWORD, Timeout, with a decimal value of 1800. This value is in seconds. You can adjust this value based on your query types and database performance. Stop and restart IIS for the change to take effect.

About the Rollup Utility

Use the database Rollup Utility (run from the rollup core) to manage data rollups from core servers.

- **Rollup core:** You can manage multiple rollup cores from the Rollup Utility. Select the core you want to manage. You first must have a drive mapped to each rollup core.

- **New:** Click to add a new rollup core that you want to manage. You first must have a drive mapped to the rollup core you're adding. Enter the rollup core's computer name and click **OK**.
- **Attributes:** Click to select the attributes you want rolled up. The attributes list is global for all core servers the selected rollup core uses. Move individual attributes or attribute trees from the Selected Attributes column (these attributes will be rolled up) to the Available Attributes column (these attributes won't be rolled up).
- **Reset database:** Click to reset the selected rollup database. This deletes all data and rebuilds all tables.
- **Add:** Click to add a core that you want to include data from in the selected rollup core.
- **Delete:** Click to remove the selected core and its data from the selected rollup core's database. **WARNING:** This option deletes the selected core's data when you click **OK**. Data from other core servers remains in the rollup database.
- **Schedule:** Click to add a rollup script for the selected core. If you don't have a core selected in the Source Cores box, this option creates rollup scripts for all cores in the Source Cores box.
- **Rollup:** Click to do an immediate rollup from the selected core. You must have a core selected for this option to be available.
- **Close:** Click to close the Rollup Utility.

Hardware-specific configuration

This chapter includes information about configuration and management of devices with unique hardware capabilities that are specific to the hardware manufacturer. It includes the following sections:

- Intel vPro support overview
- Configuring Dell OMCI devices
- Managing Dell DRAC devices
- IPMI support
- IPMI BMC configuration

Intel vPro support overview

Management Suite supports devices using Intel vPro technology, a hardware and firmware technology that enables remote device management and security. Intel vPro uses out-of-band (OOB) communication for access to devices regardless of the state of the operating system or power to the device.

In this product, the term "Intel vPro" refers to technologies provided on desktop and mobile computers with Intel vPro support. This product also supports devices with earlier versions of Intel Active Management Technology (Intel AMT). The process for provisioning devices with different versions of Intel vPro varies according to the version numbers. The information in this section applies to all versions except as noted.

The following table lists Intel vPro features supported in this product in different versions of Intel vPro.

Feature	Intel AMT 1.0	Intel vPro 2.0/2.1/2.2	Intel vPro 2.5/2.6	Intel vPro 3.0	Intel vPro 4.0	Intel vPro 5.0	Intel vPro 6.0
Provision devices	Yes	Yes	Yes	Yes	Yes	Yes	Yes
System Defense	No	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced System Defense	No	No	No	Yes	Yes	Yes	Yes
Agent Presence	No	Yes	Yes	Yes	Yes	Yes	Yes
Wireless profile & device management	No	No	Yes*	No	Yes		Yes
Serial-over-LAN & IDE redirection	Yes	Yes	LAN connection: Yes Wireless mode: Yes, if wireless profile exists	Yes	Yes	Yes	Yes
Remote configuration (zero touch provisioning)	No	2.0/2.1: No 2.2: agent-	2.5: No 2.6: agent-based	Yes	Yes	Yes	Yes

Feature	Intel AMT 1.0	Intel vPro 2.0/2.1/2.2	Intel vPro 2.5/2.6	Intel vPro 3.0	Intel vPro 4.0	Intel vPro 5.0	Intel vPro 6.0
		based only	only				
Network Environment Detection	No	No	No	Yes	Yes	Yes	Yes
Client-Initiated Remote Access	No	No	No	Yes	Yes	Yes	Yes

*A wireless profile is required for wireless management of Intel Centrino 2.5 notebooks. For Intel Centrino 2.6 notebooks, a wireless profile is required only to use Serial-over-LAN and IDE redirection features; other wireless management features can be used whether or not a wireless profile exists on the notebook.

This chapter contains information on the following:

- Configuring Intel vPro devices
- Changing the password for Intel vPro devices
- Configuring System Defense policies
- Configuring Intel vPro Agent Presence settings
- Intel vPro wireless support
- Intel vPro device management
- Remote access for Intel vPro devices

Managing devices with or without management agents

When devices are configured with Intel vPro, a limited number of management features are available even if the device does not have a LANDesk agent installed. As long as devices are connected to the network and have standby power, they can be discovered and can be added to the database to be managed with other devices on the network.

If a device has Intel vPro but no management agent installed, it can be discovered, added to the inventory database, and viewed in the **My devices** list. Management features that are available for Intel vPro-configured devices include:

- **Inventory summary:** A subset of the normal inventory data can be queried and viewed in real time for the device even if the device is powered off.
- **Event log:** A log with Intel vPro-specific events, showing severity and description of the events, can be viewed in real time.
- **Remote boot manager:** Power cycling and several boot options can be initiated from the remote management console, regardless of the state of the device's OS or power. The options available are dependent on support for the options on the device. Some devices may not support all boot options.
- **System Defense**: The Intel vPro System Defense feature enforces network security policies on managed devices. Enhanced System Defense (beginning with release 3.0) adds heuristic filtering rules to prevent malicious software attacks on the network.

Other Management Suite management options are available only when a management agent is installed on the device. For more information about management options, see Intel vPro device management.

Intel AMT version 1.0 provisioning requirements

Devices can be discovered as Intel AMT 1.0 devices only after you have accessed the Intel AMT Configuration Screen on the device's BIOS and changed the manufacturer's default password to a secure password (refer to the manufacturer's documentation for information on accessing the Intel AMT Configuration Screen). If you haven't done this, the devices will be discovered but not identified as Intel AMT devices, and you won't be able to view the same inventory summary information as you otherwise would.

In order for the core server to authenticate with discovered Intel AMT devices, the username/password credentials you enter in the device BIOS must match the credentials that you enter in the Intel vPro general configuration dialog.

When an Intel AMT device is added to the core database to be managed, Management Suite automatically provisions it, regardless of whether it has already been provisioned. Small business mode provides basic management without network infrastructure services and is non-secure, while Enterprise mode is designed for large enterprises and uses DHCP, DNS, and a TLS certificate authority service to ensure secure communication between the managed device and the core server.

When you provision an Intel AMT device in Enterprise mode, the core server installs a certificate on the device for secure communication. If another computer attempts to access the Intel AMT functionality on the device, it will not succeed because it does not have a matching certificate.

Configuring Intel vPro devices

Devices equipped with Intel vPro functionality should be configured when they are first set up and powered on, to enable Intel vPro features. This process includes several security measures to ensure that only authorized users have access to the Intel vPro management features.

Intel vPro devices communicate with a provisioning server on the network. This provisioning server listens for messages from Intel vPro devices on the network and allows IT staff to manage servers through out-of-band communication regardless of the state the device’s OS is in. The core server acts as a provisioning server for Intel vPro devices and includes features that help you provision devices when you set them up. You can then manage the devices with or without additional management agents.

This section outlines a recommended process for configuring new Intel vPro devices. During this process you will use Management Suite to generate a set of provisioning IDs (PID and PPS). These IDs are entered in the device BIOS to ensure a secure connection with the provisioning server during the initial provisioning process. This "one-touch" process can be used to configure devices with release 2.0 and later.

Devices with release 2.2/2.6 and later can also be configured using remote configuration (also referred to as zero-touch provisioning). This process does not require the transfer of PID/PPS IDs, but is initiated automatically after the device's "hello" packet is received by the provisioning server (core server) or after a LANDesk management agent is deployed on the Intel vPro device. An Intel Client Setup certificate from an authorized certificate vendor must be installed on the core server to use remote configuration.

For devices with Intel vPro release 3.0 and later, a "bare metal" or agentless remote configuration is also supported.

Devices with Intel AMT version 1.0 use a similar process but don't use the PID and PPS keys. For details, see Discovering Intel AMT 1.0 devices .

Note that the information in this section is a general description of the Intel vPro configuration process. However, individual manufacturers implement Intel vPro functionality in different ways and there may be differences in such areas as accessing the Intel AMT or ME BIOS screens, resetting the device to factory mode (unprovisioning), or in the way that PID/PPS key pairs are provided. Consult the documentation and support information provided by device manufacturers before you begin the configuration process.

This section includes information about:

- One-touch provisioning for Intel vPro devices
- Importing and exporting key files using a USB drive
- Using static IP addresses with Intel vPro devices
- Remote configuration (zero-touch provisioning)
- Discovering Intel AMT 1.0 devices

One-touch provisioning for Intel vPro devices

This section describes the process of using one-touch provisioning for Intel vPro 2.0 and later.

When an Intel vPro device is received, the IT technician assembles the computer and powers it on. After powering on the device, the technician logs in to the BIOS-based Intel ME (Management Engine) Configuration Screen and changes the default password (admin) to a strong password. This allows access to the Intel AMT Configuration Screen.

In the Intel AMT Configuration Screen, the following pre-provisioning information is entered:

- A provisioning ID (PID)
- A pre-provisioning passkey (PPS) , also known as a pre-shared key (PSK)
- The IP address of the provisioning server
- Port 9971 as the port for communicating with the provisioning server
- Enterprise mode should be selected
- The host name of the Intel vPro device

The PPS is shared by the provisioning server and the managed device, but can't be transmitted on the network for security purposes. It needs to be entered manually on the device (at the Intel AMT Configuration Screen). PID/PPS pairs are generated by Management Suite and stored in the database. You can print a list of generated ID pairs for use in provisioning, or you can export the ID pairs to a key file on a USB drive.

The IT technician should enter the IP address of the Management Suite core server for the Provisioning Server and specify port 9971. Otherwise, by default, the Intel vPro device sends a general broadcast that can be received only if the configuration server is listening on port 9971.

The default username and password for accessing the Intel AMT Configuration Screen are "admin" and "admin". The username stays the same, but the password must be changed during the provisioning process to a strong password. The new password is entered in the Intel vPro general configuration dialog, as described in the procedural steps below. After each device is configured you can change the password individually per device, but for provisioning purposes you use the password that is found in the general configuration dialog.

After the above information is entered in the Intel AMT Configuration Screen, the device sends “hello” messages when it is first connected to the network, attempting to communicate with the provisioning server. If this message is received by the provisioning server, the provisioning process will begin as the server establishes a connection with the managed device.

When the core server receives the hello message and verifies the PID, it provisions the Intel vPro device to TLS mode. TLS (Transport Layer Security) mode establishes a secure channel of communications between the core server and the managed server while the provisioning is completed. This process includes creating a record in the database with the device's UUID and encrypted credentials. When the device's data is in the database, the device appears in the list of unmanaged devices.

When an Intel vPro device has been provisioned by the core server, it can be managed using only Intel vPro functionality. To do this, you can select it in the list of unmanaged devices and add it to your managed devices. You can also deploy management agents to the device to use additional management features.

The recommended process for provisioning Intel vPro devices is as follows. Specific instructions for items 1 and 2 are given in the following procedural steps. If you choose to provision devices with a key file on a USB drive, steps 3-5 below are replaced with the steps described in the section below titled Importing and exporting key files using a USB drive.

1. Specify a new, strong password for provisioning Intel vPro devices. (See detailed steps below).
2. Generate a batch of Intel vPro provisioning IDs (PID and PPS). Print the list of keys or export them to a USB drive. (See detailed steps below).
3. Log in to the device's Intel ME Configuration Screen from the BIOS and change the default password to a strong password.
4. Log in to the Intel AMT Configuration Screen. Enter a PID/PPS key pair from the list of provisioning IDs that you printed. Enter the IP address of the core server (provisioning server), and specify port 9971. Make sure Enterprise mode is selected for provisioning. Enter the host name of the Intel vPro device.
5. Exit the BIOS screen. The device will begin sending "hello" messages.
6. The core server receives a "hello" message and checks the PID against the list of generated keys. If there is a match, it provisions the device.
7. The device is added to the unmanaged device discovery list.
8. Select the device and add it to your managed devices (click **Target** on the toolbar, click the **Manage** tab, then click **Move**). You can choose to manage it as an agentless device, or you can deploy management agents to it for additional management features.

To set the Intel vPro password

1. On the core server, click **Configure > Intel vPro options > General configuration**.
2. Under **Setup and Configuration**, type a strong password and confirm the password.
3. If you have Intel vPro devices that are already being managed and you want to use the same configuration password for those devices, select the **Synchronize this password** option.
4. If you have a highly secure configuration environment and prefer not to use TLS mode for configuring new devices, select the **Use non-TLS communications** option (we recommend that you use TLS mode).
5. Click **OK**.

The new password must be entered here before you can generate a batch of provisioning IDs.

To generate a batch of Intel vPro provisioning IDs

1. Click **Configure > Intel vPro options > ID Generation**.
2. Type the number of IDs to generate (generally the number of devices you plan to provision).

3. If you want to use a different prefix for the PIDs, type it in the **PID prefix** text box. This prefix can only contain uppercase alphabetic characters and numerals in the ASCII character set. You can enter a maximum of 7 characters for a prefix.
4. Type a batch name to identify this group of generated IDs (optional).
5. Click **Generate IDs**.
6. After the IDs have been generated, click **Print ID list** to print the list of IDs. (Only the IDs currently shown in the list are printed.) The Windows print dialog box opens; select a printer and click **Print**.
7. To view all IDs that have been previously generated, select **Show all** in the **View batch IDs** drop-down list.
8. To view one batch of generated IDs, select the batch name in the **View batch IDs** drop-down list.

The provisioning keys are stored in the database for future reference as you provision new Intel vPro devices. As the devices are provisioned and the provisioning keys are consumed, the **Generate Intel vPro IDs** page will display shading for the IDs that have been consumed, so you can track which IDs have been used.

A PID prefix is added for your convenience in identifying the IDs as PIDs, but you are not required to use a prefix. We recommend using 0-4 characters; you can use a maximum of 7 characters for the prefix.

To identify batches of provisioning keys, specify a batch name. This should be a descriptive name that indicates which devices the IDs apply to. For example, you could generate batches for each organization in your company and name the batches Development, Marketing, Finance, and so forth. If you later want to view the generated IDs, you type the batch name and click **View batch IDs** to see a list with only those IDs.

Errors in the provisioning process

If you enter a PID and PPS that are not paired correctly (i.e., the PPS is paired with the wrong PID), you will see an error message in the alert log and provisioning will not continue with that device. You will need to restart the device and re-enter a correct PID/PPS pair in the Intel AMT Configuration Screen.

If, as you type a PID or PPS, the Intel AMT Configuration Screen displays an error message, you have mis-typed the PID or PPS. A checksum is performed to ensure that the PID and PPS are correct.

Importing and exporting key files using a USB drive

You can generate provisioning IDs and export them to a key file for use in provisioning Intel vPro devices with a USB drive. The exported IDs are saved to a setup.bin file that you can copy to a USB drive. With that USB drive you can automatically populate the PID/PPS fields in the Intel AMT BIOS as you provision new Intel vPro devices, before you discover and manage them.

If a device manufacturer provides you with a set of provisioning IDs for the Intel vPro devices you have purchased, you can import those provisioning IDs into the core database so that the core server will recognize those devices as Intel vPro devices and discover them automatically.

These two processes are described below.

Exporting provisioning IDs for use with a USB drive

Management Suite generates provisioning IDs (PID/PPS pairs) that you use to provision new Intel vPro devices. You can print a list of the generated IDs and enter them manually when you provision each device. Alternately you can export the IDs to a setup.bin key file, save that file on a USB drive, and then use the USB drive to provision the devices. This can reduce errors in provisioning because you don’t need to type the IDs manually at each device.

The USB drive you use must be in FAT-16 format for this process to work.

The setup.bin file is created with a specific key file format defined by Intel. When you provision the new Intel vPro device, you connect the USB drive to the device and reboot it. During the boot process a pair of provisioning IDs (PID and PPS) is taken from the setup.bin file and entered into the device's Intel AMT BIOS. When the device sends its “hello” message on the network, the core server will recognize it and be able to communicate securely with it because the provisioning IDs are found in the core database.

To export a batch of provisioning IDs for use with a USB drive

1. Click **Configure > Intel vPro options > Import/Export**.
2. Select **Export AMT IDs to setup.bin file**.
3. For Intel vPro 2.5 or later devices, enter the password you use to access the Intel ME Configuration Screen.
4. Type a number in the **Number of IDs** text box to specify how many IDs to export. You must enter at least "1" in this field. The maximum number you can enter is the number of available IDs indicated next to the **Export AMT IDs to setup.bin file** option.
5. Specify the location of the setup.bin file. Click **Browse** and select the drive and path where you want the file saved.
   You can save the file to any location and then copy the file to a USB drive, or you can simply specify the location of the USB drive if it is connected to the core server. To use the setup.bin file for provisioning, the file must be saved to the root directory of the USB drive.
6. Click **Apply**.
   The dialog box remains open until you click **Close**.

The IDs you generate are listed with other IDs you have generated on the **Generate Intel vPro IDs** page. The IDs will be shaded in the list to indicate that they are not available for provisioning other devices.

To use exported provisioning IDs on new Intel vPro devices

1. Export a batch of provisioning IDs as described above, and save the setup.bin file to the root directory of a USB drive.
2. At each new Intel vPro device, connect the USB drive to the device and reboot it.

As the device boots, it accesses the setup.bin file and takes an available provisioning ID pair (PID and PPS) for use in the provisioning process. It then marks the provisioning ID pair as used so it will not be used by another device. The next device you provision will then take the next available provisioning ID pair.

Note that for this process to work correctly, the default username and password for accessing the Intel AMT BIOS must not have been changed (the default is typically admin/admin). You should not have already entered provisioning IDs on the device.

Importing provisioning IDs from a key file to the core database

If a device manufacturer provides you with a set of provisioning IDs for the Intel vPro devices you have purchased, you can import those provisioning IDs into the core database so that the core server will recognize those devices as Intel vPro devices and discover them automatically. The manufacturer supplies these IDs in a setup.bin key file when you purchase the devices.

To import the IDs into the core database, browse to the location of the setup.bin file that the manufacturer provided (this can be on a CD or DVD, or you can copy the file to any drive). After these IDs are saved to the database, when you start up the Intel vPro devices and they send a “hello” message, the core server recognizes them and discovers the devices.

To import provisioning IDs from a key file to the core database

1. Click **Configure > Intel vPro options > Import/Export**.
2. Select **Import from USB key file**.
3. In the **Specify the location for setup.bin** text box, enter a path or browse to the folder that contains the setup.bin file.
4. Click **Apply**.

The provisioning IDs are added to the core database and are listed on the **Generate Intel vPro IDs** page.

Using static IP addresses with Intel vPro devices

Because Intel vPro devices have two components that are assigned an IP address—the Intel vPro chip and the device’s operating system—you can potentially have two entries in your list of discovered devices for the same Intel vPro device. This happens only if you want to use a static IP address rather than using DHCP.

To use static IP addresses with Intel vPro devices, the Intel vPro firmware should be configured with its own MAC address. (For instructions on how to re-install the firmware and configure it properly, contact Intel.)

Once configured, the Intel vPro device will have a different MAC address, IP address, and host name than the device OS. To be able to manage Intel vPro devices correctly, you need to use the following settings for DHCP and static IP addresses:

- **DHCP**: Both the OS and Intel vPro use DHCP and the host names are the same.
- **Static IP**: Both the OS and Intel vPro are set to use static addresses and they are different from each other, the MAC addresses are different, and the host names are also different.

If an Intel vPro 2.x machine is provisioned in Enterprise mode, the only way to communicate with it is via the “hello” packet being sent to the setup and configuration server. After the machine is managed by LANDesk software, Intel vPro operations may be performed on it like normal. What you should not do is discover and manage the OS IP address; otherwise you will have two computer entries that represent the same computer. Because the only common identifier between the two devices is the AMT GUID, and because the AMT GUID can't be found remotely for the OS device, the two entries can't be merged.

If you want to install the LANDesk agents, you can't push the agents, because the only IP address in the database is the Intel vPro IP address, and the push utility needs access to the OS. Instead, the agents need to be pulled (from the managed Intel vPro device) by mapping a drive to LDLOGON on the core server and running ServerConfig.exe.

Before pulling the agents, we recommend changing a setting in the Configure Services utility:

1. Click **Start > All Programs > LANDesk > LANDesk Configure Services**.
2. On the **Inventory** tab, click **Device IDs** to manage duplicate records.

3. In the **Attributes List**, expand **AMT Information**.
4. Scroll down and move the **AMT GUID** attribute to the **Identity Attributes** list.

   This will force the AMT GUID to be one of the attributes that can uniquely identify a computer.

After you change this setting, when the Inventory scan from the managed Intel vPro device is imported into the database, the Inventory service matches the Intel AMT GUID from the device that’s already in the database with the OS information in the scan file.

Remote configuration (zero-touch provisioning)

This section describes the process for remote configuration of devices with Intel vPro 2.2/2.6 and later.

Remote configuration lets you configure a device in a factory default state through the setup process and then add an Intel AMT profile to make the device ready for out of band management. When the device is first powered on and connected to a network, it begins sending "hello" messages to the Setup and Configuration Server (when you manage devices with LANDesk products, the core server acts as the Setup and Configuration Server). If the Setup and Configuration Server is running, it establishes a secure connection with the Intel vPro device and begins the configuration process.

When this process is successful, the device is added to the list of discovered devices and can then be managed from the core server. Limited management is available with only the Intel vPro functionality, or a management agent can be deployed to the device for full management features.

Remote configuration has two requirements:

- DHCP is required on the network, with a DNS entry identifying the core server as the "ProvisionServer"
- An Intel Client Setup Certificate must be installed on the core server for the domain the core server is installed on (instructions are given below for purchasing and installing a certificate)

Delayed provisioning

If an Intel vPro device is powered on but does not receive a response from the Setup and Configuration Server after a certain period of time (typically 6 to 12 hours, depending on the manufacturer's settings), it stops sending hello packets and waits. At this point Intel vPro functionality is not enabled on the device.

To provision a device in this state, you can install the standard LANDesk management agent on the device. When the agent determines that the device has Intel vPro capabilities it enables Intel vPro functionality on the device and sends a call to the Web service on the core server to receive the "hello" packet. The provisioning process is then initiated from the core server.

Bare metal provisioning

Intel vPro 3.0 and later devices support a bare-metal (or agentless) approach to remote configuration. With the Setup and Configuration Server correctly set up, a DNS entry, and the correct certificate installed on the core server, the configuration process is completed without the use of agents.

If an Intel vPro device is powered on but does not begin sending "hello" messages as described above, remote configuration may not be enabled on the device. This is dependent on the manufacturer enabling remote configuration by setting Manageability Mode to "AMT" on the device. If this appears to be the case, you can deploy a LANDesk management agent to the device to enable the Intel vPro functionality and begin provisioning the device as described under "Delayed provisioning" above.

Obtaining and installing an Intel Client Setup Certificate

An Intel Client Setup Certificate is required on every Setup and Configuration Server. The certificate is valid for one namespace on one domain, so if your core server is used on multiple namespaces within a domain you need to purchase a certificate for each namespace.

The certificate must be purchased from an approved certificate vendor and must be a support class. The following vendors are supported for LANDesk products on the following devices.

Before you purchase a certificate, verify in the vendor's documentation or support information which certificates are supported on your device.

Vendor/Certificate class	Intel devices	Acer devices	Lenovo devices
Go Daddy class 2 CA	X	X	X
VeriSign class 3 Primary CA-G3	X	X	X
VeriSign class 3 Primary CA-G1	X	X	X
Comodo AAA CA	X	X	
Starfield class 2 CA			X

When you purchase a certificate you need to provide a CSR (certificate signing request) file. This file is generated for your LANDesk product along with a private key file. After you receive the certificate files from the vendor, the private key file is saved in a directory with a shared public key file and the certificate file from the vendor. This procedure is described below.

To obtain an Intel Client Setup Certificate

1. Select a vendor and log in to the vendor's web site.
2. Generate a CSR file and private key: In the \Program Files\LANDesk\ManagementSuite\amtprov directory, run AMTProvMgr2.exe with the following arguments:
   ```
   AMTProvMgr2.exe -domainName name.domain.com -country [2-letter country
   code] -state [state name] -city [city name] -organization [organization
   name]
   ```
   The arguments you need to provide may vary depending on the certificate vendor. The domain name you specify should include a namespace. For help information about the arguments and this executable, run the executable from a command prompt with the -h argument.

   This executable saves two files to the amtprov directory: certreq.csr (certificate signing request) and corecakey.pem (a private key file).
3. Open the certreq.csr file in a text editor and copy the contents.
4. At the vendor's web site, paste the contents of the certreq.csr file into the field provided, and complete the application for the certificate.

   After your certificate request is processed the vendor will send you two files: a root certificate file (a common or public file) and a certificate file for the domain you specified.
5. Copy the vendor's root certificate file and rename the copy `trusted_cert.pem`.
6. Copy the vendor's certificate file for your domain and rename the copy `corecacert.pem`.
7. Save the above two files, along with the `corecakey.pem` file (generated in step 2 above), to a folder in LDMAIN\amtprov\certStore\cert_1. You can store up to eight certificates in subfolders named cert_1, cert_2, and so on.

8. If you have additional consoles, copy these three files to the same folder path on each additional console.

Discovering Intel AMT 1.0 devices

When you run a device discovery scan, Intel AMT version 1.0 devices are discovered and added to the **Intel vPro** folder in the **Unmanaged** devices list. The devices are recognized as Intel AMT devices if they have been configured with a secure password that replaces the default set by the manufacturer.

When you add a secure password at the Intel AMT Configuration Screen, you can also enter the IP address of the provisioning server and specify port 9971, as is done with Intel vPro 2.x devices. However, no PID/PPS pairs are used in provisioning Intel AMT 1.0 devices. If you specify a provisioning server IP address, the core server acts as a provisioning server and you can manage the device as an agentless device.

Note that Intel AMT version 1.0 does not use the same level of security as vPro version 2.x. Intel recommends that devices with version 1.0 be configured on an isolated, secure network. After configuration is complete they can be moved to a less secure network for management.

Changing the password for Intel vPro devices

A secure password is required to communicate with and to provision new Intel vPro devices. For devices that you will manage, the password you enter in the Intel AMT Configuration Screen (accessed in the device BIOS) should be the same as the password that you enter in the Intel vPro General Configuration dialog. That password is saved in the database and applied globally for provisioning Intel vPro devices.

Intel vPro requires the use of a strong password to enable secure communications. Passwords should meet these requirements:

- At least 8 characters long
- Includes at least one number character (0-9)
- Includes at least one non-alphanumeric ASCII character (such as !, &, %)
- Contains both upper- and lowercase Latin characters, or non-ASCII characters (UTF+00800 and above)

After provisioning devices, you should regularly change passwords as part of your IT maintenance. You can use a different password for each Intel vPro device, or you can apply a new password to multiple devices. The new passwords you enter are stored in the database and used by Management Suite to communicate securely with managed Intel vPro devices.

To change the password for an Intel vPro device

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro Change Password**.
2. Type the new password, then confirm the password.
3. Click **OK**.

To change the password for all Intel vPro devices

1. On the core server, click **Configure > Intel vPro options > General configuration**.
2. Under **Setup and Configuration**, type a strong password and confirm the password.
3. To apply the password to all managed Intel vPro devices, select the **Synchronize this password** check box.
4. Click **OK**.

Configuring System Defense policies

Intel vPro (versions 2.0 and later) includes a System Defense feature, which enforces network security policies on managed devices. You can select and apply System Defense policies for managed devices.

When a System Defense policy is applied on an Intel vPro device, the device filters incoming and outgoing network packets according to the defined policies. When network traffic matches the alert conditions defined in a filter, an alert is generated and the device's network access is blocked. The device is then isolated from the network until you complete the remediation steps for that policy.

LANDesk Management Suite contains predefined System Defense policies that you can apply to your Intel vPro devices. Each policy contains a set of filters that define what kind of network traffic is not allowed and what the resulting actions are when traffic meets the criteria of the filter.

When a System Defense policy is active on a managed device, the device monitors all incoming and outgoing network traffic. If a filter's conditions are detected, the following occurs:

1. The managed device sends an ASF alert to the core server and an entry is added to the alert log.
2. The core server determines which policy has been violated and shuts down network access on the managed device.
3. The device is listed in the System Defense remediation queue.
4. To restore network access on the device, the administrator follows the appropriate remediation steps and then removes the device from the remediation queue; this restores the original System Defense policy on the device.

This process is described in more detail in the following sections.

Selecting and applying System Defense policies

Management Suite contains the following predefined System Defense policies that can be applied to Intel vPro devices. Policies are defined with parameters such as port number, packet type, and number of packets within a specific amount of time. When you enable a policy, it is registered with Intel vPro on the devices you have selected. Policies are saved as XML files on the managed device, in the CircuitBreakerConfig folder.

- **BlockFTPSrvr:** This policy prevents traffic through an FTP port. When packets are sent or received on FTP port 21, the packets are dropped and network access is suspended.
- **LDCBKillNics:** This policy blocks traffic on all network ports except for the following management ports:

Port description	Number range	Traffic direction	Protocol
LANDesk management	9593-9595	Send/receive	TCP, UDP
Intel vPro management	16992-16993	Send/receive	TCP only
DNS	53	Send/receive	UDP only
DHCP	67-68	Send/receive	UDP only

When the core server shuts down network access on a managed device, it actually applies this policy to the device. Then, when the device is removed from the remediation queue, the original policy is re-applied to the device.

- **LDCBSYNFlood:** This policy detects a SYN flood denial-of-service attack: it allows no more than 10,000 TCP packets with the SYN flag turned on, in one minute. When that number is exceeded, network access is suspended.
- **UDPFloodPolicy:** This policy detects a UDP flood denial-of-service attack: it allows no more than 20,000 UDP packets per minute on ports numbered between 0 and 1023. When that number is exceeded, network access is suspended.
- **RemoveAllPolicy**: Select this to remove all policies, unregistering them with Intel vPro on the selected devices.

To select a System Defense policy for all Intel vPro devices

1. On the core server, click **Configure > Intel vPro options > General configuration**.
2. Under **Default System Defense setting**, select a policy from the list.
3. Click **OK**.

To select a System Defense policy for one Intel vPro device

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro System Defense Policies**.
2. Select a policy from the list.
3. Click **Set Policy**.

Turning on Enhanced System Defense

For devices equipped with Intel vPro 3.0 or later, you can enable Enhanced System Defense. This feature prevents malicious software attacks by continuously inspecting network traffic and evaluating it with enhanced heuristic filtering rules. It identifies and blocks suspicious behavior such as repeated actions generated by worms.

When suspicious behavior is detected, the device causing the problem is isolated from further network communication except for a remediation port, through which Management Suite can reinstate the System Defense policy and restore a network connection after the problem has been resolved.

To turn on Enhanced System Defense for all Intel vPro devices

1. On the core server, click **Configure > Intel vPro options > General configuration**.
2. Under **Default Enhanced System Defense setting**, select **Turn on**.
3. Click **OK**.

To turn on Enhanced System Defense for one Intel vPro device

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro Enhanced System Defense**.
2. Click **Turn on Enhanced System Defense**, then click **Set Configuration**.

Restoring network access to devices in the remediation queue

If a device’s network access is suspended because of a System Defense policy, the device is listed in the remediation queue. It remains there until you remove it from the list, which reinstates the active policy on that device. Before you do that, you need to resolve the issue that placed the device in the queue. For example, if FTP traffic was detected, you need to verify that appropriate actions are taken to prevent further FTP traffic on the device.

To remove a device from the remediation queue

1. Click **Configure > Intel vPro options > System Defense Remediation.**

2. Select the devices that can have their original System Defense policy restored and click **Remediate**.

To remediate devices with Enhanced System Defense, click **Configure > Intel vPro options > Enhanced System Defense Remediation** in step 1 above.

Configuring Intel vPro Agent Presence settings

Intel vPro (release 2.0 and later) includes an Agent Presence tool that can monitor the presence of software agents on managed devices. You can enable Agent Presence monitoring to ensure that management agents on your devices are continually running, and be alerted when an agent stops even when other, software-based, agents can't detect the problem.

LANDesk Management Suite uses Intel vPro Agent Presence to monitor two agents: the standard management agent and the monitoring service. It is useful in situations where normal monitoring communications are not available. For example, a device's communication layer may not be functioning or the monitoring agent itself may have stopped running. By default, Agent Presence also monitors its own monitoring process so you are alerted if it has stopped running.

Agent Presence monitoring is done by configuring a timer that listens for “heartbeat” messages from management agents on the device, to verify that the agents are running. If a timer expires because it has not received a heartbeat message, Intel vPro sends an alert to the core server.

When you set up Agent Presence configuration, the agent on the device registers with Intel vPro to send the heartbeats directly to Intel vPro; if the heartbeats stop, Intel vPro can then alert the core server through out-of-band communication that the device agent is not responding. Intel vPro sends a platform event trap (PET) alert to the core server with a description of the changed state. By default, this alert is logged with device health. You can configure other alert actions to be initiated when this alert is received (for information about configuring alert actions, see Configuring alert rulesets).

When you configure Agent Presence monitoring, you can enable or disable monitoring for two agents and set the following values:

- **Heartbeat:** The maximum amount of time (in seconds) that can pass between heartbeat signals. If this time limit is exceeded without a new heartbeat being received, the agent is considered to be not responding. The default value is 120 seconds for the standard management agent and 180 seconds for the monitoring service; the minimum value for both is 30 seconds.
- **Startup time:** The maximum amount of time (in seconds) that can pass after the operating system starts before a heartbeat must be received from the agent. If this time limit is exceeded the agent is considered to be not responding. Agent Presence is configured on Intel vPro when the agent is installed, so this should allow for enough time for the agent to start running and send its first heartbeat. The default value is 360 seconds; the minimum value is 30 seconds.

To edit the Intel vPro Agent Presence configuration

1. Click **Configure > Intel vPro options > Agent Presence**.
2. To disable Agent Presence monitoring on Intel vPro devices, clear the **Enable Agent Presence monitoring** check box.
3. To disable monitoring for a specific agent, clear the check box next to the agent name.

   Even if both these check boxes are cleared, Agent Presence will continue to monitor its own monitoring process as long as it is enabled.
4. Type a new value in the **Heartbeat** text box to change the maximum allowed time between heartbeats (minimum 30 seconds).

5. Type a new value in the **Startup** text box to change the maximum allowed time for the agent to send its first heartbeat after the operating system starts on the device (minimum 30 seconds; 120 seconds is recommended).

Intel vPro wireless support

Intel vPro devices (version 2.5 and later) with wireless capabilities can be managed out-of-band via a wireless LAN connection when they are powered on and the wireless interface is active. If a notebook is in sleep mode, it can be managed out-of-band only if it is connected to a wired LAN and to AC power.

When the notebook is powered up, the Intel Active Management Technology (Intel AMT) chip on the notebook communicates with the wireless LAN driver. If Intel AMT finds a matching profile, the driver will route traffic addressed to the Intel AMT device. Even if there is a problem with the driver, Intel AMT can receive out-of-band management traffic from the wireless network interface.

For wireless management, an Intel vPro 2.5 notebook needs to have a wireless profile correctly configured by the network administrator so that Intel AMT communication with the notebook is secure. For Intel vPro 2.6 and later notebooks, the wireless profile is not required for most management features, but is required to use serial-over-LAN (SOL) and IDE-redirection (IDE-R) functionality.

For Intel AMT to work with a wireless LAN connection, it must share IP addresses with the notebook. To do this, Intel AMT must be configured to use DHCP and there must be a DHCP server available to allocate IP addresses. If Intel AMT is configured to use static IP addresses, wireless connectivity will be disabled.

LANDesk Management Suite lets you define a wireless profile for Intel Centrino Pro notebooks so you can manage them out of band as described above. When you define a profile you can then deploy it to one or more devices.

To create and deploy an Intel vPro wireless profile

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro Wireless Profiles**.
2. Click **Create Profile**.
3. Under **Profile configuration**, enter the following information:

   Profile name: type a descriptive name that will appear in the **Profile** list.
   SSID: type the wireless network's name.
   Authentication: select a method for managing wireless authentication, either Wi-Fi Protected Access (WPA-PSK) or Robust Secure Network (RSN-PSK).
   Encryption: select an encryption algorithm for wireless communication, either Temporal Key Integrity Protocol (TKIP) or Counter Mode CBC MAC Protocol (CCMP).
   Passphrase: enter and confirm a passphrase or 802.1x profile for authentication.

4. Click **OK**.
5. To edit or delete a profile, select the profile and click **Modify profile** or **Delete profile**.
6. To apply the wireless profile to the device, select the profile in the list and click **Set profile**.
7. To apply the same profile to another Intel vPro device, right-click the device, select **Intel vPro Wireless Profiles**, select the profile from the list, and click **Set profile**.
8. To select a default wireless profile for all newly managed mobile Intel vPro devices, click **Configure > Intel vPro options > General configuration** and select the profile from the **Default wireless profile** list.

When a notebook has been discovered and provisioned while connected to a wired network, it can be managed through the wired network immediately. However, when the notebook switches to a wireless connection there can be a delay before Intel vPro management is enabled for the notebook. This is due to a change in how the computer name is resolved in DNS on the network. The wireless IP address for the notebook is different than the IP address on the wired network, so there is a delay before the new IP address for the notebook matches the computer name.

Intel vPro device management

After an Intel vPro device has been added to the core database to be managed, it can be managed in limited ways even if the device does not have a LANDesk agent installed. (For information on discovering devices and adding them to the core database, see Discovering Intel AMT devices).

The following table lists the management options available for a device that has Intel vPro only compared with a device that has Intel vPro and a Management Suite management agent installed.

	Intel vPro only	Intel vPro and agent	Agent only
Inventory summary	summary	X	X
Event log	X	X	X
Remote boot manager	X	X	
Inventory history		X	X
Remote control		X	X
Chat		X	X
File transfer		X	X
Remote execute		X	X
Wake up		X	X
Shut down		X	X
Reboot		X	X
Inventory scan		X	X
Scheduled tasks and policies	limited	X	X
Group options		X	X

	Intel vPro only	Intel vPro and agent	Agent only
Run inventory report		X	X
Intel vPro alerting		X	X
Network Environment Detection	X	X	
Client-Initiated Remote Access	X	X	

To view the Intel vPro inventory summary for a device

In the **All devices** list, right-click an Intel vPro device and select **Intel vPro options > Intel vPro summary**.

The summary shows general information about the device, such as device name and IP address, as well as information specific to the Intel AMT chip and the Intel vPro device hardware, such as AMT version number, BIOS, manufacturer, and serial number.

Accessing devices provisioned with Enterprise mode

When you provision an Intel vPro device in Enterprise mode, the core server installs a certificate on the device for secure communication. If the device is to be managed by another core server, it must be unprovisioned and then re-provisioned by the new core server. If not, the device's Intel vPro access will not respond because the new core server does not have a matching certificate. Similarly, if any other computer attempts to access the Intel vPro functionality on the device, it will not succeed because it does not have a matching certificate.

Intel vPro event log

Management Suite provides a view of the event log that Intel vPro devices generate. The settings determine what events are captured in this log. You can view the date/time of the event, the source of the event (Entity column), a description, and the severity as determined by the Intel vPro settings (Critical or Non-Critical). You can also export the log data in comma-separated value (CSV format).

To view the Intel vPro event log

1. In the **All devices** list, right-click an Intel vPro device and select **Intel vPro Options > Intel vPro Event Log**.
2. To export the data in a comma-separated value (CSV) file, click the **Export** button on the toolbar and specify a filename.
3. To clear all data in the log, click the **Clear log** button on the toolbar.
4. To update the log entries, click the **Refresh** button on the toolbar.

Intel vPro power options

Management Suite includes options to power on and off Intel vPro devices. These options can be used even when a device's operating system is not responding, as long as the device is connected to the network and has standby power.

When Management Suite initiates power option commands, in some cases it is not possible to verify that the commands are supported on the hardware receiving the command. Some devices with Intel vPro may not support all power option features (for example, a device may support IDE-R reboot from CD but not from a floppy). Consult the hardware vendor's documentation if it appears that a power option is not working with a particular device. You may also check for any firmware or BIOS upgrades from Intel for the device if power options do not work as expected.

For Intel vPro devices, when you issue a power-on command, Management Suite will first send an Intel vPro wake up command. If that command is not successful, it will then send a normal Wake on LAN command to the device.

You can simply turn on or off the device's power, or you can reboot and specify how the device is rebooted. The options are described in the table below.

Power off	Shuts down the power on the device
Power on	Turns on the power on the device
Reboot	Cycles the power off and on again on the device
Normal boot	Starts up the device using whatever boot sequence is set as the default on the device
Boot from local hard drive	Forces a boot from the device's hard drive regardless of the default boot mode on the device
Boot from local CD/DVD drive	Forces a boot from the device's CD or DVD drive regardless of the default boot mode on the device
PXE boot	When restarted, the PXE-enabled device searches for a PXE server on the network; if found, a PXE boot session is initiated on the device
IDE-R boot	Reboots the device using the IDE redirection option selected (see below)
Enter BIOS setup on power on	When the device is booted, it allows the user to enter the BIOS setup
Show console redirection window	When the device is booted, it starts in serial over LAN mode to display a console redirection window
IDE redirection: Reboot from floppy	When the device is booted, it starts from the floppy disk drive that is specified
IDE redirection: Reboot from CD/DVD	When the device is booted, it starts from the CD drive that is specified

IDE redirection: Reboot from specified image file	When the device is booted, it starts from the image file that is specified (floppy image files must be in .img format, and CD image files must be in .iso format; see note below)

To use Intel vPro power options

1. In the **All devices** list, right-click an Intel vPro device and select **Intel vPro Options > Intel vPro Remote Boot Manager**.
2. Select a power command.
3. If you select **Reboot**, select a boot option.
4. If you select the IDE redirection boot method, specify a floppy or CD drive or an image file.
5. If an IDE-R session is still open and you want to close it, click **Close IDE-R session**.
6. Click **Send** to initiate the power command, or click **Close**.

Notes on using IDE redirection options

When using IDE redirection options, floppy image files must be in .img format and CD image files must be in .iso format. Some BIOSes may require the CD image to be located on a hard drive.

Intel vPro normally remembers the last IDE-R settings, but Management Suite clears the settings after 45 seconds, so on subsequent boots it will not restart the IDE-R feature. The IDE-R session on an Intel vPro device lasts 6 hours or until the Management Suite console is turned off. Any IDE-R operation still in progress after 6 hours will be terminated.

In some situations, an IDE-R boot process may appear to time out on the serial-over-LAN (SOL) console, when the boot process is actually still in process. If the boot image takes too long to initialize and send data to the SOL console, the SOL console will stop communicating and keyboard connectivity is lost. This occurs when the media used for booting has a slow response time and takes longer than 60 seconds to initialize (which is the longest timeout value allowed). If you experience this problem when booting with a floppy disk or other media, we recommend that you boot from a boot image (.img) file rather than from a removable media.

Remote access for Intel vPro devices

Intel vPro devices (version 4.0 and later) can be managed remotely from a LANDesk Management Suite console. When an Intel vPro device is outside the network on which the Management Suite console is located, communication to the core server—through the network's firewall and DMZ—is enabled by the remote access functionality.

Remote access for Intel vPro devices enables communication between a management console inside a secure network and Intel vPro devices located outside the network. This communication is through a TLS tunnel that connects the device outside the network with a server (called the Intel vPro Gateway Server) that is typically located in the network's DMZ. Communications to the Intel vPro Gateway Server are in turn sent to the Management Suite core server by secure HTTP connections, using trusted root and server certificates.

For a managed device to use remote access, it must have a remote access policy applied in its firmware. It must also have two certificates, a trusted root certificate and a client certificate, that match the Management Suite core server certificates. (These are the same certificates that are used in LANDesk products.) Remote access features let you create a remote access policy and apply it to the firmware of the managed devices.

When you have configured the device and set up the Intel vPro Gateway Server, remote sessions from the managed device are opened on a regular schedule that you specify (typically once a day). When a remote session is initiated, the device is listed in the Open Session list in the Intel vPro Remote Access Configuration dialog box. In addition, the client status page in Management Suite indicates that the session is open.

Note that as remote access was being developed, it was named Client-Initiated Remote Access, or CIRA. If you see references to CIRA, they refer to Remote Access. The Intel vPro Gateway Server was formerly named the Management Presence Server (MPS), so you may see references to MPS that are related to the Gateway Server. In addition, Intel documentation may refer to Fast Call for Help, which is the remote access option initiated by the client device.

You can enable remote access by using a server in your network to act as an Intel Gateway Server. This requires the following two general tasks:

- Run an installation executable on a server and configure the server for use as an Intel vPro Gateway Server
- Configure Remote Access Configuration and Network Environment Detection options on the Management Suite core server

Documentation for setting up remote access is located on your core server, in the \Programs Files\LANDesk\Management Suite\Install\vpro\remoteaccess folder. (This is the folder where the executable file is found.)

Configuring Dell OMCI devices

This product includes management integration with devices that have Dell OMCI software installed. OMCI (OpenManage Client Instrumentation) is a technology for Dell devices that enables remote management of device status and settings.

When LANDesk Management Suite discovers a Dell device equipped with OMCI, an OMCI tool is enabled in the **Configure** menu of the console. This gives you the ability to use OMCI to change BIOS settings on Dell OMCI devices.

The OMCI configuration process

When you open the Dell OMCI configuration tool, the default settings that are listed are taken from a Dell OMCI device in your **All devices** list. If you select a device first, that device's settings will be used to populate the list of BIOS settings. If you don't select a device, the tool will take the first OMCI device it finds and use its settings.

The BIOS Settings Configuration dialog box lists the BIOS settings that you can change. The current status of each setting is listed, and a **New setting** column lets you select different settings. In addition, you can change the BIOS password and BIOS asset tag.

After you configure these settings, they are saved as a software distribution package. You can then distribute this package to one or more Dell OMCI devices that you manage. The settings are saved as an agent on each device. With some settings, you will receive alerts when the device status changes.

If you don't see the settings that you want to change, those settings may not have been available on the Dell OMCI device that was used to populate the list. Try selecting a different managed device and then click **Configure > Dell OMCI Configuration** to populate the list with the new device's settings.

CAUTION: There are many possible BIOS settings that can be configured using this tool. In some cases, BIOS settings on one Dell device may not be available in the BIOS of another device. You should be careful to select compatible devices when you create a Dell OMCI configuration and distribute it to different devices. If the configuration contains BIOS settings that are incompatible with one of the target devices, unpredictable results may occur.

To configure OMCI settings for Dell devices

1. If you want to specify which Dell OMCI device to use to populate the list of settings, select that device in the **All devices** list.
2. Click **Configure > Dell OMCI Configuration**.
3. To apply only the BIOS settings that you modify in the list, select **Apply only modified settings to targeted clients**. To apply the full set of BIOS settings to the targeted devices, select **Apply all settings to targeted clients**.
4. In the list of BIOS settings, change the setting for each item you want to modify. In the **New setting** column, click the down arrow to select from a list of options.
5. To change the BIOS password, select **Set the BIOS password**. Type the new password and confirm it. To clear the BIOS password, clear both text boxes.
6. To change the BIOS asset tag for the device, select **Set the BIOS asset tag** and type the new tag in the **Asset tag** text box.
7. Click **OK** to save the configuration.
   A distribution package is created with the settings you have changed. To apply the configuration to Dell OMCI devices you manage, schedule the distribution package to the targeted devices.
8. Click **Tools > Distribution > Distribution Packages**.
9. Select the package in the **All packages** list. It is named **Dell OMCI BIOS Settings - <date - time>**.
   You can rename the package to identify which settings are configured, or to describe which devices it applies to.
10. Right-click the package and select **Create scheduled task**.
11. The package is listed in the **Scheduled tasks** tool. From the network view, drag each Dell OMCI device onto the OMCI package.
12. Right-click the package and select **Properties** to view the package properties.
13. Click **Delivery method** and select **Push** as the **Delivery type**, then select **Standard push** distribution as the **Delivery method**. Click **Save**.
14. Right-click the package and select **Start now**.
    As the distribution task progresses, the package status will change. When the distribution has completed, it will show the number OFdevices that were successful or that failed in the distribution task.

After the package has successfully been distributed, you can restart any of the devices you reconfigured and enter the BIOS setup to view that the changes were made.

Managing Dell DRAC devices

LANDesk Management Suite includes management integration with devices that have a Dell Remote Access Controller (DRAC). The DRAC is a remote hardware controller that provides an interface to the IPMI-compliant server management hardware on the Dell device. The DRAC has an IP address assigned to it, which is used to identify the DRAC device in device discovery and in managing the device.

Devices that contain a Dell DRAC can be managed with the same functionality as other IPMI-compliant devices. When the device has been discovered and added to the list of managed devices, it is managed as any other IPMI device. In addition, Management Suite has unique Dell DRAC features.

The OpenManage Server Administrator is a Web-based console provided by Dell for managing the Dell DRAC device. Normally it is accessed by typing the IP address of the DRAC in a browser and logging in with a username and password. When a Dell DRAC device is managed with Management Suite you can also open this utility directly from the Management Suite interface.

In addition, Management Suite lets you manage usernames and passwords for accessing the OpenManage Server Administrator, and displays three logs from this utility in the server information console.

To open the OpenManage Server Administrator for a Dell DRAC device

1. In the Management Suite network view, right-click the Dell DRAC device and select **Real-time inventory and monitoring**.
2. In the real-time inventory console, expand **Hardware** and click **Dell DRAC**. The device's IP address and other identifying information is displayed.
3. Click the **Launch** button for **Dell DRAC utility** to open the device's DRAC utility, or click the **Launch** button for **Dell DRAC power management** to open the device's OpenManage Server Administrator in a new window.

Dell DRAC logs available in Management Suite

Three logs from the OpenManage Server Administrator utility are displayed in the Management Suite real-time inventory console.

- **Dell DRAC log:** Tracks all events recorded by the Server Administrator, such as login activity, session status, firmware update status, and interaction between the DRAC and other device components. Information displayed in Management Suite includes event severity, description, and suggested corrective actions for errors.
- **Dell DRAC command log:** Tracks all commands issued to the Server Administrator. It shows what commands were performed, by whom, and when, including attempts to log in and out and access errors.
- **Dell DRAC trace log:** Useful for tracing details about network communication events, such as alerting, paging, or network connections from the DRAC.

To view logs for a Dell DRAC device

1. In the Management Suite network view, right-click the Dell DRAC device and select **Real-time inventory and monitoring**.
2. In the real-time inventory console, expand **Logs**.
3. Click **Dell DRAC log**, **Dell DRAC Command log**, or **Dell DRAC trace log**.

Managing usernames for Dell DRAC-enabled devices

To access the OpenManage Server Administrator interface you log in with a username and password that is defined for the device. The default **root** user is the first user in the list and can't be deleted, but its password can be changed. Up to 15 additional users can be added. While DRAC usernames can have different access levels, Management Suite only defines usernames at the Administrator level.

To add or edit usernames and passwords for a DRAC-enabled device

1. In the Management Suite network view, right-click the Dell DRAC device and select **Real-time inventory and monitoring**.
2. In the real-time inventory console, click **Hardware configuration**.
3. In the hardware configuration console, expand **Dell DRAC configuration** and click **Dell DRAC users**. A list of currently defined users appears.

4. To change the password for a user, click the user number and click **Change password**. Type and confirm the new password, then click **Apply**. (To assign the same password to multiple users, select them using Ctrl+click or Shift+click.)
5. To add a user, click **Add user**. Type a username and password and confirm the password, then click **Apply**. The user is added to the list.

   If you type a username that is already in the list, the new password you specify will overwrite the existing password for that user name; a second user with that name is not added to the list.

6. To delete a user, click the user number and click **Delete user**, then click **OK**. (To delete multiple users, select them using Ctrl+click or Shift+click.)

All users in this list have Administrator level access to the OpenManage Server Administrator.

IPMI support

LANDesk Management Suite includes support for Intelligent Platform Management Interface (IPMI) 1.5 and 2.0. IPMI is a specification developed by Intel, Hewlett-Packard, NEC, and Dell to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that let you access many features regardless of whether or not the machine is powered on, or what state the OS may be in. For more details on IPMI, visit Intel's Web site.

IPMI monitoring is handled by the BMC (baseboard management controller). The BMC operates on standby power and autonomously polls system health status. If the BMC detects that any elements are out of range, you can configure the resulting IPMI actions, such as logging the event, generating alerts, or performing automatic recovery actions such as system power-down or reset.

You must have SMBIOS 2.3.1 or higher installed in order for the BMC to be detected on the system. If the BMC is not detected, you may not see some IPMI information in reports, exports, and so forth.

IPMI defines common interfaces to the hardware used to monitor physical health characteristics, such as temperature, voltage, fans, power supplies, and chassis intrusion. In addition to health monitoring, IPMI includes other system management capabilities including automatic alerting, automatic system shutdown and restart, remote restart and power control capabilities, and asset tracking.

The Management Suite menu choices vary slightly for an IPMI-enabled device, depending on the state of the operating system.

Management features for IPMI-enabled devices

Monitoring capabilities depend on what has been installed on the device being monitored, as well as the state of the device. Any IPMI-enabled device with a baseboard management controller (BMC) can be monitored by the administrator console in limited ways with no additional management agents after the BMC has been configured. This includes out-of-band management when the device is powered down or the OS isn't functional. Full-featured management is available when the management agent is installed, a BMC is present, the device is powered on, and the OS is functional. The table below compares the functionality available with these different configurations.

	BMC only*	BMC + agent	Agent (no IPMI)
Out-of-band management enabled	X	X	
In-band management enabled		X	X
Device can be discovered**	X	X	X
Read environment sensors	X	X	Hardware dependent
Power on/off remotely	X	X	X
Read & clear event log	X	X	
Configure alerts	X	X	X
Read OS information		X	X
Graceful shutdown		X	X
Read SMBIOS information (processor, slots, memory)		X	X
IP syncing (OS to BMC)		X	
Watchdog timer		X	
BMC communicates with core server	X	X	
Local Management Suite components communicate with core server		X	X
Full range of Management Suite management features		X	

*Standard BMC. The mini BMC is a scaled-down version of a baseboard management controller. It has the functionality listed above, with limitations such as the following:

- Does not support serial over LAN (SOL redirection)
- Has only one username for BMC management
- Uses only one channel for communicating with the BMC

- Has a smaller system event log (SEL) repository

**If the BMC is not configured, it will not respond to ASF pings which the product uses to discover IPMI. This means that you will have to discover it as a normal computer. When you deploy a management agent, the server configuration executable will scan the system and detect it is IPMI and configure the BMC.

Conflicts with IPMI drivers

When you install this product on an IPMI device, if that device already has a hardware-specific IPMI driver installed, and if that driver is supported by this product, that driver will be used.

If there is no IPMI driver on the device, Management Suite will install the OSA IPMI driver.

If you have installed other management software that includes IPMI drivers on devices you want to manage with this product, you may need to uninstall those products before you can deploy Management Suite agents with IPMI management features.

For example, Microsoft Windows Server 2003 includes IPMI support through the installation of Windows Remote Management (WinRM), which includes a Windows Management Instrumentation (WMI) provider and an IPMI driver. However, Management Suite does not support the installation of that IPMI driver and installs its own IPMI driver. If WinRM has been installed on a device that you want to manage with Management Suite, you must first uninstall WinRM through Windows Add/Remove Programs (**Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components > Management and Monitoring Tools >** clear the **Hardware Management** check box > click **OK**).

IPMI BMC configuration

Use the **IPMI BMC configuration** page to customize settings for communicating with IPMI-enabled devices. The features described below are available for in-band devices; if a device is out of band, only the power configuration and BMC user settings are available.

It is strongly recommended that you do not change IPMI settings unless you are familiar with the IPMI specification and understand the related technologies involved in these settings. Improper use of these configuration options may prevent Management Suite from successfully communicating with IPMI-enabled devices.

The following configuration options are available:

- "Changing watchdog timer settings" on page 539
- "Changing power configuration settings" on page 540
- "Changing BMC user settings" on page 540
- "Changing the BMC password" on page 541
- "Changing LAN configurations" on page 541
- "Changing Serial Over LAN (SOL configurations)" on page 543
- "Changing IMM configurations" on page 543

Changing watchdog timer settings

IPMI provides an interface for the BMC watchdog timer. This timer can be set to expire periodically, and is configured to initiate certain actions if it expires (such as power cycling). Management Suite is configured to reset the timer periodically so it does not expire; if the device becomes unavailable (for example, it is powered down or hangs), the timer is not reset and it then expires, which initiates the action.

You can specify how much time to allow before the timer expires and select an action to perform if it does expire. You can choose to take no action, do a hard reset (shut down and restart of the device), power down the device gracefully, or run a power cycle (power down gracefully and then start up again).

You can also set the BMC to stop broadcasting ARP (Address Resolution Protocol) messages while the watchdog timer is enabled, which can reduce the amount of network traffic being generated. If you suspend ARPs, they will automatically resume if the watchdog timer expires.

To change watchdog timer settings

1. In the Management Suite network view, right-click the IPMI device and select **Real-time inventory and monitoring**.
2. In the left navigation pane of the real-time inventory console, click **Hardware configuration**.
3. Expand **IPMI BMC configuration** and click **Watchdog timer**.
4. Select **Turn on the watchdog timer** to enable the timer.
5. Specify the frequency of checking the timer (number of minutes or seconds).
6. Select an action to initiate when the watchdog timer expires.
7. If you want the BMC to stop broadcasting ARP messages while the watchdog timer is enabled, select **Suspend BMC ARPs**.
8. Click **Apply**.
9. If you have changed the watchdog timer settings, you can revert to the default settings by clicking **Restore defaults**.

Changing power configuration settings

When power is lost on an IPMI-enabled computer, you can specify what action should be taken when power is restored. We recommend that you restore the computer to whatever state it was in at the time power was lost, but you can also choose to keep it powered off or always power up the computer.

To change power configuration settings

1. In the Management Suite network view, right-click the IPMI device and select **Real-time inventory and monitoring**.
2. In the left navigation pane of the server information console, click **Hardware configuration**.
3. Expand **IPMI BMC configuration** and click **Power configuration**.
4. Select an option for when power is restored.
5. Click **Apply**.
6. If you have changed the power configuration settings, you can revert to the default settings by clicking **Restore defaults**.

Changing BMC user settings

Management Suite authenticates to a BMC with a user name/password combination that is unique to the BMC (separate from any other Management Suite user names). Management Suite reserves the first user name so it can always communicate with the BMC. If the BMC allows other user names to be defined, you can define user names with passwords for BMC authentication.

You can also specify privilege levels for each user. For advanced IMMs, you can specify protocol privilege levels (telnet, http, and https) for each channel.

CAUTION: Use extreme caution when making changes to these settings. Erroneous settings can disable the device's BMC communication with this product.

To change BMC user settings

1. In the Management Suite network view, right-click the IPMI device and select **Real-time inventory and monitoring**.
2. In the left navigation pane of the server information console, click **Hardware configuration**.
3. Expand **IPMI BMC configuration** and click **User settings**.
4. To clear the data for a user name, click the index number and click **Clear**.
5. To add or change a username, click the index number and click **Edit**.
6. Type a user name.
7. To set a password, select the **Set password** check box, then type the password and confirm it.
8. Select the privilege levels for LAN and serial access.
9. Click **Save changes**.

Changing the BMC password

Management Suite authenticates to a device's BMC using the default user name (user 1 and password). You can't change the user name but you can change its password. When you change this password setting, the change is saved in the database and on the BMC.

To change the default BMC password

1. In the Management Suite network view, right-click the IPMI device and select **Real-time inventory and monitoring**.
2. In the left navigation pane of the server information console, click **Hardware configuration**.
3. Expand **IPMI BMC configuration** and click **Password**.
4. Type the new password and then confirm it.
5. Click **Apply**.

Changing LAN configurations

IPMI messages can be carried directly from the BMC over a LAN interface in addition to the device's system interface. Enabling LAN communication allows the core server to receive IPMI-specific alerts even if the device is powered down. The core server maintains this communication as long as the device has a physical network connection with a valid network address, and as long as the device's main power remains connected.

If you choose to set custom configuration for LAN or serial communication to the BMC, use extreme caution when making changes to the settings. Erroneous settings can disable the device's BMC communication with this product.

If you have a LAN channel defined, you can use the default settings for the device's BMC, or you can change the IP address and gateway settings. Use these options to configure destinations for the SNMP traps sent by the BMC for each platform event trap (PET) event.

You can also change SNMP community string settings for sending alerts over LAN. When configuring these settings, you must specify the SNMP community string used for SNMP authentication. For each configuration, you can edit the trap destination information to specify where and how traps are sent, and whether they are acknowledged.

To set properties for LAN channel configuration

1. In the Management Suite network view, right-click the IPMI device and select **Real-time inventory and monitoring**.
2. In the left navigation pane of the server information console, click **Hardware configuration**.
3. Expand **IPMI BMC configuration** and click **LAN configuration**.
4. Select **Always available** in the LAN communication drop-down list to keep access to the BMC open. If you select **Disabled** you will not have LAN access to the BMC when the device is out of band.
5. Select the **User privilege level** for the channel: **Administrator-level** has access to all commands, while **User-level** is limited to read-only access (you will have a restricted feature set if you select User-level).
6. Select **Permanently turn off BMC ARPs** to turn off Address Resolution Protocol messages from the BMC. This reduces network traffic but can prevent communication with the BMC when the device is out of band.
7. Select **Turn off ARP responses** to stop the BMC from sending ARP message responses when the OS is not available. If you enable this setting you might prevent communication with the BMC when the device is out of band.
8. IP settings for the LAN channel are automatically set if the BMC is in sync with the OS channel. If not, the check box under the **IP settings** tab is selected. You can leave the box selected to use DHCP settings provided automatically, or you can clear the check box and edit the text fields with static settings. It is generally preferable to use automatic settings.
9. Click the **Send alerts over LAN** tab to configure SNMP community string settings (see details below).
10. Click **Apply** to save your changes.

If you click the **Restore defaults** button on this page, the settings under the **Properties for LAN channel** heading are reset to their default values, but other settings on the page are not changed. If you change any data on the **IP settings** tab and click **Apply**, you would need to manually reset those settings.

To change Send alerts over LAN properties

1. Open the **LAN configuration** page (steps 1-3 above).
2. Click the **Send alerts over LAN** tab.
3. Select the **Enabled** check box to enable sending SNMP alerts.
4. Specify the **SNMP community string** to be used for SNMP authentication.
5. To configure the trap destinations, double-click the index number to open a **Properties** dialog box.
6. Select **Enable this alert destination**. Specify the IP address to which the BMC will send alerts, as well as the corresponding MAC address.
7. Specify the number of times to retry, how frequently to retry, and the preferred gateway to use.
8. If you want the alerts to be acknowledged (which increases the amount of network traffic that is generated), select the **Acknowledge alerts** check box.
9. Click **OK**.
10. At the LAN configuration page, click **Apply** when all settings are complete.

Changing Serial Over LAN (SOL configurations)

Use SOL (Serial Over LAN) configuration options to customize serial modem settings for special uses, such as redirecting BIOS POST messages to the serial port. If the BMC is required to dial out over a modem connection, specific modem settings such as initialization strings and dial strings must also be specified.

For serial modem operation, you may need to configure the device board's BIOS and jumper settings. See the documentation for the particular device for details.

If you choose to set custom configuration for LAN or serial communication to the BMC, use extreme caution when making changes to the settings. Erroneous settings can disable the device's BMC communication with this product.

To change SOL configuration settings

1. In the Management Suite network view, right-click the IPMI device and select **Real-time inventory and monitoring**.
2. In the left navigation pane of the server information console, click **Hardware configuration**.
3. Expand **IPMI BMC configuration** and click **SOL configuration**.
4. Select **Turn on Serial-over-LAN communications** to enable SOL.
5. Select the minimum **User level required to activate SOL**.
6. Select the **Baud rate for SOL sessions** that is appropriate to the device's hardware configuration.
7. Click **Apply**.

Changing IMM configurations

The **IMM configuration** page is displayed only for IPMI devices that are equipped with an advanced IMM add-in card. The options on this page let you enable or disable protocols and features for use with the IMM-enabled device. Consult the manufacturer's documentation for the IMM before you make changes to these settings.

To change IMM configuration settings

1. In the Management Suite network view, right-click the IPMI device and select **Real-time inventory and monitoring**.
2. In the left navigation pane of the server information console, click **Hardware configuration**.
3. Expand **IPMI BMC configuration** and click **IMM configuration**.
4. Select the boxes for protocols and features that you want to enable, and add any settings that are required. Available options include:
    - KVM
    - SNMP
    - telnet
    - SMTP alerting
    - HTTP
    - HTTPS
5. Click **Apply**.

File replicator

The LANDesk file replicator is a utility designed to replicate files from a remote Web server to the local system. It provides the following features:

- **File and directory support:** Replicate individual files or directories. Directory support can be recursive.
- **Multiple task support:** Multiple download tasks can be defined and run simultaneously. Each task can download resources located in different Web servers.
- **Bandwidth control:** A maximum bandwidth in percentage or actual transmission rate can be specified that will not be exceeded during the replication operation.
- **Restartable copying:** If a copy operation is interrupted because the connection is lost or time runs out, replication will resume from the point where it was interrupted when the job is relaunched.

Your Web server must be configured properly for the file replicator to work:

- The Web server's directory browsing option must be enabled.
- Some application extensions, such as .ASP and .ASPX, have special meanings in the Web server. You must remove the application extension for these kinds of files if you want to replicate them from a Web server.

Using the file replicator

The file replicator copies files from Web sites or Web shares to a folder you specify. You can create periodic repeating tasks or single tasks that run on a schedule you specify. The file replicator uses the same HTTP transfer technology that Management Suite uses for software distributions. You can limit the transfer bandwidth by kilobytes per second or by a percentage of available bandwidth.

Management Suite setup copies the file replicator to this folder:

- \Program Files\LANDesk\ManagementSuite\Utilities\File Replicator

The replicator is a standalone Windows application and you can copy the File Replicator folder and subfolders to any server you want. If you want to access the online help, also copy ldms.chm to the same place. The default .NET Framework security configuration won't allow the file replicator to launch from a remote path. If you try to run the program remotely, nothing will happen.

To configure a replication task, you need to provide the following:

- Task parameters, such as the schedule, target folder, and bandwidth options
- Source URLs. If you specify multiple URLs, they are processed one at a time.

The file replicator caches files in the **Temporary folder** box. Once the copy finishes to the temporary directory, the replicator copies the file to the destination and deletes it from the temporary directory. This prevents partial copies from ending up on the destination if the file copy from the source is interrupted for some reason.

The file replicator stops whatever it's doing when it's opened. When you're done with the window, make sure you click **Start download**. This minimizes the replicator to the system tray and allows replication tasks to execute.

The file replicator configuration file, stored in XML format, needs to be created before you can do any replication tasks. There is no default XML configuration file. This XML configuration file can be the same or different on each server.

If the user logs off, the file replicator process in the system tray terminates. Usually with servers, file replicator must be launched when a user is not logged in. This can be done using Microsoft's Task Scheduler service or LANDesk's Local Scheduler service, as described in "Scheduling replication from the command-line" on page 546.

To create a replication task

1. Launch the file replicator (\Program Files\LANDesk\ManagementSuite\Utilities\File Replicator\LANDeskFileReplicator.exe)
2. From the **New** button's menu, click **New periodic task** or **New single task**.
3. Enter a task **Name**.
4. Enter or **Browse** for the **Destination folder**.
5. Enter or **Browse** for the **Temporary folder**.
6. Set the time you want the replication task to occur. If the task doesn't finish in the time allowed, it will resume from the point it left off the next time the task runs.
7. Select the bandwidth options you want. You can specify a value in kilobytes per second, a percentage of available bandwidth, or none.
8. Click Add to enter source URLs. The address must be in the form of http://server/path. If necessary, specify the credentials necessary to access the URL. When you're ready, click **Browse**. If the URL and credentials work, you'll see the destination in the lower half of the dialog. Check **Download recursively** if that's what you want. Click OK when you're done.
9. Repeat step 8 for each URL you want to replicate.
10. Click **Save** when you're done.
11. When you're done configuring tasks, click **Start download** to activate file replication on the schedule you specified. The file replicator minimizes to the system tray.

The file replicator stores a log of its actions.

To view the file replicator log

1. Launch the file replicator.
2. Click the **View log** toolbar button.

You can reschedule a single task. This resets the task so it will run again.

To reschedule a task

1. Launch the file replicator.
2. Select the single task you want to reschedule.
3. Click the **Reschedule task** toolbar button.

Understanding the bandwidth options

The file replicator uses bandwidth options to make sure replication doesn't saturate a device's available bandwidth. Any bandwidth options you specify apply to the device the replicator is copying files from, not the destination. There are two bandwidth options the replicator can use:

- **Value(KB):** The amount of bandwidth, in kilobytes/sec, that the job can use. Values must be in the range of 2 to 10000.

- **Percentage(%):** The amount of network bandwidth. Values must be in the range of 5 to 100.

Bandwidth options are set on a per-job basis. If you have multiple file replication jobs active at once, the job bandwidth settings can interact. For example, if you have one job that's allowed 100 KB/sec second, and another that's allowed 50 KB/sec, the total bandwidth used if the two jobs are active at the same time will be 150 KB/sec. With percentage of available bandwidth, it's slightly more complicated. If you have two jobs that are allowed 50% of available bandwidth, the total bandwidth used by both jobs won't exceed 50% of the total. Each job will end up with about 25% of the available bandwidth.

Scheduling replication from the command-line

Management Suite ships with two file replicator versions:

- The graphical version (LANDeskFileReplicator.exe), which only runs when a user is logged on.
- The command-line version (LANDeskFileReplicatorNoUI.exe), which you can run from Microsoft's Task Scheduler or the Management Suite local scheduler. Running the file replicator this way doesn't require a logged-on user.

The graphical and command-line file replicators use the same XML-format configuration file. Before using the command-line file replicator, you need to use the graphical file replicator to create an XML configuration file.

The following is the syntax for LANDeskFileReplicatorNoUI.exe:

```
LANDeskFileReplicatorNoUI.exe configfile [logfile]
```

Here is an example:

```
LANDeskFileReplicatorNoUI.exe LDHTTPCopyTaskConfig.xml replicator.log
```

The following sections describe to ways you can schedule LANDeskFileReplicatorNoUI.exe from the command-line.

- "Scheduling replication using the Local Scheduler service" on page 546
- "Scheduling replication using the Microsoft Task Scheduler service" on page 547

The examples in the steps below assume that each package server has two hard drives: the C drive for the operating system; and the D drive for data storage. It also assumes that each server is configured to have a web share named Packages that has a local patch of D:\Packages.

Scheduling replication using the Management Suite Local Scheduler service

The Management Suite Local Scheduler service is installed with the Management Suite agent configuration. The file used is LocalSch.exe. If your server isn't managed by Management Suite, this service won't exist and you'll have to use the Microsoft task scheduler instead. For more information on the local scheduler, see "Using the local scheduler" on page 127.

Once you've copied the file replicator files and XML configuration file to your server, enter the following at a command prompt to schedule replication to occur every 20 minutes:

```
"%programfiles%\LANDesk\LDClient\LocalSch.exe" /taskid=1 /freq=1200
/exe="%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File
Replicator\LANDeskFileReplicatorNoUI.exe"
/cmd="""%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File
Replicator\LDHTTPCopyTaskConfig.xml""
""%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File Replicator\replicator.log"""
```

Note that the three quotes after /cmd= in the examples below is not a mistake. Three quotes are required to handle parameters that include quotes themselves.

To change the launch interval, change the /freq= parameter's value to the number of seconds you want. In the example above, 1200 seconds equals 20 minutes.

To verify that a task was created, run the following command:

```
"%programfiles%\LANDesk\LDClient\LocalSch.exe" /tasks |more
```

Scheduling replication using the Microsoft Task Scheduler service

You can also control Microsoft's task scheduler from the command-line with the SCHTASKS command. SCHTASKS can schedule LANDeskFileReplicatorNoUI.exe to run almost any time.

For more information on SCHTASKS, see:
http://technet2.microsoft.com/windowsserver/en/library/1d284efa-9d11-46c2-a8ef-87b297c68d171033.mspx?mfr=true

Once you've copied the file replicator files and XML configuration file to your server, do the following to schedule replication to occur at the interval you want (the example below uses every 20 minutes).

To schedule replication every 20 minutes with Microsoft's task scheduler

1. In the %ProgramFiles%\LANDesk\File Replicator directory, create a batch file called “File Replicator.cmd” that contains the following line.

   ```
   "%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File
   Replicator\LANDeskFileReplicatorNoUI.exe"
   "%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File
   Replicator\LDHTTPCopyTaskConfig.xml"
   "%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File
   Replicator\replicator.log"
   ```

2. Open a command prompt on the package server by clicking **Start > Run** and typing **CMD**.
3. Enter the following command.

   ```
   schtasks /create /ru system /sc minute /mo 20 /tn "File Replicator every
   20 minutes" /tr "%ProgramFiles%\LANDesk\File Replicator\File
   Replicator.cmd"
   ```

   Note: The commands should be entered as a single command line.

4. To verify that the task was created, run SCHTASKS with no parameters and the task details are displayed.

If you want to schedule hourly replication, change the schtasks command-line above to the following:

- schtasks /create /ru system /sc hourly /tn "File Replicator hourly" /tr "%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File Replicator\File Replicator.cmd"

If you want to schedule daily replication, change the schtasks command-line above to the following:

- schtasks /create /ru system /sc daily /tn "File Replicator daily" /tr "%ProgramFiles%\LANDesk\ManagementSuite\Utilities\File Replicator\File Replicator.cmd"

Thin clients

LANDesk Handheld Manager provides extensive inventory management and software distribution for thin clients. For additional information on LANDesk Handheld Manger, see the Handheld Manager help section.

Note: This product installs with Management Suite automatically. It only needs to be activated.

Thin clients running Windows CE

Windows CE Thin client requirements

- Neoware E100 (ce5)
- HPT5520 (ce5)
- Intel X86 for thin clients

To install the LANDesk agent on thin client devices running Windows CE

Neoware E100 (ce5)

1. From the Neoware thin client, open an Internet Browser such as Internet Explorer.
2. Enter in http://[core name]/ldhm-clients
3. Click the **neoware-ce5** link.
4. Then select the **newoare-ce5.CAB** link.
5. Click Run **this program from its current location**. Click **OK** to install the CAB file.
6. The agent is installed to the \diskonchip directory, which is a hidden directory.

HPT5520 (ce5)

1. From the HP thin client, open an Internet Browser such as Internet Explorer.
2. Enter in http://<core name>/ldhm-clients
3. Click the **hpt5520-ce5** link.
4. Click the **hpt5520-ce5.CAB** link.
5. Click **Run this program from its current location**. Click **OK** to install the CAB file.
6. The agent is installed to \Hard Disk\LANDesk

To uninstall the LANDesk agent from an HP device, go to **Start > Settings > Control Panel |View or Remove Programs**. Click **LANDesk Software, Ltd.**. from the list of applications and click **Remove**.

Distributing registry files to Windows CE devices

You can send .REG registry files directly to Windows CE devices. The format of these files matches the standard Windows registry export format with two exceptions. Instead of the normal Windows registry format header, the first line of Windows CE-based .REG files must start with one of the following strings:

- **LDHM Generic Registry File:** Installs to all Windows CE devices
- **LDHM Handheld Registry File:** Installs only to handheld Windows CE devices
- **LDHM Thin-client Registry File:** Installs only to thin client Windows CE devices

- **LDHM <DeviceType> Registry File:** Installs only to the device type specified.

Thin clients running Microsoft Windows XP Embedded OS

For thin clients running the Microsoft Windows XP Embedded OS, the standard desktop agent that is installed on any Windows desktop is used instead of the Windows CE agent. The LANDesk Windows Configuration can be run on a thin client running XP Embedded the same way it would be installed on a standard desktop client machine. Most of the LANDesk agent features available on Windows XP desktop device will work on a thin client device running Windows XP Embedded. For example, hardware and software scanning, remote control, and software distribution will all work on an EX embedded thin client device.

Features supported for thin clients running XP embedded OS:

- Unmanaged device discovery
- Agent pull
- Hardware Inventory scanning
- Software Inventory scanning

NOTE: Delta scans for both software and hardware scanning will not work on thin clients that use a write filter (such as the Wyse s90 device) when the write filter is enabled. Management Gateway via Remote Control

- Remote Control
- Software Distribution

NOTE: the Wyse write filter must be disabled in order to perform a Software Distribution task on a XP embedded thin client. If the filter is enabled, a falsely successful distribution may be reported.

- Extended device discovery

Working with thin client configurations

Handheld Manager's Windows CE thin client support includes the following features:

- Creating and deploying thin client agent configuration .CAB files in the **Windows CE agent configuration** window
- Creating and deploying custom Windows CE thin client configurations in the **Thin-client configuration** window

Custom Windows CE thin client configurations allow you to customize the thin client initial connection manager dialog. Each Handheld Manager thin client configuration can add up to three configuration entries:

- **Internet Explorer**: Launches an Internet Explorer session with start page, search page, and cache size you specify. Appears in the thin client's connection manager as "Preset_IE_Configuration."
- **Remote Desktop**: Launches a Remote Desktop connection with the server and options you specify. Appears in the thin client's connection manager as "Preset_RDP_Configuration."
- **Citrix ICA**: Launches a Citrix ICA connection with the server and options you specify. Appears in the thin client's connection manager as "Preset_ICA_Configuration."

You can only deploy one configuration at a time to thin client devices. There can only be one of each entry type (Internet Explorer, Remote Desktop, and Citrix ICA). You can't change the default name that appears in the thin client's connection manager. Once you create a configuration, you can't go back and edit it. If you need to make changes to an existing configuration, create a new configuration and include the changes you want.

Once you have a configuration, deploy it by following the directions below. The thin client configuration files are stored on the core server in the \Program Files\LANDesk\ManagementSuite\LDHM\packages folder. This corresponds to the following Web share: http://<core server>/ldhm-packages.

To distribute software to a thin client device

1. Copy the program you want to install to a Web share. The default share location on the core server is \Program Files\LANDesk\ManagementSuite\LDHM\Packages. This corresponds to the following Web share: http://<core server>/ldhm-packages.
2. Click **Tools > Distribution > Scheduled tasks**, and click the **Schedule thin client task** button. Browse to the program you want to install and click **Next**.
3. Enter a **Script name** and click **Next**.
4. Adjust the download options you want and click **Next**.
5. Finish the wizard.
6. From the network view, drag handheld clients that you want to receive the package to the task you created in the **Scheduled tasks** window.
7. From the task's shortcut menu, click **Properties** and configure the task or select **Run now**. Once the start time arrives, the job status will change to **Working** and the job results will change to **Policy has been made available**, indicating that the file has been made available to the handheld the next time the handheld distribution agent runs (the default is once an hour). You can force the agent to run by running wcesdclnt.exe on the handheld.

Scanning for custom registry settings for Wyse thin clients running Windows CE

Handheld Manager’s inventory scanner allows you to customize which registry settings are scanned for on thin clients. This feature is supported for Wyse thin client devices running Windows CE. To scan for custom registry settings, create a text file named “ldcustkeys.ini”. In this text file, enter in the registry settings that the inventory scanner should scan for. For example:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ActiveSync\Address\IP
; \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Color\BaseHue
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AirSync\Restriction
```

- To comment out a line, begin the line with semicolon
- Each registry key should be on a line by itself
- Incorrect registry keys will be ignored

Supported registry types include:

- String Value
- Multi String Value (Multi strings will separated by a comma)
- Binary Value (will be display in Hex format)
- DWORD Value

Copy the ldcustkeys.ini file to the following directory on the core:

- C:\Program Files\LANDesk\ManagementSuite\LDHM\clients\wyse-ce5

You must upgrade the agent to 8.70 SP3 to use this feature. If the current version of the agent has already been installed on the device, the automatic agent update feature (wceagent.exe) will install the ldcustkeys.ini file on the client, and will update the file when changes are made to the file on the core.

The new registry settings will appear in the inventory tree view for the device under **OS > Thin Client Info**.

About the New thin client configuration dialog

Use this dialog (**Tools > Handheld > Thin-client configuration**) to create new thin-client configurations.

About the New thin-client configuration dialog's Internet Explorer tab

Use this tab to create a new Internet Explorer connection manager entry.

- **Enable Internet Explorer:** Adds this Internet Explorer configuration to the thin-client's connection manager.
- **Start page:** The full URL to the start page you want this entry to open.
- **Search page:** The full URL to the default search page this entry will use.
- **Cache size:** The amount of cache, in kilobytes, you want the browser to use.
- **Kiosk mode:** When checked, launches the browser in kiosk mode, without a menu or status bar.

About the New thin-client configuration dialog's Remote Desktop tab

Use this tab to create a new Remote Desktop connection manager entry.

- **Create Remote Desktop connection:** Adds this Remote Desktop configuration to the thin-client's connection manager.
- **Name:** The name that appears in the thin-client's connection manager. You can't change this.
- **Server:** The server that you want to connect to.
- **Low speed connection:** Makes the session faster over low-speed connections by disabling the desktop background, window and menu animation, and window contents while dragging.
- **Use connection bar:** Enables the Remote Desktop connection bar at the top of the session screen.
- **Connect local devices:** Check the box for any devices whose resources you want to use locally.

About the New thin-client configuration dialog's Citrix ICA tab

Use this tab to create a new Citrix ICA connection manager entry.

- **Create Citrix ICA connection:** Adds this Remote Desktop configuration to the thin-client's connection manager.
- **Connection title:** The name that appears in the thin-client's connection manager. You can't change this.
- **Name:** The connection name this entry will connect to.
- **Colors:** The number of colors this connection should use.
- **Compress data stream:** Whether compression should be enabled.
- **Use disk cache:** Whether the local disk cache should be enabled.
- **Sound:** Whether sound should be enabled, and if so, the local volume for audio.

LANDesk Application Virtualization

LANDesk Application Virtualization is a LANDesk Management Suite add-on product that is sold separately by LANDesk Software, Ltd.. LANDesk Application Virtualization uses Thinstall technology to virtualize an application, storing it in a single self-contained executable with the application and .DLL/device driver dependencies.

When run, virtualized applications run in an isolated environment without making changes to the Windows installation they're run on. Virtualized applications even run on locked-down devices without requiring additional privileges.

For more information, see the documentation that accompanies LANDesk Application Virtualization. When you use LANDesk Application Virtualization with Management Suite, you can deploy and manage virtualized applications.

Read this chapter to learn more about:

- Distributing virtualized applications
- Using inventory and software license monitoring with virtualized applications
- More information on virtualized applications

Distributing virtualized applications

Virtualized applications generally consist of one or more executable files. You can use software distribution to deploy these virtualized application executables to managed devices. You can use any of the software distribution delivery methods with virtualized application packages, including run from source. When you deploy a run from source virtualized application package, managed devices use a application shortcut icon to run the virtualized application executable over the network.

To create a virtualized application package

1. Use LANDesk Application Virtualization to create your virtualized application executable.
2. Click **Tools > Distribution > Distribution Packages**.
3. From the shortcut menu of the package group you want, click **New distribution package > New virtualized application package**.
4. In the **Distribution package** dialog, enter the package information and change the options you want. Note that you must enter the package name, description, and primary file. For more information on each page, click **Help**.
5. The **Shortcut** page is the only page specific to virtualized applications. Enter the shortcut icon **Name**. You can also specify if you want the icon on the **Desktop** and/or in the **Start menu**. If you check Start menu, you also can enter **the Programs folder name** that will contain the shortcut. The folder path you enter appears under **All programs**.
6. Click **OK** when you're done. Your script appears under the tree item for the package type and owner you selected.

When you deploy a virtualized application, software distribution copies the executable(s) to this folder on managed devices:

- %programfiles%\LANDesk\VirtualApplications\<distribution source path>.

The full virtualized application path includes the software distribution source path to help prevent problems with duplicate filenames. For example, if your distribution source path was vapps\myapp.exe, the path on managed devices would be %programfiles%\LANDesk\VirtualApplications\vapps\myapp.exe.

You can change the default virtualized application path if necessary in the **Agent configuration** dialog's **Software distribution** page.

Some virtualized applications require multiple executables. If that's the case, you can create a separate distribution package for these additional virtualized application executables. Then, when you create a distribution package for the main virtualized application executable, you can then include any additional dependent executables packages as dependencies. That way, if the dependent executables aren't already there, they'll be installed automatically.

Dependent executables need to be in the same shared folder when the distribution packages are created. This ensures that the dependent packages are distributed to the same folder on the managed device. If the dependent executables aren't in the same folder on the managed device they won't run.

The first time someone runs a virtualized application on a device, the "Thinstall runtime license agreement" dialog appears. Users need to click **Continue** to run the virtualized application. Users should only have to do this once.

Using inventory and software license monitoring with virtualized applications

Virtualized application executables created with LANDesk Application Virtualization have additional property information that helps Management Suite inventory and software license monitoring. In Windows Explorer, if you right-click a virtualized application executable and click **Properties**, there is additional version information:

- **ThinstallLicense:** LANDesk Application Virtualization license type and registration e-mail address.
- **ThinstallVersion:** LANDesk Application Virtualization packager version used to create this package.

You can use this information in your inventory queries to find virtualized applications that were scanned by the inventory scanner. Generally, virtualized application executable properties mirror those of the main executable inside the virtualized application. In the inventory view for a device, virtualized applications appear in the **Software > Package** list. Virtualized applications in this list have a "Virtual Application" attribute with a value of "Yes".

However, some applications don't provide version information before they are virtualized. In this case, they won't show up as virtualized applications in inventory even though they are virtualized.

Virtualized application executables will be scanned by the inventory scanner automatically only if you're using MODE=ALL inventory scanning. If you aren't using MODE=ALL and you want virtualized application inventory information in the database, you'll need to manually add the virtualized application executable information to software license monitoring's **Inventory > Files > To be scanned list**. The inventory scanner only sees the virtualized application executable. It doesn't scan within the executable.

Software license monitoring will automatically discover virtualized applications and include them in the **Product definitions > Autodiscovered** list. Software license monitoring's automatic application discovery doesn't use the inventory scanner. Software license monitoring does this by detecting the Start menu or desktop shortcut to the application.

A discovered virtualized application in the **Automatically discovered** list will only have the single virtualized application executable in its files list, but the product definition will still be based on the product within the virtualized application executable. Software license monitoring doesn't look inside the virtualized application executable and so it can't include other files that might normally be assigned to a product when it is installed without virtualization.

More information on virtualized applications

Virtual application sandbox

By default, virtualized applications create temporary files necessary for them to run under this folder:

- Documents and Settings\<username>\Application Data\Thinstall\

The inventory scanner doesn't scan this folder to prevent false reports of applications on the system.

Using non-LANDesk versions of Thinstall

The LANDesk Application Virtualization version of Thinstall has customizations that are specific to Management Suite. Other versions of Thinstall virtualized applications may not work correctly with software license monitoring or the inventory scanner.

LANDesk Inventory Manager

LANDesk Inventory Manager is a version of LANDesk Management Suite 8 that contains only these inventory-related features:

- Inventory scanning and inventory-related console features
- Custom data forms
- Software license monitoring
- Unmanaged device discovery
- Reports for the above features

The Inventory Manager installation on a core server contains all Management Suite 8 components, but when you activate a core server with an account that is licensed for Inventory Manager, the non-Inventory Manager features aren't applicable or visible in the Management Suite and Web consoles.

If you're using Inventory Manager, refer to the sections that correspond to the list of features above. Typically, you can recognize the information that doesn't apply in each chapter because those sections refer to Management Suite features like software distribution and remote control that aren't part of Inventory Manager.

Appendix: Additional inventory operations and troubleshooting

LANDesk Management Suite uses an inventory scanner utility to gather hardware and software information for the devices on your network. For information on inventory scanner basics, see the Managing inventory and Reports chapters. This chapter provides additional information about inventory scanning, as well as some troubleshooting tips.

Read this chapter to learn about:

Scanning custom information

The Windows inventory scanner utility (for Windows 95/98 and Windows NT/2000/2003/XP/Vista/7) automatically scans the device's registry for custom information. When you configure a device, the following keys are installed into the registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDESK\INVENTORY\CUSTOM FIELDS

The inventory scanner always scans the registry for the Custom Fields key and picks up any information it finds under that key. It then enters the custom information into Custom fields in the core database. The information in the Custom Fields keys can be whatever you need it to be. When you view this data in the console, it displays under Custom fields.

The inventory scanner reads two data types:

- REG_SZ
- REG_DWORD

Custom field subkeys
The inventory scanner doesn't scan for any subkeys below Custom fields.

Custom fields string length
ASCII character strings must be no longer than 255 characters. Multi-byte character set (MBCS strings must be between 127 and 255 characters).

Configuring the scanner to scan registry keys

The inventory scanner can scan for registry keys you specify and add their values to the core database. This can be useful for customized software, asset information, or other information stored in the registry that you want to include in the core database.

To use registry key scanning, add a section at the very beginning of the LDAPPL3.TEMPLATE file with this format:

```
[Registry Info]
KEY=HKLM, Software\Intel\LANDesk, version, MyData - LANDesk - Version
```

Change the values after KEY= to match the registry key you're looking for. In the example above, notice that each registry key element is separated by commas.

When the inventory scanner retrieves the registry key data, you can view it in the path specified by the last parameter. Each level is separated by " - " (space dash space). To force the scanner to use a 64-bit hive, append 64 to the hive name. For example, HKLM64.

Specifying the software scanning interval and history

You can specify when to scan a device's software and how long to save the inventory changes history log on the core server. These intervals apply to every device.

Note: A device's *hardware* is scanned every time it boots and is connected to the network.

To specify the software scanning settings

1. In the console's network view, click **Configure** > **Services > Inventory > Software**.
2. Specify the frequency of software scanning.
3. Specify the number of days to save the history.

The core server and software scanning
This feature affects only devices. It doesn't affect the core server, which is always scanned daily.

Scheduling an inventory scan task

If the device is running the Management Suite agents, you can schedule a script that triggers an inventory scan on devices.

To schedule an inventory scan

1. Click **Tools > Distribution > Manage scripts**.
2. Click **All other scripts**.
3. From the inventory scanner script's shortcut menu, click **Schedule**.
4. Configure task targets and the start time in the **Scheduled tasks** window.

The inventory scanner script is located in the \Program Files\LANDesk\ManagementSuite\Scripts directory. The script is a Windows .INI file that you can edit with any text editor. If you need to change the options or parameters within the script, open it and follow the instructions contained within it.

Scanner command-line parameters

You can add command-line parameters to the inventory scanner's (LDISCN32.EXE) shortcut properties to control how it functions.

The following table lists the scanner's command-line parameters:

Option	Description
/NTT=IP	Core server's IP address or DNS name and UDP port. For example, /NTT=123.123.123.123:5007 or /NTT=CORESERVER:5007. The OS/2 scan utility, LDISCAN2.EXE, and DOS scanner utility, LDISCAN.EXE, don't use this parameter.

Option	Description
/UDP	Scanner communicates via UDP instead of TCP. Combine this switch with /NTT=[IP].
/NOUI	Forces the scanner to run with no user interface.
/i=inifile	Provides the path (HTTP, UNC), or a drive letter to the master LDAPPL3 file. LDISCN32.EXE also copies the LDAPPL3 file they find in this location to the device's local LDAPPL3.INI file. The scanners compare the date of the master LDAPPL3 with the local LDAPPL3.INI; if the dates don't match, the master file is copied locally.
/d=directory	Starts the software scan in the specified directory. By default, the scan starts in the root directory of each local hard drive.
/L	Sends the scan to the core server the device was configured from. When you use /L, the /NTT parameter isn't necessary.
/sync	Forces a full scan, including a complete software scan. Full scan files can be several megabytes in size.
/n	Doesn't search subdirectories.
/v	Verbose mode.
/Z=retry count	How many times the scanner tries to resend the scan.
/W=wait in seconds	Have the scanner wait the number of seconds specified before starting a scan.
/? or /h	Displays the command-line syntax help.
/s=servername	Specifies the core server to store the inventory data on.
/f	Forces a software scan regardless of the software scan interval set at the console. Specify /f- to disable a software scan regardless of the software scan interval set at the console.
/t=[path]filename	Copies the contents of the specified file to the core database. Use this option to enter inventory data from standalone devices or from separate inventory files.
/o=[path]filename	Writes inventory data to the specified output file.

Option	Description
/m	Creates a non-unicode LDISCAN.MIF file in the C:/DMI/DOS/MIFS directory. This file contains the inventory data discovered during the scan.
/muni	(LDISCN32.EXE only) Creates a unicode LDISCAN.MIF file in the directory found in LDAPPL3.INI file's MIFPATH. This file contains the inventory data discovered during the scan.
/do16	Enables the 16-bit inventory scanner (inv16.exe) on managed devices.

Scanning standalone devices with a floppy disk

To scan a standalone device

1. Copy the proper inventory scanner utility and a software description file (usually LDAPPL3.INI) to a floppy disk. (You may also need to copy ELOGAPI.DLL, YGREP32.DLL, LOC16VC0.DLL, INV16.EXE, LOC32VC0.DLL, LTAPI.DLL, and LDISCN32.EXE.)
2. Run the scan with the **/O= parameter** specifying the path and filename of the output file.
3. At the command-line prompt, enter a **unique name** for the device. This name is saved in the LDISCAN.CFG file on the device's local drive. This name also appears in the Description field in the core database. For example:

```
ldiscn32.exe /f /v /o=c:\%computername%.scn
```

Adding inventory records to the core database

You can add inventory information from a standalone device or separate inventory files by running the inventory scanner from the operating system command line.

To add inventory records from a file to the core database

- Run the scan utility with the /S=, /T=, and the /NTT= parameters.

Adding BIOS text strings to the core database

There is a section in the LDAPPL3.TEMPLATE file called [BIOS Info]. This section provides the capability to search for information inside the BIOS of a computer. You can add one or more entries to the [BIOS Info] section. These entries define new keys in the core database and provide parsing instructions to the inventory scanner. The parsing instructions identify where to look in the LDBIOS.TXT file for a specific string. Using these instructions, the inventory scanner populates the core database with the strings from the LDBIOS.TXT file.

The inventory scanner uses a parsing method to locate BIOS information. This allows you to search for information one or more lines away from a specified text string. Such a search would enable you to locate random letter and number combinations assigned to computer hardware.

Text strings in LDBIOS.TXT

If you run the inventory scanner with the /do16 command line parameter, during an inventory scan, the text strings available in the BIOS are exported to a text file called LDBIOS.TXT. This hidden file is stored in the same location as the LDISCAN.CFG file, which is by default the root of the C: drive. LDBIOS.TXT stores all of the strings that are created by the scanner. If you want to store this information in the database, you can store it as a configuration file by using the CFGFILES parameter in LDAPPL3.INI.

Sample of BIOS entries in the LDAPPL3.TEMPLATE file

Here is an example from the [BIOS Info] section in the LDDAPPL3.TEMPLATE file:

```
[BIOS Info]
StringLength=4
Key = BIOS - Manufacturer
Parameters = AllValues,FirstInstance
Value = AMI|American Megatrends::AMI::BIOS - AMI
Value = Copyright.*Dell::Dell::BIOS - Dell
[BIOS - AMI]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(.*\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*\(AMI|American Megatrends\)
[BIOS - Dell]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(A.+\)::\1
Value = BIOS Version: \(A.+\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*Dell|[Cc]opyright.*Dell
```

Understanding BIOS entries

Entries in the [BIOS Info] section consist of the following:

- **[Section name]:** Identifies a new component in the core database.
- **StringLength=:** Specifies the minimum length of the strings to search for.
- **Key=:** Identifies the class and attribute name of the information returned from searching the LDBIOS.TXT file.
- **Parameters=:** Specifies the search criteria that tells the scanner where and how to search for values associated with a specific key.
- **Value=:** Specifies the value that is searched for in the BIOS. A value has three main sections, each separated by a double colon character (::). The strings identified in the value entry are case-sensitive. All characters in the value, even spaces, are included in the search unless they are an operator.

Creating MIF files

If you need a MIF file that stores a device's inventory information, you can create one by running the appropriate scanner at the command line.

To create a unicode MIF file, use the /MUNI option. To create a non-unicode MIF file, use the /M option.

To create MIF files

- Enter this at a DOS prompt:

```
LDISCN32/MUNI/V
```

Scanning NetWare servers

Management Suite uses LDISCAN.NLM to scan NetWare servers for hardware and software information. The command-line syntax for LDISCAN.NLM is:

```
LOADLDISCAN[.NLM]INV_SERV=servername
NTI=IPXaddressFILE=path[TIME=#][SCANNOW][MIF]
```

The following table lists the command-line parameters that you can use with the NetWare scanner.

Option	Description
INV_SERV = serenade	Directs the results of the scan to the specified server. The specified server must be running the inventory service.
NTT = IP address	Gives the IP address of the core server to send the inventory information to.
FILE = path	Lists the path to the LDAPPL3.INI file.
TIME = #	Sets the time of day for the server hardware scan in whole hours. The clock is in military time, so 0 = midnight and 23 = 11 p.m. Configure software scans in Options > Software Scanning. The default is 8 p.m.
SCANNOW	Forces an core server scan at the time the NM is loaded.
MIF	Creates the LDISCAN.MIF file for the core server. The .MIF file contains the inventory information gathered from the server.

To load LDISCAN.NLM on a NetWare server

- From the server console, enter the proper syntax at the LDISCAN.NLM command line.

For example, to scan a server daily and record its inventory data in the core database on "Server1," enter:

```
LOADLDISCANINV_SERV=SERVER1TIMEWORK NUMBER:NODEADDRESS:SOCKETFILERS:MONEYCHANGER
```

To unload LDISCAN.NLM from a server, enter:

```
UNLOADLDISCAN
```

Scheduling NetWare server scans

LDISCAN.NLM scans recur every day as specified by the TIME=# parameter. The TIME parameter is set in military time, so 0 is midnight and 23 is 11 p.m. The default is 8 p.m.

To change the time for server scans

- Add the TIME = # parameter to the load LDISCAN.NLM entry of LD_AUTO.NCF.

Editing the LDAPPL3.TEMPLATE file

Information relating specifically to the scanner's inventory parameters is contained in the LDAPPL3.TEMPLATE file. This template file works with the LDAPPL3 file to identify a device's software inventory.

You can edit the template file's [LANDesk Inventory] section to configure the parameters that determine how the scanner identifies software inventory. By default, LDAPPL3.TEMPLATE is located in this directory on the core server:

- \Program Files\LANDesk\ManagementSuite\LDLogon

Use this table as a guide to help you edit the [LANDesk Inventory] section in a text editor.

Option	Description
Mode	Determines how the scanner scans for software on devices. The default is Listed. Here are the settings: • **Listed:** Records the files listed in LDAPPL3. • **Unlisted:** Records the names and dates of all files that have the extensions listed on the ScanExtensions line but that are not defined in the LDAPPL3. This mode helps discover unauthorized software on the network. • **All:** Discovers files with extensions listed on the ScanExtensions line.
Duplicate	Records multiple instances of files. Set the value to OFF to record only the first instance, or ON to record all detected instances. The default is ON.
ScanExtensions	Sets the file extensions (.EXE, .COM, .CFG, etc.) that will be scanned. Use a space to separate the file extensions. By default, only .EXEs are scanned.
Version	Is the version number of the LDAPPL3 file.
Revision	Is the revision number of the LDAPPL3 file; helps ensure future compatibility.
CfgFiles 1-4	Records the date, time, file size, and contents of the specified files. You can leave out the drive letter (for example, c:) if you want to search all local drives. You can specify more than one file on each of the four lines, but the line length is limited to 80 characters. Separate path names on the same line by a space. The scanner compares the date and size of the current file with that of the previous scan. If the date and size don't match, the scan records the contents of the file as a new revision.
ExcludeDir 1-3	Excludes specific directories from a scan. You can leave out the drive letter (for example, c:) if you want to exclude all local drives. Enumeration must start at 1 and be continuous. You can use environment variables in this format: "%varname%". You can use a wildcard (*) in a "begins with" form

Option	Description
	only (ExcludeDir=%windir%\$NtUninstall*\ ). You must end each line with "\".
MifPath	Specifies where MIF files are stored on a device's local drive. The default location is c:\DMI\DOS\MIFS.
UseDefaultVersion	If set to TRUE, the scanner reports a match when a file matches an exact filename and file size entry in LDAPPL3 on filename only (the version will be reported as EXISTS). This can cause some false positives for applications that share a common filename with an unknown application. In the as-delivered LDAPPL3.TEMPLATE file, this parameter is set FALSE; that is, only add an entry if the match is exact. If the parameter is missing, it defaults to TRUE.
SendExtraFileData	If set to TRUE, sends extra file data to the core server. The default is FALSE. This means that by default, only path, name, and version are entered into the core database.

To edit the LDAPPL3.TEMPLATE file

1. From your core server, go to the LDLogon directory and open LDAPPL3.TEMPLATE in Notepad or another text editor.
2. Scroll down to the parameter you want to update and make your changes.
3. Save the file.
4. In the console, click **Tools > Reporting / Monitoring > Software License Monitoring**.
5. Click the **Make Available to Clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan if the /i scanner command line parameter is used on devices.

Troubleshooting the inventory scanner

This section describes common inventory scanner problems and possible solutions.

The inventory scanner hangs

- Make certain that you aren't including the old /DELL or /CPQ options on the command line. These options are no longer supported.
- Scan to a file using the /O= parameter. This may show a conflict with the network card or the network.

A device's hardware scans correctly, but its software doesn't

- Verify that the core database is configured to do a software scan now, and use the /f parameter to force a software scan.
- Scan to a file using the /O= parameter. This should list all of the software at the end of the file.
- Verify that the device is not trying to scan in a binary file in LDAPPL3.TEMPLATE's CfgFiles parameter.

The network view provides inventory data for only some devices

To view device information, ensure that your devices have been scanned into the core database. Devices appearing without information haven't been scanned into the core database.

To view a device's inventory data in the network view

1. Configure the device.
2. Scan the device into the core database.

For more information about configuring devices, see Configuring device agents.

For more information about scanning devices, see Managing inventory.

Specifying the number of days to keep inventory scans

By default, the core server keeps inventory scans for devices until you delete them. You can have the core delete inventory scans for devices if the device hasn't submitted a scan for the number of days you specify. Doing this can remove devices that are no longer on your network.

To specify the number of file revisions to keep in the core database

1. Click **Configure > Services > Inventory.**
2. Specify the **number of days** you want to keep inventory scans.
3. Click **OK**.

Changes to the way the inventory scanner gathers BIOS information

Beginning with Management Suite 8.7 SP3, the inventory scanner no longer uses the 16-bit inventory scanner to gather some BIOS information. By default, the scanner no longer reports on motherboard bus number, motherboard bus device attributes, and the size of attached floppy drives. Also, the inventory scanner no longer creates a hidden LDBIOS.TXT file on managed devices containing a list of BIOS strings.

If you want the inventory scanner to once again report on these options and create the LDBIOS.TXT file, you can run the inventory scanner with the /do16 switch.

Scanning for custom data on Macintosh devices

You can now gather custom data from devices running the LANDesk agent for Macintosh and process it into inventory. The information is saved in XML files within a specific directory on the client device. Use the information below to create custom data XML files in the correct location to be processed into inventory.

For information on an alternate custom data solution for Macintosh, download the custom data for Macintosh white paper from http://community.landesk.com/support/docs/DOC-1570.

Note: The implementation of custom data with the LANDesk agent for Macintosh doesn't use custom data forms. Custom data form tasks can't be deployed successfully to devices running the LANDesk agent for Macintosh.

Custom data XML file

Before you can add custom data to an inventory scan from a device running the LANDesk agent for Macintosh, you must first create a custom data XML file in the proper format. This section outlines the correct format to enable a custom data XML file to be processed without error.

Custom data XML file rules

XML files used to store custom data must comply with the following rules. Custom data XML files that do not correspond with all rules will not be processed into inventory.

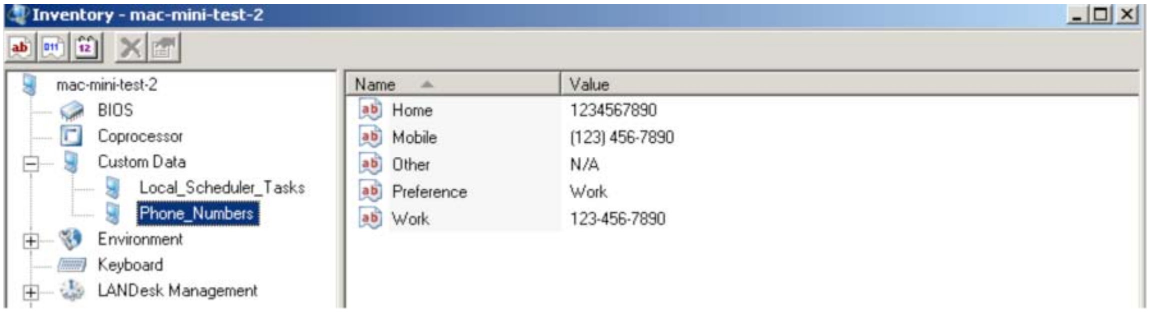
- Custom data XML files can have any name, but must end with the .XML extension. For example:
```
Phone Numbers.xml
```
- The first line in a custom data XML file must be an XML declaration. For example:
```
 <?xml version="1.0" encoding="UTF-8"?>
```
- All start tags within a custom data XML file must have a corresponding end tag. For example:
```
<Home>(123) 456-7890</Home>
```
- All tags within a custom data XML file must not have spaces. For example:
```
<Phone_Numbers></Phone_Numbers>
```
- All elements within a custom data XML that represent a single line of information must be wrapped within a parent element. For example:
```
<Phone_Numbers><Home>(123) 456-7890</Home></Phone_Numbers>
```
- In the event there is no content in an element in a custom data XML file, the element name will not be displayed as a custom data item in inventory. For example:
```
<Home></Home>
```
- In the event there is no content in any of the elements nested within a parent element in a custom data XML file, the parent element name will not be displayed as a node under custom data in inventory. For example:
```
<Phone_Numbers><Home></Home><Work></Work></Phone_Numbers>
```

Single-entry custom data XML file

Custom data XML files can be created to insert a single entry into the custom data section of inventory. To do this, the tags of each element in a custom data XML file must be named with the string that is to be displayed in inventory. Then the set of elements must be nested in parent elements with tags named to represent the string that is to be displayed under custom data in the tree view in inventory.

For example, if a custom data XML file were to be used to collect telephone numbers, the following XML format would result in the inventory record pictured below:

```
<?xml version="1.0" encoding="UTF-8"?>
<Phone_Numbers>
<Work>123-456-7890</Work>
<Mobile>(123) 456-7890</Mobile>
<Home>1234567890</Home>
<Other>N/A</Other>
<Preference>Work</Preference>
</Phone_Numbers>
```



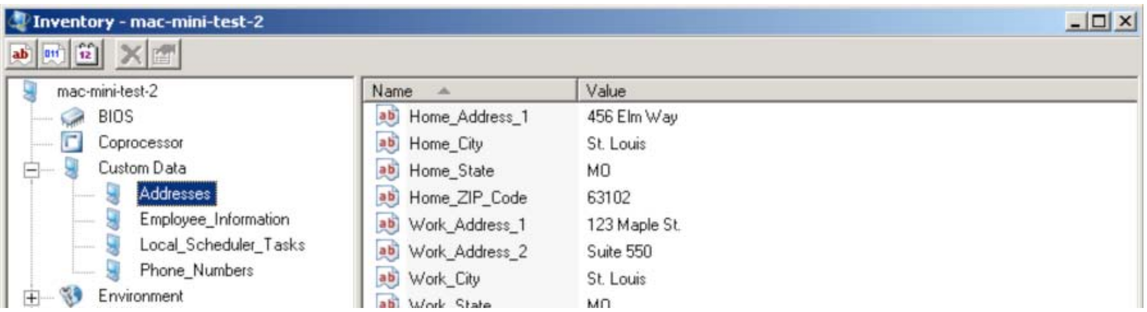
Name	Value
Home	1234567890
Mobile	(123) 456-7890
Other	N/A
Preference	Work
Work	123-456-7890

Multiple-entry custom data XML file

Custom data XML files can be created to insert multiple entries into the custom data section of inventory. To do this, the tags of each element in a custom data XML file must be named with the string that is to be displayed in inventory. Then each set of elements must be nested in parent elements with tags named to represent the string that is to be displayed under custom data in the tree view in inventory.

For example, if a custom data XML file were to be used to collect employee information, the following XML format would result in the inventory record pictured below:

```
<?xml version="1.0" encoding="UTF-8"?>
<Phone_Numbers>
<Work>123-456-7890</Work>
<Mobile>(123) 456-7890</Mobile>
<Home>1234567890</Home>
<Other>N/A</Other>
<Preference>Work</Preference>
</Phone_Numbers>
<Addresses>
<Work_Address_1>123 Maple St.</Work_Address_1>
<Work_Address_2>Suite 550</Work_Address_2>
<Work_Address_3></Work_Address_3>
<Work_City>St. Louis</Work_City>
<Work_State>MO</Work_State>
<Work_ZIP_Code>63102</Work_ZIP_Code>
<Home_Address_1>456 Elm Way</Home_Address_1>
<Home_Address_2></Home_Address_2>
<Home_Address_3></Home_Address_3>
<Home_City>St. Louis</Home_City>
<Home_State>MO</Home_State>
<Home_ZIP_Code>63102</Home_ZIP_Code>
</Addresses>
<Employee_Information>
<Title>Sales Representative</Title>
<Employee_ID>4562</Employee_ID>
<Manager>Bob Smith</Manager>
<E-Mail>John.Doe@WidgetsNMore.com</E-Mail>
</Employee_Information>
```



Name	Value
Home_Address_1	456 Elm Way
Home_City	St. Louis
Home_State	MO
Home_ZIP_Code	63102
Work_Address_1	123 Maple St.
Work_Address_2	Suite 550
Work_City	St. Louis
Work_State	MO

Custom data directory

Every custom data XML file to be processed into inventory must be saved in the custom data directory, which is located at **/Library/Application Support/LANDesk/CustomData** on every device running the LANDesk agent for Macintosh.

After a custom data XML file has been processed into inventory, the file remains in the CustomData directory. This allows for subsequent full scans (and delta scans with **Force software scan** enabled) to include information from custom data XML files saved in the custom data directory.

Inventory

During the software portion of an inventory scan, a check is made of the CustomData directory. Any XML files in the CustomData directory will be processed into custom data and included in the inventory scan sent to the core.

Inventory scan types

Custom data XML files that are in the CustomData directory are processed during all full scans, and are also processed during delta scans that include software scanning.

Inventory logging

The portion of an inventory scan that looks for and processes custom data XML files is recorded in LANDesk.log as **ldscan : Scanning for custom data**. If the custom data XML files in the CustomData directory are formatted properly, there will be no further entries in LANDesk.log regarding custom data. However, if there is an error, it will be recorded in LANDesk.log as **ldscan: Error opening or loading the CustomData file:filename.xml as XML**.

An error while processing a custom data XML file will not prevent other custom data XML files saved in the custom data directory from being processed. Likewise, errors processing custom data XML files will not prevent an inventory scan from completing or being sent to the core.

Inventory on the core

Custom data information in inventory, for a device running the LANDesk agent for Macintosh, will be updated when the custom data XML files containing information are updated and an inventory scan that updates custom data is executed on the client.

Be aware that custom data information removed from custom data XML files is not removed from inventory records on the core. To remove unwanted custom data information from an inventory record on the core, delete the record and send a new full scan from the device that the record represented.

Appendix: Additional OS deployment and profile migration information

The chapter provides supplemental information about LANDesk OS imaging and profile migration capabilities.

Read this chapter to learn about:

Creating an imaging boot disk

LANDesk OS deployment (OSD) includes a boot disk creation utility that allows you to easily create a disk you can use to boot devices into a managed state in LANDesk network. You can use this boot disk to continue OSD jobs on devices that do not have an operating system or that failed a job for some reason and are no longer bootable. Once you boot a device with this boot disk, you can schedule a job for it.

A user must have administrator rights on the core server if they want to create an OSD boot disk (even if they already have the OS Deployment right).

Boot disks are associated with the core server where they were created. If you have multiple core servers, use a boot disk created from the core server you want the device to report to.

To create an imaging boot disk

1. Click **Tools > Distribution > OS Deployment**.
2. In the **Operating system deployment** window, click the **Create a boot disk** toolbar button to open the Create Imaging Boot Disk dialog.
3. Insert a 1.44 MB diskette into the floppy disk drive and make sure the destination floppy drive is correct.

All data on the diskette will be erased.

4. Select the network adapter you want this boot floppy to support. Each floppy can only support one adapter because of disk space limitations.
5. Click **Start**. The Status box indicates the progress of the disk creation.
6. When finished, click **Close** to exit the dialog.

Adding application package distributions to the end of an OSD script

You can easily make an Enhanced Software Distribution (ESWD) application package distribution part of your OS deployment script.

To add ESWD packages to an OS deployment script

1. Open your package script in the LANDesk/ManagementSuite/Scripts directory and copy the REMEXECx= package distribution lines.
2. Edit your script by right-clicking it in the Manage Scripts window and clicking **Advanced edit**.
3. Paste the ESW REMEXEC commands at the bottom of your script, changing the REMEXEC numbering so that the numbers are sequential.
4. Insert a line before the ESWD lines you pasted in for LDSLEEP, similar to below. This allows time for the OS to finish booting before starting the package installation.

   ```
   REMEXECxx=LDSLEEP.EXE 120
   ```

   Replace xx with a unique sequential number.

Using CSVIMPORT.EXE to import inventory data

LANDesk includes a command-line utility that allows you to import inventory data into the core database. This can be useful if you're installing new devices and you have information like MAC addresses available. You can use CSVIMPORT.EXE to import this data to the core server so you can target devices ahead of time for OS deployment jobs.

CSVIMPORT.EXE requires a template file describing the field contents and what columns in the core database the data should go in. CSVIMPORT.EXE also requires the .CSV file containing the data matching the template file you specify. CSVIMPORT.EXE creates miniscan files that you can then copy to the LANDesk/ManagementSuite/LDScan directory so they get added to the core database.

Sample template file:

```
Network - NIC Address = %1%
Network - TCPIP - Adapter 0 - Subnet Mask = 255.255.255.0
BIOS - Serial Number = %2%
BIOS - Asset Tag = %3%
Display Name = %4%
```

Note that you can include custom data in the files. The entries %1, %2, and so on refer to the first column, second column, and so on. The subnet mask in this case will be applied to all entries as 255.255.255.0. The template file can't have any header text other than the actual template information.

Sample .CSV file:

```
0010A4F77BC3, SERIAL11, ASSETTAG-123-1, MACHINE1

0010A4F77BC4, SERIAL21, ASSETTAG-123-2, MACHINE2

0010A4F77BC5, SERIAL31, ASSETTAG-123-3, MACHINE3

0010A4F77BC6, SERIAL41, ASSETTAG-123-4, MACHINE4

0010A4F77BC7, SERIAL51, ASSETTAG-123-5, MACHINE5

0010A4F77BC8, SERIAL61, ASSETTAG-123-6, MACHINE6
```

Run CSVIMPORT with these three parameters: <templateFilename> <csvFileName> <outputDirectoryForScanFiles>. If you want the output to be entered in the core database immediately, specify your LANDesk/ManagementSuite/LDScan directory for output.

Creating custom computer names

The **Naming convention** page of the OS Deployment/Migration Tasks wizard lets you create computer names based on MAC addresses, text you enter, and counters (nnn...). You can also create names based on inventory data for asset tags, serial numbers, and login names by creating a COMPUTERNAME.INI file.

COMPUTERNAME.INI syntax:

```
[Rename Operations]
tok0=ASSET TAG
tok1=SERIAL NUMBER
tok2=LOGIN NAME
```

The values returned by the .INI file substitute for the $MAC token in the wizard's naming convention page.

You can only use the above three inventory values in the file. OS deployment checks the options in the numeric tok<x> order. All three of the above tokens don't have to be in the file. The first tok<x> option found that has an equivalent database entry substitutes for the $MAC token for the device being imaged. For example, in the case above, if there were no asset tag or serial number entries in the database, but there was a login name, the login name would be used for the $MAC token. If none of the options match, the MAC address is used for the $MAC token.

The login name option returns the login name returned by the most recent inventory scan.

Using the nnn computer name token

The **Naming convention** page of the OS Deployment/Migration Tasks wizard includes an nnn option that substitutes for a 3-15 digit number, depending on how many n characters you specify. For each computer name template you use in the wizard, OS deployment keeps a running counter of the numbers used. This way, subsequent jobs continue where the last job left off.

Every unique template has its own counter. If you always use the same template, the counter will span jobs. If you change your template after deploying some devices and later decide to go back to the template you originally used, the counter remembers where you left off for that template and continues counting.

Customizing the SYSPREP.INF [RunOnce] section with tokenized inventory values

The SYSPREP.INF file contains a [RunOnce] section that specifies programs to run after the device boots for the first time. If you add your own programs to that section, you can include database tokens on the program command line if they're useful to the program you're running. OS deployment substitutes the token you specify with corresponding information from the core database.

Sample tokens:

```
%Computer - Device Name%
%Computer - Login Name%
%Computer - Manufacturer%
%Computer - Model%
%Computer - Type%
%Computer - BIOS - Asset Tag%
%Computer - BIOS - Service Tag%
%Network - TCPIP - Address%
%System - Manufacturer%
%System - Model%
%System - Serial Number%
%Processor - Processor Count%
%Computer - Workgroup%
%Computer - Domain Name%
```

You can chain multiple tokens together. For example, to separate two tokens by a colon: %Computer - Workgroup%:%Computer - Device Name% could return MyWorkgroup:MyComputer.

You should only use tokens that return a single value.

Using images in mixed uniprocessor and multiprocessor environments

Uniprocessor and multiprocessor devices require different Windows 2000 and Windows XP images. Depending on your hardware configuration, you may be able to use your uniprocessor image on a multiprocessor device, or vice versa.

Devices that support advanced processor features typically have an Advanced Programmable Interrupt Controller (APIC). Devices that support advanced processor features can also have an Advanced Configuration and Power Interface (ACPI).

The support matrix for sharing an image between uniprocessor and multiprocessor devices is complex. You should refer to Microsoft's UNATTEND.TXT file for more details. Generally, you need to remember the following when sharing uniprocessor and multiprocessor images:

Both the source and target devices must have either an ACPI APIC HAL or a non-ACPI APIC HAL. You can't use an ACPI APIC image on a non-ACPI APIC device, or vice versa.

To configure multiple processor information

1. In the **Sysprep options** page of the OS Deployment/Migration Tasks wizard, select **Configure advanced multiprocessor options**.
2. In the **Multiprocessors** page, select whether you're deploying a **Windows 2000** or a **Windows XP** image.
3. Select whether the image you're using was created on a **Uniprocessor** or **Multiprocessor** device.

4. Your source and target devices have the same HAL. If your image was created on an APIC ACPI device, select **APIC**. If your image was created on a non-ACPI APIC device, select **MPS**.

Adding network adapter drivers to the DOS boot environment

There are three network adapter driver detection phases that occur during an OS deployment job:

Phase 1 (Windows)

NICINFO.EXE detects PnP drivers in Windows 2000/XP. It also detects Windows 9x if IE 4.02 or higher is installed. NICINFO.EXE writes the detected vendor and device ID to DOSNIC.INI on the virtual boot image.

Phase 2 (DOS)

AUTODETE.EXE looks for the DOSNIC.INI left by NICINFO.EXE and reads the vendor and device ID. AUTODETE.EXE then refers to NIC.TXT to find the corresponding driver to load. It copies the driver from c:\Net\Drivers on the virtual boot image to the current RAM drive image (r:\Net by default). AUTODETE.EXE then sets the Microsoft DOS network stack configuration files, SYSTEM.INI and PROTOCOL.INI.

If DOSNIC.INI is empty, AUTODETE.EXE scans all PCI device slots looking for network adapter vendor and device IDs. If the ID found matches an entry in NIC.TXT, AUTODETE.EXE loads that driver.

Phase 3 (DOS)

If DOSNIC.INI is empty and AUTODETE.EXE can't match the discovered ID with NIC.TXT, it loads the driver specified in the OS Deployment/Migration Tasks wizard. If this driver doesn't load, the device will be stuck in DOS, and you'll need to reboot it manually. If no driver was specified in the wizard, AUTODETE.EXE saves an AUTODETE.LOG file to the drive root and the device boots back into the original operating system.

NICINFO.EXE and AUTODETE.EXE don't support 16-bit PCMCIA network adapters. You can load the drivers for these network adapters by selecting the appropriate driver in the OS Deployment/Migration Tasks wizard as described in Phase 3. NICINFO.EXE can detect network adapters that support CardBus.

NICINFO.EXE requires PnP support. Windows NT 4 has no PnP support.

Adding network adapter drivers

To add network adapter drivers

1. Edit the **ALTDRIVERS.INI** file (found in the ..\ManagementSuite\ folder).
2. Edit the **NIC.TXT** file in the ..\ManagementSuite\OSD\Utilities directory.
3. Use **COPYFILE.EXE** to insert the .DOS or .EXE driver file into the virtual boot image in **..\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG**
4. Use **COPYFILE.EXE** to insert **NIC.TXT** to the virtual boot image.

Editing the ALTDRIVERS.INI file

ALTDRIVERS.INI is the driver description file.

Sample entry:

```
[Intel PRO/1000 Adapters]
DRIVER=E1000.DOS
PROTOCOL=E1000
```

- The description between brackets [ ] can be anything. This is the text that appears in the OS Deployment/Migration Tasks wizard when you manually select a network adapter driver.
- DRIVER is the .DOS or .EXE network adapter driver.
- PROTOCOL often is the same as the driver name or the manufacturer name.

Editing the NIC.TXT file

NIC.TXT has information for detecting network adapters. You'll need to edit the NIC.TXT to add custom adapter information. Here's a sample entry:

```
ven=115D "Xircom"
dev=0003 "Xircom CardBus Ethernet 10/100 Adapter"
drv="CBENDIS.EXE"
prot="XIRCOM"
```

These are the four possible keys and values:

- **ven** is four characters (for example, 1 must be 0001); description can be anything.
- **dev** is four characters; description can be anything.
- **drv** is the driver name; default extension is .DOS.
- **prot** is the protocol, often the same as the driver name or the manufacturer.

As you can tell by looking at NIC.TXT, not all drivers have all keys.

Injecting driver changes back into the virtual boot image

To inject driver changes back into the virtual boot image, use copyfile. The syntax is:

```
COPYFILE <imgfile> <srcfile> <destfile>
```

Example:

```
COPYFILE c:\Program Files\LANDesk\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG
c:\Drivers\MYNIC.DOS\Net\Drivers\MYNIC.DOS
```

The <destfile> variable can't contain the drive letter designation.

You need to copy the .DOS or .EXE network adapter driver to c:\Net\Drivers and the updated NIC.TXT to c:\Net

Adding network adapter drivers to the Windows PE boot environment

If you need to add custom network drivers to the Windows PE environment, follow the steps below.

To add Windows PE boot environment network drivers

1. Copy the network driver .INF and .SYS files to this folder on the core server:

   ..\ManagementSuite\LANDesk\Vboot\winpedrv

2. Add the network driver information to this file on the core server (see the sample entries inside for details):

..\ManagementSuite\altdriverspe.ini

Using the LANDesk imaging tool for DOS

If your license includes the OS deployment and profile migration component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT, and BACKALL.BAT.

LANDesk's imaging tool for DOS (IMAGE.EXE) is a DOS-based backup and restore utility that creates a snapshot of an entire partition or volume and saves it to a set of files, or saves it directly to most ATAPI CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

Limitations

IMAGE.EXE relies on the BIOS for processing disk functions. If a computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGE.EXE will also be limited.

System requirements

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- 16 MB RAM
- XMS

Getting started

IMAGE.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

Environment variables

You can use several different environment variables with IMAGE.EXE:

- **IMSG** displays a message on the screen. To create a message with IMSG, use the set command (i.e., set imsg=<include message of 80 characters or less here>).
- **IBXT** changes the method used to burn a set of CDs so that IMAGE.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1 (i.e., set ibxt=1). This setting may not work with all CD-R/RW drives.
- **IAR** enables IMAGE.EXE to auto-respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set iar=Y). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.
- **IOBS=A** tests the network speed and uses the best buffer size for uploading/downloading an image.

Command-line options

You can use command-line options with IMAGE.EXE. Separate the options by spaces and enter them in the order shown below. Use the /? command-line option to view a list of additional command-line options not explained here.

To create a compressed image to a file

Format 1: image /Ch# d:\filename.img (no validation)

Format 2: image /Ch#V d:\filename.img (validation)

Format 3: image /Ch#VB d:\filename.img (byte-for-byte validation)

Explanation: Replace the h with the source hard drive number from 0 to 7 and the # with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as 0xPVV where P is the extended partition and VV is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGE.EXE without any command-line options and select Create Image. The screen that lists the partitions and volumes will display the ID in parentheses as a hexadecimal number. You should prefix that number with a 0x on the command line.

To create an uncompressed image to a file

Format 1: image /Ch# /U d:\filename.img (no validation)

Format 2: image /Ch#V /U d:\filename.img (validation)

Format 3: image /Ch#VB /U d:\filename.img (byte-for-byte validation)

Explanation: Same as above.

To create a compressed image to a CD drive

Format 1: image /Ch# /CDx (ATAPI)

Format 2: image /Ch# /CDSx (ASPI)

Explanation: The h and # information is the same as above. The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS) to get a list of the devices.

To create an uncompressed image to a CD drive

Format 1: image /Ch# /U /CDx (ATAPI)

Format 2: image /Ch# /U /CDSx (ASPI)

Explanation: Same as above.

To restore an image from a file

Format 1: image /R d:\filename.img (no validation)

Format 2: image /RV d:\filename.img (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

To restore an image from a CD

Format 1: image /R /CDx (ATAPI)

Format 2: image /R /CDSx (ASPI)

Explanation: The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS) to get a list of the devices.

To limit the file size on creation

Format: d:\filename;s

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.

Issues to be aware of

- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- When restoring an image, you shouldn't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system will reboot. This is required because the partitions and file system being used by the OS have changed. If a reboot didn't occur, the OS would still think the partition and file system was as it was before the restore. This could cause data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition goes to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If an existing partition or volume occupies the same starting location as the partition to be restored, then a warning message is issued before overwriting that partition or volume.
- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGE.EXE via AUTOEXEC.BAT if desired.

Using the LANDesk imaging tool for Windows

LANDesk's imaging tool for Windows (IMAGEW.EXE) is a Windows 32-based backup and restore utility that creates a snapshot of an entire partition or volume and saves it to a set of files, or saves it directly to most types of DVD+RW or CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

IMAGEW.EXE is compatible with LANDesk's imaging tool for DOS (IMAGE.EXE).

Updated version of IMAGEW

LANDesk Management Suite now includes an updated version 2 of IMAGEW, which includes support for Windows 7. This version saves image files with a different file extension, and it includes some new functionality. If you have used version 1 of IMAGEW in the past you can continue to use it as documented in the following section.

Version 2 of IMAGEW is installed as part of LANDesk OS Deployment in the ..\ManagementSuite\osd\imagew 2 directory.

For information about using IMAGEW 2, visit the LANDesk Support Community Web site at community.landesk.com.

Using IMAGEW version 1

The following information applies to IMAGEW version 1.

Limitations

For use with Windows 9x/Me, IMAGEW.EXE requires that the system support Int 13h extensions. If your computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGEW.EXE will also be limited on those OSes.

System requirements

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- Windows 32-based environment with 32 MB RAM minimum recommended
- Administrator privileges when running on Windows NT, Windows 2000, or Windows XP

IMAGEW.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

Creating images

You can use various environment variables and command-line options to ensure that the images you create meet your requirements.

Environment variables

Environment variables for IMAGEW.EXE must be used with command-line options. The following environment variables are available:

- **IBXT** changes the method used to burn a set of CDs so that IMAGEW.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1 (i.e., set ibxt=1). This setting may not work with all CD-R/RW drives.
- **IAR** enables IMAGEW.EXE to auto respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set iar=Y). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.

Command-line options

You can use command-line options with IMAGEW.EXE. Separate the options by spaces and enter them in the order shown below. Use the /? command-line option to view a list of command-line options not explained here.

To create a compressed image to a file

Format 1: imagew /Ch# d:\filename.img (no validation)

Format 2: imagew /Ch#V d:\filename.img (validation)

Format 3: imagew /Ch#VB d:\filename.img (byte-for-byte validation)

Explanation: Replace the h with the source hard drive number from 0 to 7 and the # with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as 0xPVV where P is the extended partition and VV is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGEW.EXE without command-line options and select Create Image. The screen that lists the partitions and volumes will also display the ID in parentheses as a hexadecimal number. You should prefix that number with a 0x on the command line.

To create an uncompressed image to a file

Format 1: imagew /Ch# /U d:\filename.img (no validation)

Format 2: imagew /Ch#V /U d:\filename.img (validation)

Format 3: imagew /Ch#VB /U d:\filename.img (byte-for-byte validation)

Explanation: Same as above.

To create a compressed image to a CD drive

Format 1: imagew /Ch# /CDx

Explanation: The h and # information is the same as above. The x after /CD is the CD drive number to use. Omit the x to get a list of the devices.

To create an uncompressed image to a CD drive

Format 1: imagew /Ch# /U /CDx

Explanation: Same as above.

To restore an image from a file

Format 1: imagew /R d:\filename.img (no validation)

Format 2: imagew /RV d:\filename.img (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

To restore an image from a CD

Format 1: imagew /R /CDx

Explanation: The x after /CD is the CD drive number to use. Omit the x to get a list of the devices.

To limit the file size on creation

Format: d:\filename;s

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.

Issues to be aware of

- When running under Windows NT/2000/XP Pro, you must have administrator privileges. Under Windows 2000/XP, you can run as any user by right-clicking and selecting the Run As option.
- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- If you create a backup without a lock being obtained, that backup may not be in a consistent state if updates to the drive were occurring during the backup.
- When restoring an image, you can't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system may need to reboot. This is required under certain conditions and determined by the program. If you don't reboot when asked, the OS will think the partition and file system is as it was before the restore, potentially causing data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition will go to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If

an existing partition or volume occupies the same starting location as the partition to be restored, a warning message is issued before overwriting that partition or volume.

- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGEW.EXE via AUTOEXEC.BAT if desired.

Understanding the Windows PE preboot environment

Windows PE is a mini-Windows system that provides limited services based on the Windows XP Professional and the Windows Server 2003 kernels. Windows PE is a hardware-independent Windows environment that contains the following:

- A subset of the Microsoft Win32 application programming interfaces (APIs).
- A command interpreter capable of running batch files.
- Support for adding Windows Script Host (WSH), HTML Applications (HTA), and Microsoft ActiveX Data Objects (ADO) to create custom tools or scripts.

Windows PE uses TCP/IP to provide network access and supports the same set of networking and mass- storage device drivers that Windows XP supports. Some limitations worth noting are that connectivity is limited to outgoing connections only (resource sharing is disabled), and to prevent client-usage of the OS, a hard-coded reboot will occur after 24 hours of use.

LANDesk has customized the Windows PE operating system to only include necessary libraries, utilities, and drivers. Additionally, the LANDesk agent files have been copied to the image to facilitate LANDesk functionality. Also, the command file initially loaded by the PE operating system has been modified to include the LANDesk staging commands. Starting with Service Pack 2 for LANDesk 8.7, WMI support was added to the image.

This section will provide a list of the files that have been either added or modified in the PE image, an overview of the boot process and an explanation of each line in the startup command file.

Files modified or added to the WinPE image

In addition to drivers, the LANDesk Windows PE image includes the following modified or added files.

File	Purpose
winbom.ini	Turns off the Windows PE firewall
\i386\txtsetup.sif	LANDesk signature file
\i386\system32\winpeshl.ini	Defines the shell location
\i386\system32\peshell.exe	The actual shell used
\i386\system32\setupreg.hiv	Includes the LANDesk path
\i386\system32\startnet.cmd	Command file run at startup
\i386\system32\all.reg	LANDesk registry modifications
\i386\system32\winpe.bmp	LANDesk background wallpaper
\CBA8	LANDesk agent
\LDCLIENT	LANDesk agent

LANDesk WinPE boot process

The WinPE boot process starts like this:

1. Once the boot sector is loaded, SETUPLDR uses NTDETECT.COM to scan the hardware so the correct HAL can be loaded.
2. The WINPEOEM.SIF is used to load boot drivers (administrators can customize this file to control which mass-storage drivers are loaded) and then NTOSKRNL.EXE finishes the environment setup and calls SMSS, which in turn loads the registry and calls Winlogon.
3. Winlogon starts the services, finishes driver loading and starts a user session.
4. CMD.EXE is executed and processes the STARTNET.CMD. This batch file is used to load the networking drivers and any other commands one adds to it. The original Windows PE STARTNET.CMD looks like this:

   ```
   factory winpe
   ```

The LANDesk-modified WinPE image by default includes a custom STARTNET.CMD file. In version 8.7sp2, it looks like this:

```
@echo off
set path=%path%;x:\cba8;x:\ldclient
\ldclient\GetBootOptions set /a err = %errorlevel%
if %err% gtr 0 goto nofix
ldclient\Diskinfo fix
:nofix
factory winpe
reg import all.reg
 \ldclient\wait4ip /t 180
if %errorlevel% gtr 0 goto fail
CD \CBA8
RESIDENTAGENT.EXE /register
RESIDENTAGENT.EXE /start
CD \ldclient
 winpepds /install
 winpepds /start
If %err% gtr 0 goto pxe
miniscan /nodeviceid /usemacasname
Goto end
:pxe
if %err% lss 2 goto pxemenu
:pxeboot
miniscan /x /nodeviceid /usemacasname
goto end
:pxemenu
miniscan /nodeviceid /usemacasname
Replcore PxeMenuStart.cmd
call PxeMenuStart.cmd
goto end
:fail
@echo "Failed to get localhost IP address or resolve core server name. Please check your
network and try again."
@pause
:end
```

STARTNET.CMD command definitions

The following section describes each line in STARTNET.CMD.

@echo off

Hides the output of this CMD file. REM this command out when troubleshooting the STARTNET.CMD.

set path=%path%;x:\cba8;x:\ldclient

Sets the path to include the added LANDesk agent files.

\ldclient\GetBootOptions

This executable sets the errorlevel to 0, 1, or 2. The values are 0 if the machine was virtual booted, 1 if the machine was PXE booted and the PXE menu was chosen, and 2 if the machine was PXE booted and managed boot was chosen.

set /a err = %errorlevel%

Sets the ERR variable to the value derived by GetBootOptions.

if %err% gtr 0 goto nofix

This line has the script skip to the next line if the machine was PXE-booted.

\ldclient\Diskinfo fix

This line is only processed if not PXE booting. Diskinfo.exe used with the fix switch resets the MBR to boot back into the original active partition. Vbooting had previously set this to boot to the WinPE RAM drive.

factory –winpe

The FACTORY.EXE command is used to load drivers and when called with the –winpe switch it will generate a unique name for the PE session (usually minint-<random suffix>) and then process the WINBOM.INI, which is where you can configure and add to the PE behavior. For example, since by default FACTORY.EXE is scanning all of the available drivers to find the one that matches the discovered hardware, you could limit the number of drivers scanned (thereby increasing bootup speed) by modifying the NetCards section of the WINBOM.INI file.

reg import all.reg

Imports the LANDesk environment settings into the WinPE registry. Specifically, the core server's name and the port used for inventory are defined in the ALL.REG file. Here is an example ALL.REG:

```
 Windows registry Editor version 5.00
 [HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM]
“CoreServer”=”<core_name>”
“InventoryServerPort”=”5007”
```

\ldclient\wait4ip /t 180

The wait4ip executable ensures we have an IP address before gathering inventory for this machine. The /t 180 defines a timeout limit of 3 minutes. A /s can be added to silence the output of this program. Additional information is available by executing with a /?.

if %errorlevel% gtr 0 goto fail

Skips the rest of the commands in this file if an IP address can't be obtained.

CD \CBA8

Changes the directory from X:\i386\system32 to X:\CBA8.

residentagent.exe /register

RESIDENTAGENT.EXE is the service that listens for and accepts connections for remote commands, and then starts the application needed to handle the request (which is how the LANDesk imaging operations are carried out). The /register switch will install and register the RESIDENTAGENT.EXE as a service. This is logged in the CBA8 directory in RESIDENTAGENT.LOG.

residentagent.exe /start

The /start switch will start the RESIDENTAGENT.EXE service, which proceeds to load necessary libraries. This too is logged in the RESIDENTAGENT.LOG.

CD \LDClient

Changes the directory from X:\CBA8 to X:\LDClient.

winpepds /install

WINPEPDS is the module pinged by the core server to discover this machine, verifying this is the correct managed node. The /install switch will install the service.

winpepds /start

The /start switch starts the WINPEPDS service.

if %err% gtr 0 goto pxe

This line means that PXE booted machines will continue the script at the PXE section further below.

miniscan /nodeviceid /usemacasname

This line is only executed by virtual booted machines, and is their last command. Miniscan is the utility used to grab minimal information about the system and store it in the LDMS inventory database. Running miniscan without switches will include a device name and ID in its scan file, and thereby will show up in the console as “minint-<random suffix>”. However, using the /nodeviceid /usemacasname switches removes this information from the scan file and limits the data sent to 3 things: MAC Address, IP Address, and Processor Count. In the console, these devices show up named after their MAC address.

if %err% lss 2 goto pxemenu

Tells PXE-booted machines that are supposed to get the menu to skip to the PXEmenu section.

miniscan /x /nodeviceid /usemacasname

This line is executed by those PXE booted machines that are a managed boot. If the /x is used when calling miniscan, an extra attribute is sent in the Network portion of the scan file, Pxeboot=Yes.

miniscan /nodeviceid /usemacasname

This line is only executed by PXE-booted machines that are to display a menu. Miniscan is the utility used to grab minimal information about the system and store it in the LDMS Inventory database. Running miniscan without switches will include a device name and ID in its scan file, and thereby will show up in the console as “minint-<random suffix>”. However, using the /nodeviceid /usemacasname switches removes this information from the scan file and limits the data sent to three things: MAC Address, IP Address, and Processor Count. In the console, these devices show up named after their MAC address.

replCore PxeMenuStart.cmd

REPLCORE.EXE is used to replace the %CoreServer% variable in the file it is pointed to with the value found in the registry String Value HKLM\Software\Intel\LANDesk\LDWM\CoreServer (this was populated with the ALL.REG earlier in the process). In this case, the PxeMenuStart.cmd is about to be called and it uses sdclient to contact the core server and therefore must have the correct core name in its command line.

call PxeMenuStart.cmd

If the menu option is chosen by the PXE booted machine, then the PXEMENUSTART.CMD will be executed. Two of the significant lines are:

```
sdclient /f /o /p=”http://%CoreServer%/landesk/files/dosmenu.cfg”
RunBatch 500 X:\LDClient PxeMenu dosmenu.cfg
```

First, sdclient is used to retrieve the DOSMENU.CFG from the core server. Then RunBatch (a simple utility that calls a process after a defined delay) is used to launch PXEMENU.EXE fed with the parameter of DOSMENU.CFG.

@echo "Failed to get localhost IP address or resolve core server name. Please check your network and try again."

If an IP address could not be obtained, this error message appears, indicating that the NIC or NIC drivers should be investigated.

Appendix: Additional software distribution information

This chapter explains how to use LANDesk Management Suite's software distribution (SWD) to distribute software and files to devices throughout your network.

Read this chapter to learn about:

- Processing custom scripts
- Scripting guide for deployment scripts (.INI) files
- Understanding Software Distribution error codes

Processing custom scripts

Custom scripts that control scheduled tasks (**Tools > Distribution > Scheduled tasks**) are processed in three sections:

- **Premachine:** The Premachine section of the custom script is processed first, and only once at the start of the task. Use this section for tasks that have no targeted device, and/or for Targeted Multicast. During the Premachine section of the script, only local commands, LOCxxx, should be used.
- **Machine:** The commands in this section of the script run second and only once per targeted device. These commands can use either the remote or local execution commands, and are primarily used for remotely executing SDCLIENT.EXE. Before the commands in this section of the script can be performed, the SWD agent must be installed on the targeted devices.
- **Postmachine:** This section is processed last, and again, only once after all devices have been processed. Software distribution does not add commands to this section, and it only supports the local commands, LOCxxx. The commands in this section won't be processed if devices in the task can't run them. The InventoryScanner.ini script that comes with Management Suite contains details about the script commands.

Custom Script Commands

Custom scripts support various local and remote commands:

- **LOCEXEC:** Local execute, this command is used to execute an application on the local device, which is always the core server.
- **LOCDEL:** Local deletion, deletes a file on the local device.
- **LOCMKDIR:** Local make folder, creates a folder on the local device.
- **LOCRD:** Local remove folder, this command is used to remove a folder on the local device.
- **REMCOPY:** Remote copy, copies a file from the local device to a remote device.
- **REMEXEC:** Remote execution, executes an application on the specified remote device
- **REMDEL:** Remote deletion, deletes a file on the remote device
- **REMMKDIR:** Remote make folder, this command creates a folder on the remote device
- **REMRD:** Remote remove folder, this command deletes a folder on the remote device

Command-line parameters

Software distribution is facilitated by a deployment script. SDCLIENT.EXE manages the packages using command-line parameters from the script file that are passed to the application.

SDCLIENT.EXE supports the following command-line parameters:

```
sdclient.exe /p="<package path>" [/g=<pkg guid>] [/All] [/R] [/N] [/An] [/Ac] [/Ab]
[/fui] [/msi] [/exe] [/bw=xxx] [/E]
```

Parameter name	Description
/p=<package path>	Package Path. The package path must be specified, regardless of the package type. This parameter specifies the UNC or URL path to the package that is to be installed on the local device.
/g=<pkg guid>	Package GUID. For SWD or AutoInstall packages. This parameter specifies the GUID for the package. The package GUID is used to check the local .CFG file cache for a copy of the package's .CFG file.
/All	Uninstall Flag. This flag is set to indicate that the SWD or MSI package should be uninstalled rather than installed. This flag is case-sensitive (/all won't work).
/R	Always Reboot Flag. This flag indicates that the device should always be rebooted after the package installation. Not all MSI packages follow this guideline.
/N	Never Reboot Flag. This flag indicates that the device should never be rebooted after the package installation.
/An	Silent Installation Flag. This flag indicates that the installation should be silent. This means that no UI, or the smallest amount of UI possible, should be displayed during the installation.
/Ac	Disable Cancel Flag. This flag prohibits the user's ability to cancel the installation.
/Ab	No Background Flag. This flag only applies to SWD packages. When a package is being installed, the blue background won't be displayed.
/fui	Full UI Flag. This flag indicates that the full UI for legacy and MSI packages should be used.
/msi	MSI Package Flag. This flag indicates that the package path points to an MSI package file.
/exe	Executable Package Flag. This flag indicates that the package path points to a legacy package or a generic executable file.

Parameter name	Description
/bw=xxx	Bandwidth Requirements. Specifies a minimum bandwidth requirement for the package script to be run.
/F	Generic File Flag. This flag causes SDCLIENT.EXE to download the file to the LDCLIENT folder.
/msg=""	Sends a message to the core server while the task is executing. This message appears in the task status inside the **Scheduled tasks** window's **Message** column.

HTTP and UNC paths

These are examples of software distribution .INI files that reflect the differences between HTTP and UNC path script files.

HTTP path script file:

```
; This file was generated by Desktop Manager
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=http://<web
server>/packages/test package.exe -g={6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-
9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

UNC path script file:

```
; This file was generated by Desktop Manager
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=\\sample_core\onefile\test
package.exe -g={6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac
-Ab
```

Notice that both .INI files have similar elements. In the MACHINES section, the -P option designates the path where the device will download the software package. In the HTTP example, the path is http://<web server>/packages/test package.exe.

The next option is the -G option, which is the GUID, a unique number identifier for each package. This number identifier is generated by the Package Builder, and it helps prevent confusion during installation between packages with similar names.

Scripting guide for deployment scripts (.INI) files

You don't have to use the Create Software Distribution Script window to create the deployment script file. A deployment file is an .INI file containing the settings the device should use for installing a package. You can create your own deployment files in a text editor such as Notepad if you prefer.

A software distribution .INI script file has these components:

```
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe
/p="http://computer_name/95Packages/Acro32_95.exe"
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-66E3BC2DF01A0D4B2F88670DE4}
/Ac
/N
```

REMEXEC0 command parameters

The parameters for the REMEXEC0 command have been placed on separate lines to make the components more visible. When placed in an .INI file, the command needs to be on one line.

REMEXEC0 is the Remote Execute command. If you want to use more than one REMEXEC0 command in a single script file, increment the command each time it is used. For example, if you used three REMEXEC calls in a single .INI file, they should be REMEXEC0, REMEXEC1, and REMEXEC2. These commands don't need to increment if they're in separate files.

The C:\Program Files\LANDesk\LDClient parameter is the correct path to the SWD agent.

The /p parameter is the path statement where the device can download the package. For example:

```
/p="http://computer_name/95Packages/Acro32_95.exe"
```

The /g parameter points to a GUID identification number for the package. For example:

```
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-66E3BC2DF01A0D4B2F88670DE4}
```

If you use this parameter, the device will only download the package with that exact ID number. Use the Create Distribution Script window to generate this ID number, because it's embedded in the software package.

The /Ac parameter hides the install from users. They can only cancel the installation if they're prompted for something. The /Ab parameter hides the background. The /An parameter hides all of the UI and prevents any interaction (prompts from reaching the users.

The /Ah+ parameter heals a package that was previously installed, without prompting the user. The /Ah- parameter reinstalls a package that was previously installed, without prompting the user.

The /N parameter doesn't force a reboot on the device after the package is installed. The /R parameter forces a reboot on the device after the package is installed. If you don't use either the /N or /R parameters, the device will reboot only if files in use were updated or a reboot is needed to complete the installation.

An optional /D parameter opens a debug window used to view operational parameters for SDCLIENT.EXE. The debug window displays the package path and name, the GUID, any error or message codes, as well as the exit code returned to the Scheduled Tasks window.

If the software distribution script is designed to uninstall an existing application, two uninstall option parameters can be used:

- The /Au parameter uninstalls the last instance of a package and rolls back one install instance.
- The /All parameter uninstalls all instances of a package and completely removes the package.

If you follow these guidelines, you can create your own software distribution scripts and schedule them to be sent to devices. These scripts are stored in the DTM\Scripts folder on the core server.

Understanding software distribution error codes

From the console, the right panel in the **Scheduled tasks** window displays the task status. If you click Failed under the task, you can see devices that failed the job and the resulting messages and logs. The status and errors are logged to the following files:

- If the error occurred while attempting to access the package, the error is logged in the AICLIENT.LOG file.
- If the error occurred while processing the package (for example, copying files), the error is logged in the INST32.LOG file.

- The SDCLIENT.LOG file contains general summary information about each installation request received from the core server.

These log files are stored on each device. The following table lists the error codes you may encounter in these files.

Error code	Definition
101	The user cancelled the install.
102	File access was denied.
103	The password used isn't valid.
104	No network found, or incorrect path provided.
105	A download error occurred.
106	A socket could not be created.
107	Unable to open an HTTP session.
108	A CFG download error occurred.
109	A save CFG error occurred.
110	No save CFG folder exists.
111	A file access error occurred.
112	A get CFG error occurred.
113	Unable to create a backup CFG.
114	A spawn error occurred because another package is already being installed.
117	The backup directory can't be created.
180	Networking error. Can't initialize.
188	Timed out while downloading over HTTP.
189	HTTP connection aborted.

Error code	Definition
191	Host not found.
197	HTTP file not found.
201	The UNC file cannot be found.
202	The file was not found on the installation disk.
203	Unable to create a file in the specified location.
204	Not enough disk space on the destination drive for installation.
205	An invalid drive was specified, or the drive required for this install was not available.
206	The file has a long filename and can't be installed by the 16-bit install program. You still have the option to continue to install other files.
207	The specified file is not an executable.
208	Multiple uninstall registry entries exist with the same source path.
209	Unable to locate the uninstall executable.
210	Encountered an invalid compressed file, or HTTP error(s).
211	A successful AFXSOCKETINIT command must occur before using this API.
212	The network subsystem failed.
213	No more file descriptors are available.
214	The socket can't be created. No buffer space was available.
215	The specified address was already in use.
216	The connection attempt was rejected.
217	The provided host address was invalid.

Error code	Definition
218	The network can't be reached from this host at this time.
219	The attempt to connect timed out without establishing a connection.
220	The virtual circuit was aborted due to a timeout or other failure.
221	The virtual circuit was reset at the remote site.
222	A non-stated HTTP error occurred.
223	An HTTP error occurred; the file wasn't open for reading.
224	An HTTP error occurred; no content-length setting provided.
225	An HTTP error occurred; not enough memory available.
226	A memory allocation error occurred.
227	Unable to read the file.
228	Insufficient memory available.
229	The .CFG file has an error at line XX.
240	The temporary path specified is invalid. It can't be accessed or created. The target computer has a configuration problem.
301	This application has never been installed on this computer; it can't be uninstalled.

Appendix: Additional security scanner information

LANDesk Security Suiteincludes the Patch and Compliance tool as the main component of its comprehensive security management solution. Use this tool to: download updates for various security content type's definitions and patches; create, configure, and run security assessment scans, compliance scans, and remediation scans; enable security alerts; generate security reports, and more. For more information , see Patch and Compliance and Patch and Compliance help.

This section provides supplemental information about using the Patch and Compliance security scanner.

Read this section to learn about:

- Security scanner command-line parameters

Security scanner command-line parameters

The security scanner is called VULSCAN.EXE. The scanner supports the following command-line parameters:

Parameter name	Description
General parameters	
/AgentBehavior=ScanRepairSettingsID	Overwrites the default behavior of the security scanner (scan and repair settings) for only the current security assessment or remediation scan job. The ScanRepairSettings ID is a number value.
/ChangeBehaviors /AgentBehavior=ScanRepairSettingsID	Changes the default scan and repair settings for any subsequent security assessment or remediation scan job by writing the scan and repair settings to the device's local registry. Use the exact syntax to the left, with both switches in the command line. The ScanRepairSettings ID is a number value. **Note:** You can use this option to change the default scan and repair settings for a device without having to do a full agent configuration deployment to the device.
/ShowUI	Shows the scanner UI on an end user device.
/AllowUserCancelScan	Shows a Cancel button on the scanner UI that lets the end user cancel the scan.
/AutoCloseTimeout=Number	Timeout value in seconds.

Parameter name	Description
	Note: If the value is set to -1, then the scanner UI waits for the end user to manually close it.
/Scan=Number Code (0-8)	Identifies which security content type is being scanned for. The number codes for the different security content types are: 0 - vulnerability 1 - spyware 2 - security threat 3 - LANDesk updates 4 - custom definition 5 - blocked application 6 - software updates 7 - driver updates 8 - antivirus 100 - all types
/Group=GroupID	Identifies the security content group being scanned for. This option overrides specific content type parameters, if present.
/AutoFix=True or False	Enables or disables the autofix feature.
Repair parameters	
/Repair (Group=GroupID, or Vulnerability=VulnerabilityID, or Vulnerability=All)	Tells the scanner which group or vulnerability to repair (remediate). You can specify All for vulnerabilities in order to repair all detected vulnerabilities instead of a single vulnerability by its ID.
/RemovePatch=PatchName	Removes the specified patch from the patch repository.
/RepairPrompt=MessageText	Lets you display a text message that prompts the end user.
/AllowUserCancelRepair	A string that allows the end user to cancel repair if using a repair prompt.
/AutoRepairTimeout=Number	A timeout value of repair prompt in seconds. If it's set to -1, then the UI waits for user to close

Parameter name	Description
	manually.
/DefaultRepairTimeoutAction	A string for the default action for vulscan to take if timeout expires for repair prompt, acceptable values. Values include: start and close.
/StageOnly	A string to retrieve patch or patches needed for repair but don't install.
/Local (get files from peer)	Forces peer only download.
/PeerDownload	Same as /local.
/SadBandwidth=Number	Maximum percentage of bandwidth to use when downloading.
Reboot parameters	
/RebootIfNeeded	Use this parameter to reboot a machine if needed
/RebootAction	A string that determines vulscan's reboot behavior when repairing, acceptable values: always, never, or empty (anything else), If anything else, then vulscan will reboot if needed.
/RebootMessage	A string that displays text message to user in a reboot prompt.
/AllowUserCancelReboot	A string that allows user to cancel reboot if using a reboot prompt.
/AutoRebootTimeout=Number	Timeout value of reboot prompt in seconds, if set to -1, then UI waits for user to close manually.
/DefaultRebootTimeoutAction	A string that determines the action for vulscan to take if timeout value expires for reboot prompt, acceptable values: reboot, close, snooze.
/SnoozeCount=Number	Number of snoozes, vulscan decrements each time the user clicks snooze on the reboot prompt.
/SnoozeInterval=Number	Number of seconds for vulscan to sleep between snoozes.
MSI parameters	

Parameter name	Description
/OriginalMSILocation=path	Path to original MSI location.
/Username=username	Username for MSI directory.
/Password=password	Password for MSI directory.
Disable parameters	
/NoElevate	Don't launch vulscan via core tech.
/NoSleep	Prevents sleeping during definition scan (1/18th).
/NoSync	Doesn't get mutex, scans multiple instances.
/NoUpdate	Don't get a new version of vulscan.
/NoXML	Don't look for msxml.
/NoRepair	Same as autofix=false. Overrides autofix settings if present.
Data files parameters	
/Dump	Dumps vulnerability data directly from Web service.
/Data	Pulls in vulnerability data (from /dump).
/O=Path\Filename	Output scan results.
/I=Path\Filename	Input scan results.
/Log=Path\Filename	Overrides log file name.
/CoreServer=Server name	Identifies core server name.
/Reset	Removes delta file base information (wipes out application data directory).
/Clear or /ClearScanStatus	Clears all vulnerability scan information.

Appendix: Context-sensitive help

Antivirus help

LANDeskAntivirus features are accessed from the Security Configurations tool window (**Tools > Security > Security Configurations**).

Antivirus lets you download and manage antivirus content (virus definition files); configure antivirus scans; and customize antivirus scanner display/interaction settings that determine how the scanner appears and operates on target devices, and which interactive options are available to end users. You can also view antivirus-related information for scanned devices, enable antivirus alerts, and generate antivirus reports.

The main section for "LANDesk Antivirus" on page 366 introduces this complementary security management tool, which is a component of both LANDesk Management Suite and LANDesk Security Suite. In that section you'll find an overview, antivirus content subscription information, as well as step-by-step instructions on how to use Antivirus features.

This section contains the following online help that describes the Antivirus dialogs. From the console interface, these help sections are accessed by clicking the **Help** button on their respective dialog:

- "Antivirus Download Updates help" on page 596
- "Antivirus tasks help" on page 600
- "Antivirus settings help" on page 602

Antivirus Download Updates help

About the LANDesk Antivirus page on the Download Updates dialog

Use the **LANDesk Antivirus** page of the **Download Updates** dialog to configure settings for downloading virus definition file updates from LANDesk Security Suite services. You can select to download Antivirus content (virus definition/pattern files), specify when virus definition files are available to distribute to managed devices (immediately or after a pilot test period), and whether definition files are backed up.

You should be aware that the **Updates** page of the **Download updates** dialog includes several Antivirus updates in the definition type list, including one named LANDesk Antivirus Updates. When you select this type, both the scanner detection content AND the virus definition file updates are downloaded.

Antivirus updates are scanner definitions that detect:

- Installation of common antivirus scanner engines (including the LANDesk Antivirus agent)
- Real-time scanning status (enabled or disabled)
- Scanner-specific pattern file versions (up to date or old)
- Last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)

Antivirus scanner detection content versus virus definition content
Antivirus updates does not imply actual virus definition (or pattern) files. When you download third-party antivirus updates, only scanner detection content is downloaded to the default repository, but scanner-specific virus definition files are not downloaded. However, when you download LANDesk Antivirus updates, both the scanner detection content AND the LANDesk Antivirus-specific virus definition files are downloaded. LANDesk Antivirus virus definition files are downloaded to a separate location on the core server. The default virus definition file repository is the \LDLogon\Antivirus\Bases folder.

You must have the proper LANDesk Security Suite content subscription in order to download each type of security content.

A basic LANDesk Management Suite installation allows you to download and scan for LANDesk software updates, and to create and use your own custom definitions. For all other security content types, such as platform-specific vulnerabilities, spyware, and including virus definition (pattern) files, you MUST have a LANDesk Security Suite content subscription in order to download the corresponding definitions. For information about Security Suite content subscriptions, contact your reseller, or visit the LANDesk Web site.

After you specify the types of content you want to download and the other options on the Download updates dialog:

- To perform an immediate download, click **Update Now**. If you click **Apply**, the settings you specify will be saved and will appear the next time you open this dialog. If you click **Close**, you'll be prompted whether you want to save the settings.
- To schedule a download security content task, click **Schedule update** to open the **Scheduled update information** dialog, enter a name for the task, verify the information for the task, and then click **OK** to add the task to Scheduled tasks.

Task-specific settings and global settings
Note that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific. However, all of the settings on the other pages of the **Download updates** dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global settings it is effective for all security content download tasks from that point on.

To save your changes on any page of this dialog at anytime, click **Apply**.

The **LANDesk Antivirus** page contains the following options:

- **Virus definitions approved for distribution:** Displays the date and version number of the most recently approved virus definition files that are now available to distribute to your managed devices. Approved virus definition files are located in the default folder (\LDLogon\Antivirus\Bases) from which they are deployed to target devices as part of on-demand and scheduled antivirus scans. The exact time of the virus definition file update (downloaded from the LANDesk security content site, which has the very latest known pattern files) is noted in parentheses below this field.
- **Virus definitions currently in pilot testing:** Displays the date and version number of the virus definition files currently residing in your pilot folder, if you've downloaded virus definitions to that location. Pilot testing helps you verify the validity and usefulness of a virus definition file before using it to scan your managed devices for viruses. Virus definitions that have been downloaded to the pilot test folder can be deployed to designated "test" target devices.
- **Virus definition updates:**
  - **Immediately approve (make available to all computers):** Downloads virus definitions directly to the default folder (\LDLogon\Antivirus\Bases). Virus definitions downloaded to the default folder are approved and can be deployed to target devices for antivirus scanning.
  - **Restrict them to a pilot test first:** Download virus definition files to the pilot folder for testing purposes. Virus definitions in the pilot folder can be deployed to designated test machines before being deployed to your managed devices.

        - **Automatically approve pilot definitions after test period expires (during next update):** Automatically moves downloaded virus definition files from the pilot folder to the default virus definition folder when the next virus definition update after the time period specified below occurs. This option is available only if you're restricting virus definition file updates to a pilot test, and lets you automate the approval of definition files. If you don't enable this option, virus definition files in the pilot folder must be approved manually with the **Approve now** button.
        - **Minimum test period:** If you've enabled automatic approval of virus definitions in the pilot folder, this value specifies the duration of the test period. Be aware that during this period scheduled virus definition file update tasks are not processed.
    - **Show reminder dialog if definitions are out of date:** Displays a message on the core server console when virus definition files have not been updated in the past seven (7) days.
    - **Download virus definition files for LANDesk Antivirus 8:** Ensures virus definition files that were part of version 8 of LANDesk Antivirus are included in the download.
    - **Get latest definitions:** Starts an immediate virus definition file download process. The **Updating Definitions** dialog shows download progress.
    - **Approve now:** Lets you move virus definition files from the pilot folder to the default virus definition folder so that they can be deployed to target devices for antivirus scanning.
- **Virus definition backups:**
    - **Make backups of previous definitions:** Saves downloads of earlier virus definition files. This can be helpful if you need to go back to an older definition file to scan and clean infected files, or to restore a virus definition file that resolved a particular problem. (Virus definition file backups are saved in separate folders named by the date and time they were created, under: \LDLogon\Antivirus\Backups\)
    - **Number of backups to keep:** Specifies the number of virus definition file downloads to save.
    - **History: Lists all of the available virus definition file backups.**
    - **Restore:** Moves the selected virus definition file backup to the antivirus default folder so that they can be distributed to target devices.
    - **Delete:** Removes the selected virus definition file backup permanently from the core server.
- **Download now:** Immediately downloads the selected security content types. The **Updating Definitions** dialog shows progress and status of the download.
- **Schedule download:** Opens the **Scheduled download information** dialog, where you can type a unique name for this download task, verify the download settings, and click OK to save the task in the Scheduled task tool. (Note that only the definition types, languages, and definition and patch download settings are saved and associated when you create a particular task. Download settings on the other pages of this dialog, such as patch download location, proxy settings, and alerting settings, are global, meaning they apply to all the security content download tasks. However, you can change those settings at any time and they will be effective for all security content download tasks from that point on.)
- **View log:** Lets you select the location and level of detail in a log file containing virus definition file download information.
- **Apply:** Saves your selected download settings so that they are applied to the **Download updates** dialog and appear the next time you open the dialog.
- **Close:** Closes the dialog without saving your latest settings changes.

For a description of the options on the other pages of the **Download updates** dialog, see "About the Download Updates dialog" on page 651 in the Patch and Compliance help section.

Antivirus tasks help

About the Create LANDesk Antivirus task dialog

Use this dialog to create a task that updates virus definition files, configures antivirus scans on target devices (with antivirus settings), or both. Antivirus settings determine scanner behavior, scanned objects, and end user options.

On-demand antivirus scans
You can also run an on-demand antivirus scan on a device via the device's shortcut menu.

This dialog contains the following options:

- **Task name:** Identifies the antivirus scan task with a unique name.
- **Actions to perform:** Specifies what the task is going to do. You can select one or both of the actions.
  - **Update virus definitions:** Specifies the task will update the virus definition files based on the settings on the antivirus page of the Download updates dialog.
  - **Start antivirus scan:** Specifies the task will run an antivirus scan on target devices.
- **Create a scheduled task:** Adds the scan task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
  - **Automatically target all LANDesk Antivirus machines:** Adds managed devices that have been configured with the LANDesk Antivirus agent to the task's target devices list.
  - **Start now:** Runs the antivirus scan on devices with the LANDesk Antivirus agent, adding it to the Scheduled tasks tool, as soon as you and click **OK**.
  - **Update virus definitions (including pilot) on core:** Automatically updates virus pattern files before the scan is launched, including virus definition files that currently reside in the pilot folder. (Note: The Update virus definitions option above much be selected in order to use this option.)
- **Create a policy:** Adds the antivirus scan task as a policy to the Scheduled tasks window, where you can configure the policy's options.
- **LANDesk Antivirus settings:** Specifies antivirus settings used for the scan task. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates. Select one of the settings from the drop-down list. Click **Edit** to modify the options for the selected settings. Click **Configure** to create a new settings.
- **Virus definition files:** Displays information about the currently downloaded definition files. Click **Download updates** to go to the LANDesk Antivirus page of the Download updates dialog to configure and schedule a virus definition file download.

About the LANDesk Antivirus scan now task dialog

Use this dialog to run an immediate on-demand antivirus scan on one or more target devices.

1. Right-click the selected device (or up to 20 multi-selected devices), and then click **LANDesk Antivirus scan now**.
2. Select an antivirus settings.
3. Specify whether to update virus definition files before scanning. (Note: This option automatically updates virus pattern files before the scan is launched, including virus definition files that currently reside in the pilot folder.)

4. Click **OK**.

Antivirus settings help

About the LANDesk Antivirus settings dialog

Use this dialog to create and edit an antivirus settings. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates.

If you want to modify a device's default antivirus settings without redeploying an antivirus scan task, make your desired change to any of the settings on the various pages of the Antivirus settings dialog, assign the new settings to a change settings task, and then deploy the change settings task to target devices.

Once configured, you can apply antivirus settings to antivirus scan tasks and to change settings tasks.

This dialog contains the following pages:

- "About the Antivirus: General settings page" on page 602
- "About the Antivirus: Real-time protection page" on page 603
- "About the Antivirus: Virus scan page" on page 604
- "About the Antivirus: Scheduled scan page" on page 606
- "About the Antivirus: Virus definition updates page" on page 608
- "About the Antivirus: Quarantine/Backup page" on page 609

About the Antivirus: General settings page

Use this page to configure the basic antivirus scanner settings on target devices.

This page contains the following options:

- **Name:** Identifies the antivirus settings with a unique name. This name appears in the settings drop-down list on an antivirus scan task dialog.
- **Show LANDesk Antivirus icon in system tray:** Makes the LANDesk Antivirus icon appear in the device system tray. The icon's appearance depends on the status of antivirus protection, indicating whether real-time protection is enabled. If the arrow icon is yellow, real-time protection is enabled meaning the device is continuously being monitored for viruses. If the icon is gray, real-time protection is not enabled.

  Note: End users can double-click the icon to open the LANDesk Antivirus client and perform tasks. They can also right-click the icon to access the shortcut menu and select to run a scan and update antivirus files.

- **Enable email scanning:** Enables real-time email scanning on target devices. Real-time email scanning continuously monitors incoming and outgoing messages (supported applications include: Microsoft Outlook), checking for viruses in both the body of the message and any attached files and messages. Any detected viruses are removed.
- **Enable right-click scanning:** Provides an option on the LANDesk Antivirus client that allows end users to select a file, group of files, folder, or group of folders, and right click the selection to perform an antivirus scan.
- **Scan for risky software in addition to viruses (extended database):** Provides an option on the LANDesk Antivirus client that allows end users to scan for riskware (i.e., FTP, IRC, remote control utilities, etc.) using an extended database that is loaded on the managed device.

- **Allow user to add files and folders to Trusted Items list:** Provides an option on the LANDesk Antivirus client that lets users identify files and folders they don't want scanned for viruses. Files and folders in this list are ignored by an antivirus scan. Users should be made aware that they should move only safe files to their trusted items list.
- **CPU utilization when scanning:** Lets you control CPU usage on target machines when LANDesk Antivirus runs an antivirus scan.
- **Owner:** Lets you specify an owner for the antivirus settings in order to prevent unauthorized modification. Only the owner and users with the Administrator right can access and modify the settings. Other users can only view the settings. The public user option allows universal access to the settings.
- **Set as default:** Establishes this antivirus settings (including the option settings on all of the Antivirus settings dialog's tabs) as the default on target devices. Unless an antivirus scan task has a specific antivirus settings associated with it, the default settings are used during scan and definition file update tasks.
- **Restore defaults:** Restores the predefined default settings for all of the antivirus options on the dialog's tabs.

About the Antivirus: Real-time protection page

Use this page to enable and configure real-time file protection, which files to protect and what to exclude, and end user notification.

Real-time protection is an ongoing (background) scan of specified files, folders, and file types by extension. When real-time protection is running, files are scanned for viruses every time they are opened, closed, accessed, copied, or saved.

When real-time protection is enabled, the LANDesk Antivirus system tray icon is yellow. The icon is gray when real-time protection is turned off.

This page contains the following options:

- **Enable real-time file protection:** Turns on real-time file protection on target devices. Real-time file protection runs in the background and scans for known viruses according to the downloaded virus definition files
- **Show real-time messages on client:** Displays messages on target devices to notify users of certain LANDesk Antivirus activities. End users are notified when an infected file is detected, quarantined, deleted, skipped, or cleaned. Message dialogs show the path, file name, virus name, and a note telling the end user to contact their network administrator.
- **Allow user to disable real-time scanning for up to:** Provides an option on the LANDesk Antivirus client that allows the end user to turn off real-time file protection for a specified period of time. You should keep the amount of time to a minimum so that users can't disable real-time protection long term.
- **Exclude network paths:** Limits real-time file scanning to local drives, and does not include mapped network drives.
- **Scan all file types:** Specifies that files of all types on the target device are scanned by an antivirus scan. This may take a long time so it is a good idea to scan all file types with an on-demand scan rather than real-time protection.
- **Scan infectable files only:** Specifies that infectable files only are scanned. Infectable files are those types of files known to be vulnerable to virus infections. Scanning only infectable files is more efficient than scanning all files because some viruses affect only certain file types. However, you should make a habit of regularly scanning all the files with an on-demand scan in order to ensure devices are clean.

  Note: Infectable file types are identified by their format identifier in the file header rather than by their file extension, ensuring that renamed files are scanned. Infectable files include: document files such as Word and Excel files; template files that are associated with document files; and program files such as Dynamic Link Libraries (.DLLs), communication files (.COM), Executable files (.EXEs), and other program files. See below for a complete list of infectable file types.

- **Use heuristics to scan for suspicious files:** Utilizes the scanner's heuristic analysis capability when scanning target devices. Heuristic scanning attempts to detect files suspected of being infected by a virus by looking for suspicious behavior such as a program that: modifies itself, immediately tries to find other executables, or is modified after terminating. Using heuristic scanning may negatively affect performance on managed devices.
- **Exclude the following files and folders:**
  - **Add:** Opens the **Add excluded path** dialog where you can create new exclusions to specify the files, folders, or file types (by extension) you want to exclude from an antivirus scan associated with this settings.
  - **Edit:** Opens the selected exclusion so you can modify a file path, file name, file extension, and variables.
  - **Delete:** Removes the selected exclusion from the antivirus settings.

About the Add excluded path dialog

Use this dialog (accessed from the Real-time protection dialog) to add exclusions that specify objects that aren't scanned for viruses by either an antivirus scan or real-time protection. Antivirus scan tasks (and change settings tasks) associated with this antivirus settings will use these exclusions.

You can exclude specific files, entire folders, and file types by their extensions.

This dialog contains the following options:

- **Type:** Indicates the type of object you want excluded from antivirus scanning. Select a type and then enter its precise attributes in the Object field.
- **Object:** Type the full file path and name of (or browse to and select) the file or folder you want to exclude. If you selected the file extension type, type the extension's characters in the Object field.
- **Insert variable:** Allows you to use system environment variables to identify the path to a folder or an object that you would like to exclude from the antivirus scan or protection scope.

About the Antivirus: Virus scan page

Use this page to specify which files to scan for viruses, what to exclude from the scan, and whether to use heuristics to scan for suspicious files.

This page contains the following options:

- **Scan all file types:** Specifies that files of all types on the target device are scanned by an antivirus scan. This may take a long time so it is a good idea to scan all file types with an on-demand scan rather than real-time protection.
- **Scan infectable files only:** Specifies that infectable files only are scanned. Infectable files are those types of files known to be vulnerable to virus infections. Scanning only infectable files is more efficient than scanning all files because some viruses affect only certain file types. However, you should make a habit of regularly scanning all the files with an on-demand scan in order to ensure devices are clean. See below for a complete list of infectable file types.
- **Use heuristics to scan for suspicious files:** Utilizes the scanner's heuristic analysis capability when scanning target devices. Heuristic scanning attempts to detect files suspected of being infected by a virus by looking for suspicious behavior, such as: a program that is self-modifying, immediately tries to find other executables, or appears

changed upon termination. Using heuristic scanning may negatively affect performance on managed devices.

- **Exclude the following files and folders**
  - **Add:** Opens the **Add excluded path** dialog where you can create new exclusions to specify the files, folders, or file types (by extension) you want to exclude from an antivirus scan associated with this settings.
  - **Edit:** Opens the selected exclusion so you can modify a file path, file name, file extension, and variables.
  - **Delete:** Removes the selected exclusion from the antivirus settings.
- **Clean up registry:** Specifies the registry is included in the antivirus scan.

System restore point scanning
LANDesk Antivirus will scan the files in any system restore point folders that may exist on the managed device.

Infectable file types

Infectable file types are identified by their format identifier in the file header rather than by their file extension, ensuring that renamed files are scanned.

Infectable files include: document files such as Word and Excel files; template files that are associated with document files; and program files such as Dynamic Link Libraries (.DLLs), communication files (.COM), Executable files (.EXEs), and other program files. See below for a list of infectable file types by the file format's standard or original file extension.

- ACM
- ACV
- ADT
- AX
- BAT
- BIN
- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML
- HTT
- INF
- INI
- JS
- JSE

- JTD
- MDB
- MSO
- OBD
- OBT
- OCX
- PIF
- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH
- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD
- WSF
- WSH

About the Antivirus: Scheduled scan page

Use this page to enable and configure a recurring scheduled antivirus scan on target devices.

LANDesk Antivirus scan types
You can scan your managed devices for viruses with scheduled scans, on-demand scans, as well as real-time file and email protection. End users can also perform on-demand scans of their own computer.

This page contains the following options:

- **Have LANDesk Antivirus scan devices for viruses at a scheduled time:** Enables a recurring scheduled antivirus scan that runs on target devices according to the start time, frequency, time restriction, and bandwidth requirement you specify.
- **Change settings:** Opens the Schedule dialog where you can set the scheduling options. See "About the Schedule periodic antivirus scans dialog" on page 606.
- **Allow user to schedule scans:** Lets the end user create a local scheduled antivirus scan on their own machine.

About the Schedule periodic antivirus scans dialog

If you want this antivirus settings to include a recurring antivirus scan, use this dialog to specify start time, frequency, time restriction, and bandwidth requirement settings. Antivirus scan tasks (and change settings tasks) associated with this settings will use the rules defined here.

All criteria in this dialog that you configure must be met before the task will execute. For example, if you configure a schedule that repeats every day between 8 and 9 o'clock with a **Machine state** of **Desktop must be locked**, the task will only execute if it's between 8 and 9 o'clock AND the machine is locked.

This dialog contains the following options:

- **Start:** Click this option to display a calendar where you can select the day you want the task to start. Once you pick a day, you can also enter a time of day. These options default to the current date and time.
- **Repeat after:** Schedules the scan to recur periodically. Select the number of minutes, hours, and days to control how often the task repeats.
- **Time range:** If you want the task to run between certain hours, select the start and end hours. The hours are in 24-hour (military) time format.
- **Weekly between:** If you want the task to run between certain days of the week, select the start and end days.
- **Monthly between:** If you want the task to run between certain dates of the month, set the start and end dates.
- **Minimum bandwidth:** When configuring local scheduler commands, you can specify the minimum bandwidth criteria necessary for the task to execute. The bandwidth test consists of network traffic to the device you specify. When the time comes for the task to execute, each device running the local scheduler task will send a small amount of ICMP network traffic to the device you specify and evaluate the transfer performance. If the test target device isn't available, the task won't execute. You can select these minimum bandwidth options:
  - **RAS:** The task executes if the device's network connection to the target device is at least RAS or dialup speed, as detected through the networking API. Selecting this option generally means the task will always run if the device has a network connection of any sort.
  - **WAN:** The task executes if the device's connection to the target device is at least WAN speed. WAN speed is defined as a non-RAS connection that's slower than the LAN threshold.
  - **LAN:** The task executes when the device's connection to the target device exceeds the LAN speed settings. LAN speed is defined as anything greater than 262,144 bps by default. You can set the LAN threshold in agent configuration (**Tools > Configuration > Agent Configuration > Bandwidth Detection** page). Changes won't take effect until you deploy the updated configuration to devices.
  - **To computer name:** Identifies the computer that is used to test the device bandwidth. The test transmission is between a target device and this computer.
- **Machine state:** If you want the task execution criteria to include a machine state, select one from the drop-down list.
- **Additional random delay once all other filters pass:** If you want an additional random delay, use this option. If you select a random delay that extends beyond the time limits you configured for the task, the task may not run if the random value puts the task outside the configured time limits.
  - **Delay up to:** Select additional random delay you want.
  - **And at least:** If you want the task to wait at least a certain number of minutes before executing, select this option. For example, if you're scheduling an inventory scan, you could enter a five here so a computer has time to finish booting before the scan starts, improving the computer's responsiveness for the user.

About the Antivirus: Virus definition updates page

Use this page to configure virus definition (pattern) file updates scheduling, user download options, and access options, for target devices with this antivirus settings.

This page contains the following options:

- **Download pilot version of virus definition files:** Download virus definition files from the pilot test folder instead of from the default repository(\LDLogon\Antivirus\Bases) on the core server. Virus definitions in the pilot folder can be downloaded by a restricted set of users for the purpose of testing the virus definitions before deploying them to the entire network. When you create an antivirus scan task, you can also select to download the latest virus definitions updates, including those residing in the pilot test folder, then associate an antivirus settings with this option enabled to ensure that the test machines receive the latest known virus definition files. If this option is selected, virus definition files in the default folder (\LDLogon\Antivirus\Bases) are not downloaded.
- **Users may download virus definition updates:** Provides end users on target devices the option of downloading virus definition files by themselves. This option displays on the LANDesk Antivirus client and can be accessed from that dialog as well as by right-clicking the LANDesk Antivirus system tray icon.

  Note: When an end user downloads virus definition files, the device attempts to connect to servers in the following order: 1) preferred server (if one is configured); 2) core server; 3) LANDesk security content subscription website.

- **Schedule virus definition updates:** Enables a recurring scheduled virus definition file update that runs on target devices according to the start time, frequency, time restriction, and bandwidth requirement you specify.
- **Change settings:** Opens the Schedule dialog where you can specify the scheduling options.
- **Download from:** Specifies the source site from which virus definition files are downloaded. Depending on which option you select from the drop-down list here, one or both of the download source site options (core server and Internet security content server) described below are enabled and can be configured.
- **Core download options:** Lets you configure core server settings if you've selected one of the download source site options above that includes the core.
  - **Download updates as a single file if changed file count is greater than:** Specifies the maximum number of new or updated individual virus definition files that are downloaded separately before they are downloaded as a single compressed file.
  - **Disable peer download:** Prevents virus definition file downloads via peer download (the local cache or a peer in the same multicast domain).
  - **Disable preferred server:** Prevents virus definition file downloads via a preferred server. For more information about preferred servers, see "Software distribution" on page 143.
- **Internet download options:** Lets you configure security content server settings if you've selected one of the download source site options above that includes the Internet.
  - **Source site:** Specifies the security content server that is accessed to download the latest definitions to your database. Select the server nearest your location.
  - **Fall back to alternate source site on failure:** Automatically attempts to download updates from another security content server, where the antivirus signatures reside, if the specified source site is unable to transmit files.

About the Schedule periodic antivirus updates dialog

If you want this antivirus settings to include a recurring virus definition update, use this dialog to specify start time, frequency, time restriction, and bandwidth requirement settings. Antivirus scan tasks (and change settings tasks) associated with this settings will use the rules defined here.

For information about the options, see "About the Schedule periodic antivirus scans dialog" on page 606 above since it is a common dialog.

About the Antivirus: Quarantine/Backup page

Use this page to configure the size of the quarantine/backup folder, and the object restore options you want to make available to end users.

This page contains the following options:

- **Limit size of quarantine / backup folder:** Allows you to specify the maximum size of the shared quarantine\backup folder on target devices. This folder is a safe, isolated storage area on devices that have LANDesk Antivirus. By default, the quarantine storage size is 50 MB and quarantined objects are stored for 90 days. Objects in the quarantine\backup folder can be rescanned, deleted, or restored.

  Note: Quarantined files are automatically rescanned with the latest virus definitions whenever an on-demand scan is run or whenever the antivirus pattern files are updated on the device, in order to find out if any infected objects can be cleaned. If a quarantined file can be cleaned, it is automatically restored and the user is notified.

  Note: When a virus infection is discovered, the infected file is first backed up (with a *.bak extension in the \LDClient\Antivirus\ folder) and then cleaned. If it can't be disinfected the original file it is moved to the quarantine folder (with a *.qar extension in \LDClient\Antivirus folder). Then the virus string is removed and the file is encrypted so it can't be accessed or executed.

- **Maximum size:** Specifies the maximum size of the shared quarantine/backup folder on devices with the LANDesk Antivirus agent.
- **Restoring objects:** Specifies end user rights for restoring objects that have been quarantined.
  - **Allow user to restore suspicious objects:** Provides end users the option of restoring suspicious objects detected by an antivirus scan or by real-time protection. Suspicious objects are those which contain code that is either modified or reminiscent to that of a known virus. Suspicious objects are automatically quarantined. If this option is checked, end users can move the original file from the quarantine folder to a specified destination folder or to its original location, where it was stored before quarantining, disinfection, or deleting. Note that If real-time protection is running, the restored file is scanned and if it's still infected it's put back in the quarantine.
  - **Allow user to restore infected objects and risky software:** Provides end users the option of restoring infected objects detected by an antivirus scan or by real-time protection. Infected objects are those containing harmful code which is detected by a known viruses definition (pattern or signature) file. Infected objects can further damage managed devices. Risky software is essentially client software that has the possibility of being risky for the end user. For example: FTP, IRC, MIrc, RAdmin, or remote control utility software. (In the case of a false-positive scan result, the end user may feel confident and comfortable enough to restore the file. This option lets users restore files to network shares. If they restore an infected file to the original location, the next antivirus scan will

detect the same virus, even if it's false-positive, and simply put the file back in quarantine.)

  - **User must enter password to restore objects:** Requires users to enter the specified password before they can restore suspicious or infected objects, or risky software. The user is prompted to enter the password when they attempt to restore the object from the quarantine/backup folder. If you enable this option to password protect quarantined objects, you must share this password with the users you want to be able to restore those objects.
  - **Password:** Enter the password needed for users to restore quarantined objects.
- **Deleting files:** Specifies whether files are automatically deleted.
  - **Automatically delete quarantine files:** Indicates all quarantined files older than the specified period will be automatically deleted.
  - **Automatically delete backup files:** Indicates all backed up files older than the specified period will be automatically deleted.

Inventory help

About the Inventory window

Use the **Inventory** window to view a device's complete inventory, including the following components:

- **BIOS:** Type, date, ID bytes, manufacturer, ROM version, SMBIOS version, and system model for the BIOS. The BIOS permanently resides in the computers ROM (read-only memory) and enables the computer's memory, disk drives, and monitor to communicate.

Additional BIOS information appears in the Inventory window as BIOS text strings. To view and search BIOS text strings, expand the **BIOS** object, select **BIOS Strings**, right-click the **Data** attribute and select **Properties**, and then click **Extended Values**. During an inventory scan, the available text strings are exported to the BIOS to a text file, LDBIOS.TXT. You can set up a query in the LDAPPL3.INI file that outputs one or more of the BIOS text strings to the console. For more information, see "Appendix: Additional inventory operations and troubleshooting" on page 557 .

- **Bus:** Bus type. The bus connects the microprocessor, disk drives, memory, and input/output ports. Bus types can be ISA, EISA, VESA Local Bus, PCI, and USB.
- **Coprocessor:** Type of coprocessor, if present. The coprocessor is distinct from the main microprocessor, though it can reside on the same motherboard or even the same chip. The math coprocessor evaluates floating point operations for the main microprocessor.
- **Custom data:** Any custom data enabled for the inventory scanner.
- **Database:** Database driver and version information.
- **Environment:** File locations, command path, system prompt, and other variables for the Windows environment.
- **Health:** Device health as determined by the LANDesk agent.
- **Keyboard:** Keyboard type attached to the device. Currently, the most common type of keyboard is the IBM-enhanced keyboard. Code page is the language the keyboard uses.
- **LANDesk Management:** Information about the agents, client manager, and Alert Management System (AMS). Also contains information about the inventory scanner and initialization files.
- **Local users and groups:** The local Windows user groups and group membership.

- **Mass Storage:** Storage devices on the computer, including floppy drives, hard disks, logical and tape drives, and CD-ROM. The hard disk and floppy drive objects include head, number, sector, and total storage attributes.
- **Memory:** Page file, physical, and virtual memory attributes. Each of these memory objects includes byte attributes. The first byte is the amount of memory available. The second byte is the total memory.
- Motherboard
- **Mouse:** Type of mouse attached to the device. Mouse type values include PS/2, serial, and infrared.
- Multimedia files
- **Network:** Network adapter, NIC address, and the adapter's node address information. The Network object includes information for each protocol loaded on the computer. Typical values include IPX*, NetBEUI, NetBIOS, and TCP/IP objects.
    - **IPX** is a protocol that NetWare* servers can use to communicate with their devices and other servers. The IPX object contains the address, network number, and node address attributes.
    - **NetBEUI** allows a computer to communicate with Windows NT/2000, Windows for Workgroups, or LAN Manager servers. Microsoft now recommends using TCP/IP for these connections.
    - **NetBIOS** is an interface (API) for applications to send and receive packets to each other over TCP/IP, NetBEUI, or IPX.
    - **TCP/IP** is a protocol that enables a computer to communicate over the Internet and with WANs. This object contains the address (contains the computer's TCP/IP address), host name (contains the computer's DNS context), IP routing enabled, and NetBIOS resolution (uses DNS and WINS proxy enabled attributes).
- **Network Adapters:** Attributes for every installed network adapter on the device.
- **OS:** Operating system, drivers, services, and ports. These objects and their attributes vary according to the configurations of the loaded drivers and services.
- **Ports:** Objects for each of the computers output ports (serial and parallel). Each output port contains address and name attributes. The address attribute contains the hardware address for the port.
- **Power management:** Power management settings on the device.
- **Printers:** Objects for each printer connected to the computer, either directly or through a network. The printer objects contain driver, name, number, and port attributes. The port attribute contains either the network queue or the port the printer is connected to.
- **Processor:** Attributes of the device's CPU. Detects Intel, Motorola 680x0, and PowerPC processors.
- **Resources:** Objects for every hardware resource of the computer. Each hardware resource object contains attributes that describe the type of resource and any ports and interrupts it is using.
- **Security:** Antivirus software and version.
- **Software:** Objects for every software application installed on the device's hard drive. Each software program object lists attributes that typically contain the software name, location, and version number.
- **System:** Motherboard and chassis information.
- **ThinkVantage Technologies:** Lenovo ThinkVantage technologies software information.
- **Video:** Objects for each video adapter on the device. The video adapter object typically contains attributes that describe the resolution and the number of supported colors.

About the Inventory attribute properties dialog

Use this dialog to view an attribute's properties. The **Characteristics** tab can display the following information. Depending on the attribute and whether you are adding, editing, or viewing an attribute, not all fields may appear.

- **Name:** The name of the core database attribute whose properties you're viewing.
- **Value:** The value assigned to this inventory attribute.
- **User defined:** Indicates whether the selected attribute was defined by the user or not. This option can't be changed.
- **Format specifier (Integer values only):** Notation used to display the value in appropriate form. For example, %d MB displays the attribute value without decimal values; %.1f MB displays the attribute value to the first floating decimal point in MB units. If no factor value is entered, this format specifier must describe integer values (%d). If a factor value is entered, this format specifier must describe floating point values (%f).
- **Factor (Integer values only):** Integer value used to divide the attribute into units. If you change the factor value, you must enter the appropriate code in the format specifier field. For example, to view the number of Megabytes if the attribute is recorded in Kilobytes, enter the value 1000.
- **Formatted value:** Sample text demonstrating the specified format and factor.

About the Inventory change settings dialog

Use this dialog to select which inventory attributes are logged when changes occur at individual devices, and to determine where those changes are logged.

- **Current inventory:** Lists all objects stored in the core database. Click an object to display its attributes in the Log event in list. Expand an object group to see the data objects contained within it.
- **Log event in:** Lists the attributes of the inventory object selected in the Current inventory list.

To set where inventory changes are logged, select an attribute and check one or more options. Check the **Inventory** option to log inventory changes in the device's **Inventory changes history** dialog. Check the **NT Log** option to log inventory changes in the Windows NT event log. Check the **AMS** option to send inventory changes as an alert via AMS (configure AMS alerts with the Alert Settings tool).

- **Log/Alert severity:** Lists the alert priority options. This feature is dimmed until an attribute is actually selected. You can select a severity level of None, Information, Warning, or Critical.

About the Inventory changes history dialog

Use this dialog to view a device's inventory changes. You can also print and export the inventory changes history from this dialog.

- **Device Name:** Displays the name of the device(s) selected in the console's network view for which inventory change data is requested.
- **Component:** Identifies the system component that has changed. (Only components selected in the **Inventory Change Settings** dialog can appear here.)
- **Attribute:** Identifies the specific component attribute being logged.
- **Time:** Indicates when the change occurred.
- **New Value:** Shows the new (changed value for the listed attribute).
- **Old Value:** Shows the old (previous value for the listed attribute).

- **Print:** Opens a standard print dialog where you can print the contents of the inventory changes history.
- **Export:** Opens a Save As dialog where you choose a name and location for the exported .CSV file containing the inventory changes history.

Note: The **Inventory changes history** dialog box shows the history in chronological order. You can't sort the data by clicking on the column headers.

About the Create/Edit a Custom Data Form dialog

Custom data forms are not supported in LANDesk Security Suite
Custom data forms is not available with a LANDesk Security Suite only license. You must have a full LANDesk Management Suite license in order to use the custom data forms feature.

Use this dialog to create or edit a custom data form.

- **Form name:** Identifies the form and appears on the form viewer when a user fills out the form.
- **Description:** Provides additional information to users about the form.
- **Add:** Opens the **Add question** dialog where you can create a new question for the form.
- **Edit:** Opens the **Edit question** dialog where you can edit any of the question's options.
- **Delete:** Removes the question from the form.
- **Page break:** Controls the layout of the form by adding page breaks to group questions on pages. When there's a page break, users click the Next button to proceed to questions on the next page.

Note: The maximum number of questions per page is nine.

- **Preview:** Opens the form so that you can preview how it will look for users. In preview mode, you don't have to fill in any data and nothing you type is saved.

About the Add/Edit question dialog

Use this dialog to create or edit questions that appear on the custom data form. Forms consist of questions and a place for users to put their answers. First, identify the question:

- **Question text:** One-line description of what's being asked for. This text appears beside the data field.
- **Inventory Name:** Name of the database field in the core database. If you wanted to query the core database for this item, the label ID is what you would query on.
- **Description:** Additional information that appears when users click Help (or press F1 while in this question's data field).

You also need to specify what type of data field (control to show beside each question, and if it is required. The available data fields are:

- **Edit box: Users** type their answer in an editable text box.
- **Combo box (edit list):** Users select one of the predefined list items, or type in a new one of their own.
- **Combo box (fixed list):** Users select one of the predefined list items.
- **Make the control a required field to fill out:** Forces the user to answer the question. The user can't finish a form or move to the next form page before responding to required fields.

About the Add items dialog

Use this dialog to add items to a drop-down list that the user can choose from when answering that question on a form.

- **Item name:** Identifies the item. This name appears in the question's drop-down list.

- **Items list:** Lists all the items that appear in the question's drop-down list.
- **Insert:** Places the item in the Items list.
- **Delete:** Removes the item from the Items list.

About the Select Multiple Forms to Distribute dialog

Use this dialog to create a group of forms that shows the group name and lists available forms that can be part of a group.

- **Name of group:** Identifies the group in the **Custom data forms** window.
- **Available forms:** Lists all of the available forms you can add to the group.
- **OK:** Saves the group and closes the dialog.
- **Cancel:** Closes the dialog without saving the group.

Local accounts management help

About the New user dialog

Use this dialog to create a new user. For more information, see "Managing local users" on page 270.

- **User name:** Specifies the user name for the new user
- **Full name:** Specifies the full name of the user.
- **Description:** Provides a description of the user
- **Password:** Specifies a password for the user to authenticate to the console.
- **Confirm password:** Confirms the password.
- **User must change password at next logon:** Causes the user to have to change their password upon initial logon into the console.
- **User cannot change password:** Disallows the users from changing the password.
- **Password never expires:** Causes the password to never expire, so the user won't have to change the password.
- **Account is disabled:** Disables the account.

About the Edit user dialog

Use this dialog to edit the user properties. The dialog consists of three configuration tabs, **General**, **Member of**, and **Profile**.

For more information, see "Managing local users" on page 270.

General

Use this configuration page to specify the user name, full name, and description of the user. You can also change some of the account properties.

- **User name:** Specifies the user name of the user (if available).
- **Full name:** Specifies the full name of the user.
- **Description:** Specifies the description of the user
- **User must change password at next logon:** Specifies if the user to has to change their password upon logging in to the console.
- **User cannot change password:** Specifies if the user can change their password.
- **Password never expires:** Specifies if the password will expire.
- **Account is disabled:** Specifies if the account is disabled.

- **Account is locked:** Unlocks the account so the user can authenticate to the console. This option is available when the user has unsuccessfully tried to log in to their account over three times in one session.

Member of

Use this configuration page to assign the user to groups.

- **Selected groups:** Lists the groups the user is a member of.
- **Add:** Launches the **Select groups** dialog, which enables you to add the groups you want the user to be a member of.
- **Remove:** Removes the user as a member of the selected groups and removes the groups from the list.

Profile

Use this configuration page to specify the account information for the user.

- **User profile path:** Specifies the network path to the user's account and profile.
- **Logon script:** Specifies the logon scripts.
- **Local path:** Specifies a local path as the home directory.
- **Connect:** Specifies a network directory as the home directory. Select a drive and then insert the network path.

About the Group properties dialog

Use this dialog to configure the group. For more information, see "Managing local groups" on page 271.

- **Group name:** Specifies the name of the group.
- **Description:** Provides a description of the group.
- **Members:** Lists the users that belong to the group.
- **Add:** Launches the **Select users** dialog, which enables you to add users to the group.
- **Remove:** Removes the selected users from the group.

Managed device help

The **Agent configuration** window (**Tools > Configuration > Agent configuration**) is where you customize device agent configurations. Use the **Agent configuration** dialog to specify the agents you want to install and the options for those agents. You can create as many agent configurations as you want. Only one configuration can be the default. You can use this window to create Windows, Macintosh, Linux, and server agent configurations.

To create a configuration

1. Click **Tools > Configuration > Agent configuration**.
2. Click the **New** button to create a new Windows configuration. Click the **New Mac** button to create a new Macintosh configuration.
3. Complete the **Agent configuration** dialog as described in the following sections. Click **Help** on a page for more information.

Note: If you use the **Agent configuration** dialog to create a new default agent configuration, be aware that all devices who are configured by WSCFG32 using login scripts will be automatically reconfigured with the new default configuration settings the next time they log in, even if their current settings match the new default settings.

The following sections describe the **Agent configuration** dialog pages.

About the Agent configuration dialog's Start page

The **Agent configuration** dialog's **Start** page contains the following options:

- **Configuration name:** This option appears above all dialog pages. Enter a name that describes the configuration you're working on. This can be an existing configuration name or a new one. This name appears in the **Agent configuration** window.
- **Default configuration:** Shows whether this configuration is the default configuration that gets installed. The only way to change this option is by clicking **Set as default** from the configuration's shortcut menu.

Agent components to install (Standard):

- **Standard LANDesk agent:** Installs the standard LANDesk agent that forms the basis of communication between devices and the core server. This option is required. You can't disable it, but you can customize the components associated with it. (Note the security scanner is automatically installed with the standard LANDesk agent, but you configure it with the options on the security and patch scan page below.)
- **Custom data forms:** Presents a form to users for them to complete. You can query the core database for the data users enter. Use this to retrieve customized information from users directly.
- **Remote control:** Lets you take control of a device or server from across the network. Minimizes the time it takes to resolve customer issues from a centralized help desk. Use this to provide remote management of devices across the LAN/WAN.

Power Management:

- **Power Management:** Allows you to control the power consumption on your managed computers from a central location. You can easily create and deploy power management policies and generate reports to evaluate financial and power savings. You control the conditions under which computers and monitors stand by, hibernate, or power down. However, users can delay specific power management actions using a client-side user interface to ensure that unsaved data is protected.

Distribution:

- **Software distribution:** Automates the process of installing software applications or distributing files to devices. Use this to install applications simultaneously to multiple devices or to update files or drivers on multiple devices.

Security:

- **LANDesk Antivirus:** Installs the Antivirus agent on managed devices. Antivirus uses the security scanner (installed with the standard LANDesk agent) to scan for and identify viruses on managed devices, and to provide options for handling infected files and folders. Administrators download virus definition updates and configures virus scans at the console, including how the Antivirus client displays on managed devices and which options are available to the end user. You must first select the **Antivirus** agent checkbox on the Agent configuration's **Start** page in order to configure the **Antivirus** page under **Security**.
- **Endpoint Security:** Installs the Endpoint Security agent on managed devices. Endpoint Security protects your managed devices from zero-day attacks, firewall intrusions, and unauthorized device connections. Endpoint Security services is comprised of these separate and complementary components: HIPS, Firewall, and Device Control.

Real-time Inventory and Monitoring:

Provides several methods to monitor a device’s health status. While alert rulesets are defined at the Core Server Console and deployed to multiple devices, on individual devices you can define performance monitoring counters to monitor specific performance issues.

- **Baseline components:** Installs an agent that monitors system hardware such as fan speeds, disc space, and over all temperature of the device.
- **Extended components:** Installs an agent that monitors system process, services, and overall performance.

Other options:

- **Select all:** Selects all available agents in the **Agents to install** list.
- **Clear all:** Clears all available agents in the **Agents to install** list, except for the **Standard LANDesk agent**, which is mandatory.
- **Defaults:** Selects all agents in the **Agents to install** list, except for the security agents.
- **Perform full Inventory scan during installation:** When this configuration is installed on clients, whether to do a full inventory scan during the agent installation. The default is checked.
- **Show start menu on end user device:** When checked, creates Windows Start menu entries for installed agents that have a user interface. Clearing this option installs the agents but doesn't create any Start menu entries.
- **Temporary install directory:** Specifies the temporary folder used on managed devices during agent installation. This folder must be writeable for agent installation to succeed.

Deploying the standard LANDesk agent

All Management Suite components require the standard LANDesk agent (formerly known as CBA), which is installed by default on all device installations. Among other things, the standard LANDesk agent provides device discovery and manages core server/device communication.

By default, the standard agent includes the LANDesk Security Suite security scanner.

Use the Standard LANDesk agent pages to configure the Standard LANDesk agent, which includes these components and settings:

- Inventory scanner
- Local scheduler
- Bandwidth detection
- Device reboot options

About the Agent configuration dialog's Standard LANDesk agent page

Use this page to configure certificate-based security and what scope devices using this configuration will have.

Trusted certificates

Select the core server certificates you want devices to accept. Devices will only communicate with cores and consoles they have certificates for. For more information on certificates and copying them from other core servers so you can select them here, see "Agent security and trusted certificates" on page 81.

Below the trusted certificates box you can modify the core server that devices using this agent configuration will communicate with. By default, this box contains the current core server. The core name can either be a Windows computer name, an IP address, or fully-qualified domain name. A fully-qualified domain name for a core may be necessary if you'll be pushing agent configurations to devices in multiple domains or anytime a device can't resolve the core name unless it is fully-qualified. Managed devices will use the information you enter here to communicate with the core server, so make sure the name you enter is resolvable from all devices that will receive this configuration.

The core name you enter here as part of an agent configuration are added to a device's registry under:

- HKLM\Software\Intel\LANDesk\LDWM\CoreServer

Once you've selected trusted certificates, and changed the core name if necessary, you can test them. When you click **Test**, a message box appears indicating whether the device name or IP address you entered was resolvable. Note that the **Test** button doesn't ping the device you entered or verify that the name or IP address belongs to a core server.

Location (scope)

If you want devices to be included in scopes that are based on custom directories, enter a directory path in the **Path** field. The path you enter here defines the device's computer location inventory attribute. Scopes are used by Management Suite role-based administration to control user access to devices, and can be based on this custom directory path.

Custom directory paths use a format that's similar to a file path, but with forward slashes as separators. If you want to use custom directory-based scopes, first decide how you want to categorize your devices for role-based administration. You might do categorize devices by geographic locale, department or group name, or any other organizational detail you prefer.

Directory paths you enter here as part of an agent configuration are added to a device's registry under:

- HKLM\Software\Intel\LANDesk\Inventory\ComputerLocation

You don't have to fill in this field. If you leave it blank, the device's computer location attribute is defined by its Active Directory or eDirectory path.

When the inventory scanner is run on a device, it records the device's computer location inventory attribute. If you entered a custom directory path in the **Path** field, that path is the directory the scanner records. If you left the custom directory path blank, the scanner tries to populate the computer location inventory attribute with the device's Active Directory or NetWare eDirectory path. If neither a custom directory path or an LDAP-compliant directory is found, the computer location attribute isn't defined. However, the device can still be accounted for in both query scopes or device group scopes.

For more information on how scopes are used in Management Suite role-based administration, and how you can define a scope using custom directory paths, see "Role-based administration" on page 44.

About the Agent configuration dialog's Inventory scanner page (under standard LANDesk agent)

The **Agent configuration** dialog's **Inventory scanner** page contains the following features:

- **Manual update:** The software list used to exclude titles during software scans is loaded down to each remote device. Each time the software list is changed from the console, you must manually resend it to remote devices.
- **Automatic update:** Remote devices read the software list from the core server during software scans. If this option is set, each device must have a drive mapped to the LDLOGON directory on the core server so they can access the software list. Changes to the software list are immediately available to devices.
  - **Update using HTTP:** Beginning with Management Suite8, the inventory scanner can use HTTP for LDAPPL3.INI file transfers. This allows the scanner to support Targeted Multicast features like polite bandwidth and peer download. Peer download allows devices needing LDAPPL3.INI updates to check with the core server for the latest version's date, then broadcast to peers on their subnet to see if a peer has the update in its multicast cache. If a peer has the update, the

file transfer happens on the local subnet without generating network traffic across routers or WAN links.

Run Inventory Scans:

- **Event-driven scans:** Configures the inventory scanner schedule on the managed device. By default the scan is set for once a day to scan the device and report back to the core server.
- **When user logs in:** Runs the inventory scanner when the user logs into the managed device.
- **Max random delay:** Specifies a time range during which the task may run. This delay allows tasks that run on login to not run all at the same time, assuming the delay interval is long enough.
- **When IP address changes (mini scan only):** The IP address trigger only sends a mini scan to the Core Server which makes the inventory much faster in IP address changes
- **Change settings:** Changes settings and configures a custom schedule based on time, day of week, or month, whether a user is logged in, on IP address changes, and available network bandwidth. The default schedule is to run a scan every day with a random delay of up to one hour.

About the Agent configuration dialog's Local scheduler page (under standard LANDesk agent)

The local scheduler agent enables Management Suite to launch device tasks based on a time of day or bandwidth availability. The local scheduler agent is most useful for mobile computers that may not always be on the network or may connect to the network via a dialup connection. For example, you can use the local scheduler to allow mobile computer package distribution only when those devices are on the WAN.

When you schedule software packages for distribution, or when you create application policies, you can specify which bandwidth the packages or policies require before they are applied.

The local scheduler runs as a service on Windows NT/2000/XP, or as a pseudo-service on Windows 95/98.

The **Local scheduler** page contains the following features:

- **Frequency at which the agent polls the local registry for tasks:** How often the local scheduler checks for tasks. The default is 10 seconds. The polling interval you select is stored on the local computer.
- **Bandwidth detection frequency:** How often the local scheduler should check bandwidth. The default is 120 seconds. Bandwidth checks happen only when there's a pending scheduled task.

About the Agent configuration dialog's Alerting page (under standard LANDesk agent)

Alert rulesets define which events require immediate action or need to be logged for your attention. A ruleset contains a collection of alert rules, each of which has a corresponding alert action. When you define an alert ruleset you can deploy it to one or more devices to monitor the items that are important for that kind of device.

You can deploy one of the predefined rulesets or you can deploy rulesets you've created inside the alerting tool.

The Alerting page contains the following features:

- **Add:** Click **Add** to add an existing ruleset to the **Selected alert ruleset** list. Rulesets in this list will be deployed to devices receiving this agent configuration.

- **Remove:** Click a ruleset and click **Remove** to remove it from the **Selected alert ruleset** list.

About the Agent configuration dialog's Bandwidth detection page (under standard LANDesk agent)

Bandwidth detection enables bandwidth detection between devices and the core server. You can limit Management Suite actions such as software distribution based on available bandwidth. Use this option if you have remote devices or devices that connect to the network via a slow link.

The **Agent configuration** dialog's **Bandwidth detection** page contains the following features:

- **Choose bandwidth detection method:** Select whether to use ICMP or PDS for bandwidth detection. ICMP sends ICMP echo requests of varying sizes to the remote device and uses the round trip time of these echo requests/responses to determine the approximate bandwidth. ICMP also distinguishes between LAN (high speed) and WAN (slow, but not dialup connections). However, not all routers or devices support ICMP echo requests.
  If your network isn't configured to allow ICMP echo requests, you can select PDS. The PDS bandwidth tests aren't as detailed, but they detect either a LAN or a low-bandwidth RAS (typically dialup connection). The PDS method only works if the PDS service is running on the package server. You can install this service by deploying the standard LANDesk agent to the package server.
- **LAN threshold, in bits per second:** The threshold that classifies a connection as WAN rather than LAN. The default is 262144 bps.

About the Agent configuration dialog's Device reboot options page (under standard LANDesk agent)

Once you install Management Suite agents on devices, they may need a reboot to complete the agent configuration. The **Agent configuration** dialog's **Device reboot options** page contains the following features:

- **Do not reboot devices after configuration:** Devices won't reboot, even if the selected components require a reboot. If a reboot is necessary, components won't work correctly until the device reboots.
- **Reboot devices if necessary:** Reboots devices only if a selected component requires a reboot.
- **Reboot with user option to cancel:** If a selected agent requires a reboot, users will have the option to cancel the reboot. If a reboot is necessary, components won't work correctly until the device reboots. You can select how long the reboot prompt stays on the user's screen before the computer reboots. This timeout is useful for users that are away from their computers when the device deployment happens.
- **Allow user to cancel reboot within this time period:** If you want to give users a chance to cancel the reboot before it happens automatically, enter how long you want the reboot prompt to appear.

About the Agent configuration dialog's Software usage monitoring page (under standard LANDesk agent)

The **Software usage monitoring** page is used to track usage statistics for Software License Monitoring. This feature collects information on three types of data: usage statistics from software license monitoring, additional inventory information, and application blocking capabilities.

The Software Usage Monitoring window contains the following options:

- **Monitor software usage:** Enables tracking of software through software licensing monitoring, inventory scans, and application blocking through the application blocker feature.

Deploying custom data forms

You can create and distribute custom data forms to collect device information that will supplement the standard information available in the core database. The forms you create using the Form Designer can be distributed by a device deployment service or by using the **Agent configuration** dialog.

Customize the forms that are distributed to devices in your management domain using the form designer. For more information, see "Using custom data forms" on page 97.

About the Agent configuration dialog's Forms sent with agent page

The custom data forms section consists of two pages. The **Custom data forms** page contains the following features:

- **Manual update forms:** Selected forms are sent to each device. If the forms change or new forms are added, you must manually resend the forms to remote devices.
- **Automatic update:** Remote devices check the core server for updated forms each time the inventory scanner is run, such as at startup. Each device must have a drive mapped to the LDLOGON directory on the core server to access the updated forms.
- **Display forms to end user:** Choose how remote devices access custom forms:
    - **On startup:** The selected forms run automatically at startup on each device.
    - **When inventory scanner runs:** The selected forms run only when the inventory scanner is run on each device. The inventory scanner runs automatically on startup, and can be run manually by devices at any time.
    - **When launched from the LANDesk program folder:** The selected forms appear as items in the device's LANDesk Management folder. They aren't automatically run.

The **Forms sent with agent** page lists all defined custom data forms. Mark which forms are made available to devices receiving this configuration task. You'll have to create forms (**Tools > Configuration > Custom Data Forms**) before they can appear in this list.

Deploying software distribution

Software distribution automates the process of installing software applications and distributing files to devices. Use this agent to install applications simultaneously to multiple devices or to update files or drivers on multiple devices.

Software distribution uses a Web or file server to store packages. Devices access this package server when downloading a package. You'll need to configure a package server as described in the software distribution chapter in the *User's Guide*. You can deploy the software distribution agent to devices before you set up a package server. For more information, see "Software distribution" on page 143.

About the Agent configuration dialog's Software distribution page

The **Agent configuration** dialog's **Software distribution** page contains the following features:

- **Client destination:** The location where deployed virtualized applications are stored on managed devices. This option has no effect if you aren't distributing virtualized applications created with the LANDesk Application Virtualization add-on.

- **Enable LDAP group targeting:** Allows virtual access to virtual applications to be assigned to specific OUs or groups from an active directory.

About the Agent configuration dialog's Policy options page (under software distribution)

The policy-based distribution agent enables you to automatically install sets of applications on groups of devices. Use this agent to manage groups of devices that have common software needs.

The LANDesk software deployment portal runs on managed devices and shows available software for that managed device. To display available software, the software deployment portal needs to get policy information periodically from the core server. Policy updates happen when:

- A user launches the LANDesk software deployment portal from the Windows Start menu.
- At logon if the run at logon **LANDesk software deployment portal** option is checked.
- At logon if the run at logon **Update policy information from core** option is checked.
- At the local scheduler interval you specify when you click the **Change settings** button. By default, managed devices use the local scheduler to get policy updates once a day .

The **Policy options** page contains the following features:

- **When user logs on:** If checked, the managed device updates policy information after a user logs on. The **Max random delay** lets the user delay the update by the time entered (in hours).
- **When IP address changes:** If checked, the managed device updates policy information when the IP address changes.
- **Change settings:** Use this to change how often and when the local scheduler will look for policy updates. This schedule is in addition to any of the run at logon options you check.

About the Agent configuration dialog's LaunchPad page (under software distribution)

Use this page to configure what LaunchPad customization end-users can do. The LaunchPad organizes links to deployed software on managed devices. Deployed software can be local, hosted, or just-in-time installed applications. The LaunchPad page contains the following features:

- **Allow users to size LaunchPad panes:** Allows users to move and resize the panes.
- **Allow users to move and dock LaunchPad panes:** Lets users to dock panes in any part of the desktop.

About the Agent configuration dialog's Portal page (under software distribution)

The Portal window on managed devices lists all software distribution package tasks that have been distributed using a policy based delivery method. Use this page to customize the Portal window's appearance.

A policy-based delivery method behaves differently from a push in that it requires the managed device to initiate the request for the policies. This means the package isn't pushed to the device from the core server, but its details are stored in the database on the core server until the managed device queries the core server for any policy-based software distribution tasks assigned to it. When the portal is opened it automatically launches the policy sync tool to update its list with any new tasks that have been assigned to the managed device.

The Portal window contains the **Optional columns** and **Display columns and order for Application** fields. These fields are used to lay out the options for customizing additional information about all packages in the LANDesk Desktop Manager Software Deployment Portal window on the managed device. The Software Deployment Portal window contains the **Available** and **History** tabs that are set up in the Agent configuration **Portal** page. The **Optional columns** field enables you to arrange the **Application** and **History** columns that appear on the tabs and group the information in a logical way.

The Portal page contains the following features:

- **Application:** Displays packages that are currently listed for optional or recommended user initiated software deployment.
- **History:** Displays all packages that have been already attempted or installed though a policy using the portal.
- **Optional columns:** The columns that appear in the **Application** and **History** tabs on the LANDesk Desktop Manager Software Deployment Portal window on the managed device.
    - **Size:** Displays the physical size of the package to inform the user before proceeding the download of a large application.
    - **Group:** Allows the LANDesk administrators to specify a group in each individual distribution package task to applications which will enable the end user to sort the application list by, for example, type of application, vendor, or category. Groups are assigned in each individual software distribution scheduled task.
    - **Description:** Displays the description from the properties of the distribution package.
    - **Status:** Indicates whether the installation was successful or failed.
    - **Last Run:** Indicates the date and time of the last attempt to install the package.
    - **Type:** Indicates whether the package is required, recommended, or optional.
- **Display columns and order for Application/History:** Displays the default columns in the Application and History tabs on the LANDesk Desktop Manager Software Deployment Portal window on the managed device. The default list contains the following:
    - **Name (required):** Displays the name of the distribution package.
    - **Description** (optional)
    - **Status** (optional)
    - **Last Run** (optional)
    - **Type** (optional)
    - Use the **Up** and **Down** buttons to rearrange the order in which the columns appear.

Deploying remote control

When deploying remote control, you need to consider which security model you want to use. You have these choices:

- **Local template:** This is the most basic security that uses whatever remote control settings are specified on the device. This model doesn't require any other authentication or group membership.
- **Windows NT security/local template:** This security model uses a Windows NT Remote Control Operators group. Members of this group are allowed to remote control devices. Permitted users still use the device's remote control settings, such as permission required.
- **Integrated security:** This is the most secure option and is the default. Integrated security is described in the next section.

About Integrated security

Integrated security is the new default security model. Here's an outline of the integrated security remote control communication flow:

1. The remote control viewer connects to the managed device's remote control agent, but the agent replies that integrated security authentication is required.
2. The viewer requests remote control rights from the core server.
3. The core server calculates remote control rights based on the viewer's scope, role-based administration rights, and Active Directory rights. The core server then creates a secure signed document and passes it back to the viewer.
4. The viewer sends this document to the remote control agent on the managed device, which verifies the signed document. If everything is correct, the agent allows remote control to begin.

Warning: Integrated security requires the core server
With integrated security remote control, if the core server isn't available, consoles won't be able to remote control devices. Integrated security remote control requires the core server to work.

Using Windows NT security/local template with Windows XP devices

For Windows NT security/local template authentication to work with Windows XP devices, you must configure devices so that the Windows XP sharing and security model for local accounts is classic (local users authenticate as themselves). If you don't do this, the default guest-only authentication won't work with remote control's Windows NT security.

To set the Windows XP security model to classic

1. On the Windows XP device, click **Start > Control Panel**.
2. In the **Administrative Tools, Local Security Policy** applet, click **Security Options > Network access: Sharing and security model for local accounts**, and set it to **Classic - local users authenticate as themselves**.

About the Agent configuration dialog's Remote control page

The **Agent configuration** dialog's **Remote control** page contains the following features:

- **Local template:** Uses only the local device simple permissions set from the remote control **Permissions** page.
- **Windows NT security\local template:** Only allows members of the Remote Control Operators group to initiate remote control connections from the console to remote devices. Permitted users are still required to use the permissions set from the Remote Control Settings page of this wizard.
  Since the Remote Control Operators group is a local group, each device has its own copy of the group. To avoid managing each device's Remote Control Operators group individually, include global (domain level) groups with each local group.
  Permitted users still use the device's remote control settings, such as permission required.
- **Integrated security:** This is the default security model and is described earlier in this chapter. Permitted users are still required to use the permissions set from the **Permissions page**.

Adding users to the Remote control operators group and the View only group

If you select **Windows NT security/local template** as your security model, the **Remote control operators group** and **View only group** boxes list the users for the console or for the selected Windows NT domain. The users you select here will have remote control access to the devices that receive the settings defined in this configuration settings file. **View only group** users can only view remote devices. They can't take over the mouse or keyboard.

When adding users to one of the remote control groups, the console uses the logged-on user's Windows credentials, not the LANDesk console user's credentials, to list the users in a domain. If the **List users from** box isn't showing the domain you want, log in to Windows as a user with rights on that domain.

To choose from an existing server or domain

1. In the **Remote control** page, click **Windows NT security/local template** and click the **Add** button.
2. In the **List names from** box, select either the core server name or a Windows NT domain name containing user accounts.
3. In the user list, select one or more users and click **Insert** to add them to the **Inserted names** list.
4. Click **OK** to add the selected names to the Remote Control Operators group on each device that receives these configuration settings.
5. If you want any of these users to be in the **View only group**, select them and move them over. Users can only be in one group.

To manually enter names

You can enter names manually by clicking in the **Inserted names** list and using any of the following formats to enter names. Use semicolons to separate names.

- **DOMAIN\username** where DOMAIN is the name of any domain accessible to the target device.
- **MACHINE\username** where MACHINE is the name of any device in the same domain as the target device.
- **DOMAIN\groupname** where DOMAIN is the name of any domain accessible to the target device, and groupname is the name of a management group in that domain.
- **MACHINE\groupname** where MACHINE is the name of any device in the same domain as the managed node, and groupname is the name of a management group on that device.

If you don't specify a domain or device name, it is assumed that the user or group specified belongs to the local device.

Click **OK** to add the names to the Remote Control Operators user group on the target device.

About the client setup dialog's Permissions page (under remote control)

The **Remote control** section's **Permissions** page contains the following features:

- **Remote control:** Grants permission to control the device.
- **Chat:** Grants permission to chat with the device.
- **File transfer:** Grants permission to transfer files to and from the device's local drives.
- **Draw:** Grants permission to use the viewer window's drawing tools on the device.
- **Reboot:** Grants permission to reboot the device.
- **View only:** Remote control operators can only view the device, they can't interact with it remotely.
- **Run programs on remote device:** Grants permission to run programs on the device.
- **Specify remote control settings:** Configures and sets up permissions for Remote control users. Customized messages can be created when asking for permissions to perform the difference commands that remote control offers.
  - **Close inactive session after:** Allows the remote session to disconnect automatically due to inactivity. If a value of 0 is entered, the console won't automatically disconnect the remote session due to inactivity.

- **End user must grant permission for remote control session:** Allows a user that is logged onto a remote control managed device to respond affirmatively to the request before control of their managed device is taken.
- **Only when the user is logged on: Prompts the user currently logged on for permission.** If nobody is logged on, remote control doesn't require permission.
- **Ask permissions to use all features at one time:** Allows permissions to be required once per session as opposed to requiring permission for each feature (file transfer, remote execute, etc.) If the **Ask for all Allowed Permissions at Once** checkbox is checked, the user is prompted for permissions only once during the remote control session, regardless of the processes that are performed.
- **Display a custom message:** Prompts the user with a custom message created here for permission to do one of the following (must check **Permission required** to use):
  - Remote control
  - Chat
  - Remote execute
  - File transfer
  - Reboot
  - All permissions
- **Close permission message box after:** Allows the user to accept or deny permission (in seconds) to the managed device. This is a configurable time setting for how long the permission window remains open when asking permission to remotely control a managed device.

About the Indicators page (under remote control)

The **Remote control** section's **Indicators** page contains the following features:

- **Floating desktop icon:** Displays the remote control agent icon on the device screen at all times or only when being remotely controlled. When being controlled by the console, the icon changes to show a magnifying glass and the icon's title bar turns red.
- **System tray icon:** Places the remote control agent icon in the system tray. Again, the icon can be visible all the time or only while being remotely controlled.
- **Use mirror driver:** Checked by default, this option uses the remote control mirror driver on devices for faster remote control performance.
- **Lock the remote control computer when the session ends:** Locks the managed device to secure mode whether the user is logged in or not.

Deploying Security services

The security scanner (i.e., patch and compliance scanner) is installed by default with the standard LANDesk agent. However, you need to use the options on the specific Security and patch scan page when creating device agent configurations in order to configure certain aspects of how and when the security scanner runs on managed devices. You can also enable and configure custom variable override settings, frequent security scans, real-time spyware, and application blocking

The security scanner allows you to scan managed devices for known OS and application vulnerabilities and other security risks, such as: spyware, viruses, unauthorized applications, software and driver updates, system configuration security threats, custom security definitions, and more. The content of your security scan depends on your Security Suite content subscription and which security type definitions you've downloaded. You can also remediate detected problems via autofix, repair tasks, and repair policies. For details on these procedures, see "Patch and Compliance" on page 296.

Information about the following security-related pages can be found below. Click a link to go to that section.

- "About the Patch and Compliance Scan page" on page 627
- "About the Custom Variables page" on page 628
- "About the Frequent Security Scan page" on page 628
- "About the Antivirus page" on page 629
- "About the Spyware page" on page 629
- "About the Application Blocker page" on page 630
- "About the Windows Firewall page" on page 630
- "About the Endpoint Security page" on page 631
- "About the Agent Watcher page" on page 631
- "About the 802.1X Support page" on page 631
- "About the Agent configuration dialog's Extended device discovery page" on page 632

About the Patch and Compliance Scan page

Use this page to configure how the security scanner (i.e., patch and compliance scanner) is launched and how it behaves on managed devices with this agent configuration. (**Note:** You can also run security scans as scheduled tasks and policies from the console, or manually at a managed device.)

This page contains the following options:

- **Event-driven scan:**
    - **When user logs in:** Places the security scanner in the Windows registry's run key which causes the scanner to launch whenever a login occurs on managed devices with this agent configuration.
- **Schedule-driven scan:**
    - **Change settings:** Opens the **Schedule security and patch scan** dialog, where you can configure scheduling settings for security scans that are launched by the local scheduler. The local scheduler automatically launches a security scan on a recurring basis, at the earliest opportunity within the time period and restrictions you specify. You can also configure options for running the security scanner when a device meets certain conditions, such as: only when a user is logged in, only if a specified minimum bandwidth is available, and any time a device's IP address changes. Once you've configured these scheduling settings for the security scanner, simply click **Save** to return to the main page where the scheduling criteria now appears.
- **Global settings:** Applies to all devices with this agent configuration, overriding task-specific settings.
    - **Never reboot:** Ensures devices with this agent configuration won't reboot when the security scanner is running. This is a global setting for all devices with this agent configuration, which means it overrides any end user reboot settings that are applied to either a security scan or repair task. In other words, regardless of the end user reboot settings used by a security task, this global setting will take precedence. Check this option if you know you don't want devices to reboot

during any security scanner operation, and leave it clear if you want to be able to configure the reboot options with the Patch and Compliance tool.

- **Never autofix:** Ensures devices with this agent configuration won't allow a security and patch scan to perform an auto fix when remediating detected vulnerabilities, even if the vulnerability has auto-fix enabled. As a global setting for all devices with this agent configuration, this setting overrides any end user auto-fix setting you've applied to a security scan task. Use this setting if you want to guarantee devices can't have detected vulnerabilities automatically remediated by a security scan.

- **Scan and repair settings:** Determines the information displayed by the security scanner on managed devices, end user interaction, reboot operation, and content settings when the scanner is launched on managed devices with this agent configuration by the method selected above (run key during login, local scheduler, or both). Select a scan and repair setting from the drop-down list to apply it to the configuration you're creating. You can also click **Configure** to create and apply a new scan and repair setting or to edit an existing one.

About the Custom Variables page

Use this page to assign a custom variable override setting to devices with this agent configuration.

The security scanner can utilize custom variables (editable values included in certain security types' definitions) to scan for and modify specific settings, and to implement standard system configuration settings to managed devices. You can change the value of a setting and select whether to override the current value with the new value, and then use this agent configuration to apply the configuration to target devices. In some situations you may want to ignore a custom variable setting, or in other words create an exception to the rule. Custom variable override settings let you decide which custom variables to essentially ignore when scanning devices so that they are not detected as vulnerable and are not remediated even if they meet the actual conditions of a definition's detection rules.

A custom variable override setting is not required with an agent configuration.

You can select an existing setting from the drop-down list, click **Configure** to create a new setting, or leave the field blank.

This page contains the following options:

- **Custom Variable settings:** Specifies custom variable override settings used on target devices when they're scanned for security definitions that include custom variables (such as security threats and viruses). Custom variable override settings let you specify setting values you want to ignore or bypass during a security scan. This is very useful in situations where you don't want a scanned device to be identified as vulnerable according to a definition's default custom variable settings. Select a setting from the drop-down list. From the drop-down list, you can also select to remove the custom variable override settings from target devices. The **Remove custom variable settings** option lets you clear a device so that custom variable settings are in full affect. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Custom variable override settings dialog" on page 677.

About the Frequent Security Scan page

Use this page to enable and configure a recurring security scan for a specific collection of high-risk vulnerabilities or other security definitions on devices with this agent configuration. A frequent security scan is useful if you need to regularly scan devices for particularly aggressive and harmful security attacks.

Group scans only
Frequent security scans are based on the security definitions contained in a group you've selected from predefined security content groups.

This page contains the following options:

- **Use the frequent security scanner:** Enables a frequent security scan on devices with this agent configuration.
- **Scan only when a user is logged in:** Restricts the frequent security scan so that it runs only if a user is logged into the target device.
- **Every:** Specifies the time interval for a the frequent security scan.
- **Scan and repair settings (that scans for a group):** Specifies the scan and repair settings that control the security scanner for frequent security scans. Scan and repair settings determine whether the security scanner displays on devices while running, reboot options, and user interaction. The setting you select must be configured to scan a group, not a type. You can also click **Configure** to create a new scan and repair setting that is associated with a group.

About the LANDesk Antivirus page

Use this page to select an antivirus setting that applies to devices with this agent configuration, and to select whether to remove any existing antivirus products from those devices when they are configured.

In order to select an antivirus setting, you must first check the **LANDesk Antivirus** agent's checkbox on the **Start** page.

Antivirus settings let you control how the antivirus scanner operates on target devices. You can define antivirus scan parameters such as: files and folders to be scanned or excluded, manual scans, real-time scans, scheduled scans, quarantine and backup options, virus pattern file update options, and the information and interactive options that display on end user devices during the antivirus scan.

Deploying LANDesk Antivirus to devices that already have an antivirus product installed
If another antivirus product is installed on target devices, you can select to have it removed automatically during agent configuration by selecting the **Remove existing antivirus product** option. If you choose not to remove the other antivirus product during agent configuration, LANDesk Antivirus is disabled until you manually remove the other product. However, you can still deploy the service to target devices.

For a current list of antivirus products that can be removed from devices, see "List of third-party antivirus products that can be automatically removed" on page 371.

This page contains the following options:

- **Remove existing antivirus product:** Automatically removes other antivirus software that might already be installed on devices before installing LANDesk Antivirus. (**Note:** You can also select to remove existing antivirus software from managed devices when creating an **Install or update Antivirus** task.)
- **Antivirus settings:** Antivirus settings determine whether the Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates. Select a setting from the drop-down list. Click **Configure** to create a new setting.

About the Spyware page

Use this page to enable real-time spyware detection and notification on devices with this agent configuration.

Real-time spyware detection checks only for spyware definitions that reside in the **Scan** group, and that have autofix turned on. You can either manually enable the autofix option for downloaded spyware definitions, or configure spyware definition updates so that the autofix option is automatically enabled when they are downloaded.

Real-time spyware detection monitors devices for new launched processes that attempt to modify the local registry. If spyware is detected, the security scanner on the device prompts the end user to remove the spyware.

This page contains the following options:

- **Enable real-time spyware blocking:** Turns on real-time spyware monitoring and blocking on devices with this agent configuration.

  Note: In order for real-time spyware scanning and detection to work, you must manually enable the autofix feature for any downloaded spyware definitions you want included in a security scan. Downloaded spyware definitions don't have autofix turned on by default.

- **Notify user when spyware has been blocked:** Displays a message that informs the end user a spyware program has been detected and remediated.
- **If an application is not recognized as spyware, require user's approval before it can be installed:** Even if the detected process is not recognized as spyware according to the device's current list of spyware definitions, the end user will be prompted before the software is installed on their machine.

About the Application Blocker page

Use this page to enable real-time unauthorized application blocking and notification. Real-time application blocker checks only for applications that reside in the **Scan** group.

With real-time application blocking, remediation is NOT a separate task. Application blocking takes place as part of the security scan itself, by editing the registry on the local hard drive to disable user access to those unauthorized applications. Security services uses the Software license monitoring tool's softmon.exe feature to deny access to specified application executables even if the executable file name has been modified because softmon.exe reads the file header information.

This page contains the following options:

- **Enable blocking of unauthorized applications:** Turns on real-time application blocking on devices with this agent configuration.
- **Notify user when an application has been blocked:** Displays a message that informs the end user they have attempted to launch an unauthorized application and access has been denied.

About the Windows Firewall page

Use this page to enable and configure the Windows firewall on managed devices with this agent configuration. You can enable/disable the firewall, as well as configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, and programs).

You can use this feature to deploy a configuration for the Windows firewall on the following Windows versions:

- Windows 2003
- Windows XP (SP2 or later)
- Windows Vista

This page contains the following options:

- **Configure Windows Firewall:** Enables automatic Windows firewall configuration on devices with this agent configuration.
- **Windows Firewall settings:** Specifies the Windows firewall settings deployed on target devices with this agent configuration. Select a setting from the drop-down list to apply it to the configuration you're creating. You can also click **Configure** to create and apply a new scan and repair setting or to edit an existing one.

About the Endpoint Security page

Use this page to select an Endpoint Security setting for managed devices with this agent configuration. Endpoint Security includes these components: HIPS, Firewall, and Device Control.

In order to select an Endpoint Security setting, you must first check the Endpoint Security agent checkbox on the **Start** page.

This page contains the following options:

- **Endpoint Security settings:** Specifies the Endpoint Security settings for managed devices with this agent configuration. Endpoint Security settings determines general Endpoint Security operation (such as location awareness, administrator password, end user stop option, and pop-up messages), as well as which security policies are deployed for HIPS, LANDesk Firewall, and Device Control. You can also click **Configure** to create a new settings.
- **Update configuration from core:** Lets you update Endpoint Security settings on target devices configured with this agent configuration.

About the Agent Watcher page

Use this page to enable and configure the LANDesk Agent Watcher utility on devices with this agent configuration.

Agent Watcher allows you to actively monitor devices for selected LANDesk agent services and files. Agent watcher restarts agent services that have been stopped and resets the startup types for services that have been set to automatic. The utility also removes monitored agent files from lists of files to be deleted on reboot, in order to prevent deletion. Additionally, Agent Watcher alerts you when agent services cannot be restarted, when agent files have been deleted, and when agent files are scheduled to be deleted on reboot.

This page contains the following options:

- **Use the Agent Watcher:** Enables the Agent Watcher utility on devices with this agent configuration.
- **Agent Watcher settings:** Specifies Agent Watcher settings deployed on target devices with this agent configuration. Agent Watcher settings determine which services and files are monitored and how often, as well as whether the utility remains resident on the device. Select a setting from the drop-down list. Click **Configure** to create a new setting. For more information about an option, click **Help**.

About the LANDesk 802.1X Support page

Use this page to enable the LANDesk 802.1X NAC solution. You can use 802.1X to enforce your compliance security policy on managed devices that support 802.1X, by running compliance security scans, granting or blocking access depending on device health status (compliance), putting unhealthy (non-compliant) devices in quarantine, and performing remediation.

Enabling and configuring 802.1X NAC with an agent configuration
In order to enable 802.1X NAC and configure the options on this page, you must first check the **802.1X Radius Server** option on the 802.1X Configuration dialog in the Network Access Control tool (**Tools > Security > Network Access Control > Configure 802.1X > Radius Server**). After you check that option, you can use this page to configure 802.1X with an agent configuration.

This page contains the following options:

- **Enable 802.1X support:** Turns on 802.1X NAC on devices with this agent configuration. 802.1X NAC uses the EAP type specified in the NAC tool. The EAP type setting is core-wide. In other words, all devices configured with this agent configuration will be configured with the EAP type specified in the console.
- **Configure PEAP settings:** Opens a dialog where you can specify server and trusted certification authority settings.
- **Quarantine network address:**
    - **Use IP in self-assigned range:** Specifies that devices determined to be unhealthy (non-compliant), based on the compliance security policy, will be sent to a quarantine network area using the TCP/IP protocol's built-in self-assigned IP address range functionality.
    - **Use DHCP in quarantine network:** Specifies that devices determined to be unhealthy (non-compliant), based on the compliance security policy, will be sent to a quarantine network area using a DHCP server and remediation server you've configured.
        - **Select primary remediation server:** Specifies the remediation server you want to use for repairing unhealthy devices so that they can be scanned again and allowed access to the corporate network.
        - **Remediation backup server:** Lets you configure a backup server for remediation, in case the primary remediation can't be accessed. Click **Configure** to add a remediation server.
- **Quarantine client if no health scan has been performed within:** Use this option to automate device quarantine by specifying a maximum period of time a device can be considered healthy without having a compliance security scan run on it. If this time expires without a scan, the device is automatically placed in the quarantine network area.

Deploying Extended device discovery

About the Agent configuration dialog's Extended device discovery page

Use this page to enable and configure extended device discovery on managed devices with this agent configuration.

Extended device discovery is an extension of Unmanaged device discovery tool, and finds devices on your network that haven't submitted an inventory scan to the core database. With extended device discovery, you can use one or both of the following discovery methods: ARP (address resolution protocol) discovery, and WAP (wireless access point) discovery.

With ARP discovery, the extended device discovery agent listens for network ARP broadcasts. The agent then checks any ARP-discovered devices to see whether they have the standard LANDesk agent installed. If the LANDesk agent doesn't respond, the ARP-discovered device displays in the Computers list. Extended device discovery is ideal in situations involving firewalls that prevent devices from responding to the normal ping-based UDD discovery methods.

Keep in mind that you don't have to deploy the extended device discovery agent to every managed device on your network, though you can if you want to. Deploying this agent to several devices one each subnet should give enough coverage.

This page contains the following options:

- **Use Address Resolution Protocol (ARP):** Enables extended device discovery using the address resolution protocol (ARP) discovery method on devices with this agent configuration.
- **Choose an ARP discovery setting:** Specifies the ARP setting that controls the extended device discovery agent when performing ARP discovery on your network. ARP settings determine the discovery scan frequency and logging level. Select a setting from the drop-down list to apply it to the configuration you're creating. You can also click Configure to create and apply a new setting or to edit an existing one
- **Use Wireless Access Point discovery (WAP):** Enables extended device discovery using the wireless application protocol (WAP) discovery method on devices with this agent configuration.
- **Choose a WAP discovery setting:** Specifies the WAP setting that controls the extended device discovery agent when performing WAP discovery on your network. WAP settings determine the discovery scan frequency and logging level. Select a setting from the drop-down list to apply it to the configuration you're creating. You can also click Configure to create and apply a new setting or to edit an existing one.
- **Configuration download frequency (in minutes):** Specifies how often managed devices with the extended device discovery agent installed check with the core server for an updated extended device discovery configuration. The agent always updates its configuration from the core when it first loads. The default value is 720 minutes (12 hours). If you set this value too high, it will take a long time for configuration changes to propagate to devices. If you set this value too low, there will be more load on the core server and the network.

Deploying power management

About the Agent configuration dialog's Power Management page

Use the **Power Management** page to select the power policy to be distributed out to the client machine. LANDesk Power Management (Power Management) functionality allows administrators to centrally control end-node power consumption by facilitating the creation, financial evaluation, and deployment of power management policies. While administrators centrally control the conditions under which computers and monitors stand by, hibernate, or power down, users can forestall specific Power Management actions on the client-side if needed. In addition, a “soft” shutdown option protects unsaved user data. A pre-populated database of OEM wattage consumption values is matched to actual hardware inventory data, and available custom wattage settings allow high levels of precision in the estimation of financial and power savings.

The Power Management window contains the following features:

- **Power policy settings:** Selects a power policy that has been created and configured to be used on managed devices.
- **Choose a power policy:** Specifies the power policy that will be sent out with the agent configuration. By default one power policy is available or none.
- **Collect the client usage info:** Collects power usage from the individual client usage. This information is used to create more accurate reports of power usage and to know the exact power demands of the managed devices and the monitors that are connected to them.

Deploying Desktop Manager

About the Agent configuration dialog's Desktop Manager page

Desktop Manager enhances the end-user experience by providing a consolidated desktop client UI that includes access to both the Software Deployment Portal and the LaunchPad console from a single shortcut off the Start menu.

Use the **Desktop manager** pages to configure how Desktop Manager looks.

The **Desktop manager** page contains the following features:

- **Available applications:** Lists the applications that can be configured for access through Desktop Manager. Available applications include:
  - **LaunchPad:** A console that provides access to packages, executables, URLs and process manager links that have been individually configured for a managed device. LaunchPad provides one-click access to local, hosted, or just-in-time applications- which are not installed until the icon is clicked by an end-user.
  - **Software Deployment Portal:** Displays all software distribution packages that have been deployed using an optional or recommended policy based delivery method.
- **Show in Desktop Manager:** Displays the applications that will be displayed and accessed through Desktop Manager. Use the >> and << to select or deselect desired applications. By default both LaunchPad and Software Deployment Portal are included.

About the Agent configuration dialog's Customization page (under Desktop Manager)

Use the **Customization** page to configure shortcut location selections for Desktop Manager and start up and shut down preferences.

The **Customization** page contains the following features:

- **LANDesk program group:** Creates a Start menu entry to the LANDesk program group.
- **Windows desktop:** Creates a shortcut on the desktop.
- **Windows Start menu:** Creates a Start menu entry.
- **Run Desktop Manager when the user logs on:** Runs the Desktop Manager when a user logs on to the managed device.
- **Do not allow Desktop Manager to be closed:** Prevents end users from closing the Desktop Manager window.

About the Agent configuration dialog's Branding page (under Desktop Manager)

Use the **Branding** page to customize the look and feel of Desktop Manager.

The **Branding** page contains the following features:

- **Application title:** Allows for customization of the application window's title. The default is LANDesk Desktop Manager.
- **Your message:** Allows an Administrator to enter a custom message to be displayed in the bottom-center of the Desktop Manager window. By default no message displays.
- **Your corporate icon:** Add a company icon file to replace the default icon on Desktop Manager. The selected icon appears in the upper left hand corner next to “Software Deployment Portal”.
- **Your corporate logo:** Adds a company logo to display at the bottom left corner of the window. The Avocent|LANDesk logo always displays in the bottom right corner.

Using the Client Setup Utility

About the Client Setup Utility dialog

The **Agent configuration utility** dialog displays the status of a scheduled device configuration task as the task is processed. This dialog is for information only; the devices to be configured were selected when the task was scheduled.

The **Agent configuration utility** dialog contains the following features:

- **Clients to configure:** Lists the devices scheduled to receive these configuration settings.
- **Clients being configured:** Lists the devices that have been contacted by the console and are in the process of being configured with this settings file.
- **Clients completed:** Lists the devices that the console has configured during this scheduled session. If the configuration attempt was successful, the status is Complete. If the configuration attempt failed for any reason, the status is Failed. These statuses are mirrored in the Scheduled Tasks window when this task is selected.
- **Creating configuration files:** Displays a status bar indicating the completion status of the entire configuration task.

Deploying to NetWare servers

You can install the inventory scanner to NetWare servers. The NetWare agent configuration utility will modify the AUTOEXEC.NCF to load the scanner on startup. You must have the NetWare client loaded on the console you're installing the agent from and you must have write access to the NetWare server you want to install the agents on.

To install remote control and inventory on a NetWare server

1. In the Management Suite console, click **Configure > Deploy LDMS client to NetWare server**.
2. Enter the NetWare server name. Click **Install**, and then click **OK**. This installs the agents to the NetWare server.

About the Add a bare metal server dialog

Use the **Add a bare metal server** dialog to add devices to the queue so they can have provisioning tasks run on them. This is particularly helpful for the initial provisioning of new devices. Devices are added to the holding queue by using an identifier. A server identifier is a piece of information that can be used to uniquely identify a server. A server identifier may be a MAC address (most common), a vendor serial number, an IPMI GUID, or an Intel AMT GUID. In all cases, the identifier must be able to be queried by an agent running in the preboot environment on the target server. You can add devices one at a time or many at a time.

To add a single device

1. In the **Network view**, expand the **Configuration** group. From the **Bare metal server** item's shortcut menu, click **Add devices**.
2. Click **Add**. Type a descriptive name in the **Name** text box. While the display name is optional, it is highly recommended. On a bare-metal device, the display name is the only differentiator in the Provisioning view.
3. Select an identifier type from the **Identifier type** list (Mac address, serial number, IPMI GUID, or Intel AMT GUID), and enter the value in the **Identifier** text box. Click **Add**.
4. Repeat steps 2-3 to add other devices. You can also add other identifiers for the device; just add another identifier with the same display name.

5. Click **OK**.

To add multiple devices

1. In the **Network view**, expand the **Configuration** group. From the **Bare metal server** item's shortcut menu, click **Add devices**.
2. In the **Identifier type** list, select an identifier type that matches the data you will import.
3. Type the location of a text file (CSV) which contains the identifier information in the text box (or click **Browse** to find the file), and click **Import**.

Each identifier should be separated by a comma in the CSV file. The import file format is identifier; display name.

Deploying to Linux and UNIX servers

You can use the console's agent configuration tool to deploy agents to supported Linux and UNIX operating systems. For more information on Linux agent deployment, see "Configuring Linux and UNIX device agents" on page 83.

About the Start page (under Linux Agent configuration)

The Linux **Agent configuration's Start** page has these options:

- **Configuration name:** Enter a name that describes the configuration you're working on. This can be an existing configuration name or a new one. This name appears in the **Agent configuration** window.
- **Standard LANDesk agent**, **Remote control**, and **Software distribution**: These options install by default and you can't disable them.
- **LANDesk vulnerability scanner:** Installs the Linux version of the vulnerability scanner. The scanner only reports on problems, it doesn't remediate them.
- **Real-time inventory and monitoring:** Installs an agent which supports real-time inventory and monitoring from the LANDesk Management console.
- **Defaults:** Resets the options to default (disables the **LANDesk vulnerability scanner** option).

About the Standard LANDesk agent page (Under Linux Agent configuration)

The Linux **Agent configuration**'s **Standard LANDesk agent** page has these options:

- **Trusted certificates for agent authentication:** certificates control which core servers can manage devices. Check the core server certificates that you want installed with this configuration. For more information, see "Agent security and trusted certificates" on page 81.
- The other options on this page are dimmed and don't apply to Linux agent configurations.

About the Inventory scanner page (Under Linux Agent configuration)

The **Linux Agent configuration**'s **Inventory scanner** page has these options:

- **Start inventory scan:** You can select **Daily, Weekly, or Monthly**. The option you select adds a command to the server's cron.daily, cron.weekly, or cron.monthly file that runs the inventory scanner.

About the System Manager page (Under Default windows configuration)

The System Manager page is available if you have installed System Manager on your core server. It has these options:

- **Install monitoring:** Installs the System Manager monitoring agent on devices. This agent reports device health to the core server. You can configure alerts in the System Manager console based on the monitoring agent data.
- **Monitoring** and **Alerting:** Select any monitoring and/or alerting rulesets you want included with the configuration. These rulesets are stored in the ldlogon/alertrules folder. New rulesets can be created in the System Manager **Monitoring** or **Alerting** tools. In order for newly-created rulesets to display in the drop-down lists, you must generate the XML for the custom ruleset in the System Manager console.

Configuring the LANDesk Management Gateway

The LANDesk Management Gateway is an Internet appliance that provides secure communication and functionality over the Internet. It acts as a meeting place where console and managed devices are connected through their Internet connections—even if they are behind firewalls or use a proxy to access the Internet.

Read this topic to learn about:

- "Setting up the Management Gateway connection" on page 637
- "Posting the core certificate to the Management Gateway" on page 637
- "Managing client certificates" on page 637
- "Creating an on-demand remote control agent package" on page 638

Setting up the Management Gateway connection

The **Gateway information** tab lets you specify and test the connection and proxy settings used by the core to connect to the Management Gateway.

To specify the connection information

1. On the **Gateway information** tab, specify the Management Gateway information.
2. If the Management Gateway uses an internal address that is different from its public address (for example, if it's located in a DMZ-type environment, check **Use separate internal address** and specify the internal name and address).
3. If the core will connect to the Management Gateway through a proxy, check **Use proxy** and specify the proxy settings.
4. Click **Test settings** to test the core server connection to the Management Gateway.
5. If the test fails, check the information you entered and correct any mistakes, then click **Test settings** to make sure the connection works.

Posting the core certificate to the Management Gateway

Before the core can connect through the Management Gateway, you must post the core certificate to it.

To post the core certificate

1. On the **Certificates** tab, click **Post to Management Gateway**.
2. Click **OK** to post the certificate.

Managing client certificates

Each managed device is required to have a valid digital certificate in order to connect through the Management Gateway. You can manage the list of devices that have been granted certificates by blocking or deleting the ability of any formerly trusted device to connect through the Management Gateway.

To block or delete connection ability

1. Select the device(s) you want to block or delete. You can use **Shift-click** or **Ctrl-click** to select multiple devices.
2. Click **Block selection** or **Delete selection**.
3. When finished, click **OK**.

To unblock connection ability

1. Uncheck the **Block** checkbox for each device you want to unblock.
2. When finished, click **OK**.

Creating an on-demand remote control agent package

You can create an on-demand remote control agent package that can be downloaded by devices that have not been configured to connect through the Management Gateway. This allows them to be remote controlled through the Management Gateway.

To create an on-demand remote control agent

1. Click the **Certificates** tab.
2. Click **Create**.
3. Specify the organization name. The device will only be viewable to administrators that belong to the same organization.
4. Click **Save**.
5. Specify the location to which you want the remote control agent to be saved.
6. Click **Save**.

After creating the remote control agent, you can distribute it on CD or post it to an accessible location for download by managed devices.

OS deployment and Profile migration wizard help

This chapter contains the following context-sensitive help topics for the OS deployment/Profile migration tasks wizard.

Help for the OS deployment/Profile migration tasks wizard

This chapter provides descriptions of the options and settings found on each page (and dialog) of the OS deployment/Profile migration tasks wizard. This wizard is used to create scripts that capture or deploy OS images, and capture or restore user profiles. Scripts can then be scheduled as tasks on target devices on your network. The wizard is accessed from either the toolbar button or shortcut menus in the Manage Scripts window (**Tools > Distribution > Manage Scripts**).

You can also access this information by clicking the Help button on the corresponding wizard page itself.

For detailed step-by-step instructions on how to use the OS deployment/Profile migration tasks wizard, and what you need to know in order to plan and implement image deployment and migration jobs, see "OS deployment" on page 201 and "Profile migration" on page 257.

All pages of the OS deployment/Migration tasks wizard are described here. However, the pages you actually see when running the wizard depends on the type of imaging or migration task you selected on the first page of the wizard.

About the OS deployment/Migration tasks wizard: Choose a task page

Use this page to specify which type of OSD/profile migration script you want to create, based on the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device. Images can be captured using the built-in LANDesk imaging tool, or a third-party tool such as Ghost, PowerQuest, or another tool of your choice.
- **Capture profile:** Creates a script that captures and stores a device's unique user settings, application and desktop settings, and files. You can also use this option to access the Collection Manager dialog to create a User-initiated profile migration package that can be run locally at individual devices.
    - **Continue with file capture errors:** Allows the profile capture process to continue even if files designated to be captured report file errors (such as invalid file names, locked files, or files that change size during the capture). The profile capture completes, and file errors are recorded in the log file.
- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.
- **Deploy image (with profile capture and restore):** Creates a script that performs a comprehensive deployment and migration job (capturing profile data, deploying an OS image, and then restoring the profile).
- **Restore profile:** Creates a script that restores previously captured profile data (user settings, application and desktop settings, and files to target devices).
- **Generic DOS tasks:** Creates a script that runs DOS commands (including application launches on devices).

About the General page

Use this page to configure the following characteristics of an OS imaging task:

Note: Some of the options listed below may be disabled, depending on what type of task (capture or deploy) you selected.

- **Name:** Identifies the script with a unique name. If the name you enter is already being used, you'll be prompted to replace the existing script. You should enter a name that helps you quickly and easily identify the script by its function or by the intended target devices on your network.
- **Description:** Additional text you can add to describe the script.
- **Choose network adapter to use if the driver autodetection fails:** (capture image only) Ensures that the image deployment job is successful to all target devices.

  We recommend that you enable this option, and then select a network adapter that is common to your systems. This is especially important if you're deploying to laptops. You should carefully choose a listed network adapter to ensure your job succeeds.

OS deployment uses a phased approach to network adapter detection:

- OS deployment first tries to detect the network adapter from the target device's operating system prior to imaging over it.
- If that fails, OSD will reboot the target device and try to detect the network adapter from DOS.
- If that fails, OSD uses the network adapter you specified in the Undetectable network adapters option on this page of the wizard.
- If the adapter you specify fails, you must go to the target device and manually reboot it. The device will reboot normally into its original OS.

About the Capture profile dialog: General page

Use this page to identify the OS deployment or profile migration script. The text you enter here is used when the script displays in the Manage Scripts and Scheduled Tasks windows:

- **Name:** Identifies the script with a unique name. If the name you enter is already being used, you'll be prompted to replace the existing script. You should enter a name that helps you quickly and easily identify the script by its function or by the intended target devices on your network.
- **Description:** (Optional) Helps you remember the script with the text you type in here.
- **Continue with File capture errors:** Allows capture to continue, even if there are errors during the capture.

If you add this script to the LANDesk PXE DOS Menu, the description you enter here will appear in the menu.

About the capture image dialog: Credentials page

Use this page to provide authentication credentials for the network share, or shares, where the OS image and the imaging tool used to create the image are stored:

You can enter only one set of credentials that will be used to access both shares, so the shares must have matching credentials. The credentials must belong to a local user account on the device hosting the share.

- **Domain and user name:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password/Confirm password:** Enter and confirm the user's password.

About the capture image dialog: Image type and path page

Use this page to specify the image type you want to capture with this script, where the image will be stored, and where the imaging tool is located:

- **Image type:** Identifies the file type (format) of the image file captured by this script, selected from the list of imaging tools.
- **Enter the UNC path to the desired image, including the name of the image:** Locates the server and share where the image file will be stored. The image must be stored on a share accessible by devices. Note that the share name cannot include any spaces. You can enter just the device name in UNC format, then browse for the remainder of the path by clicking the browse button. In some cases, browsing for a path will insert a local path. You must convert this to UNC format.

During the imaging process, devices will map this UNC path to drive I:.

- **Enter the UNC path to the imaging application, including the name of the application:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename. Note that the share name cannot include any spaces. In some cases, browsing for a path will insert a local path. You must convert this to UNC format.

During the imaging process, devices will map this UNC path to drive H:.

About the capture image dialog: Additional commands page

Use this page to customize the script by adding custom commands.

- **Enter additional commands to run before the end user device is rebooted and imaged:** You can add commands in this text box, one per line, as if you were typing at a command prompt. Commands are sent to devices one at a time. These commands are run after the device is rebooted and imaged.

About the deploy image dialog: Methods and credentials page

Use this page to provide authentication credentials for the network share, or shares, where the OS image and the imaging tool used to create the image are stored:

- **Use Multicast:** Uses existing multicast domain representatives on subnets of your network to deploy the OS image via the LANDesk Targeted Multicast technology. Multicasting enables you to transmit software packages to multiple devices at once, significantly reducing time and bandwidth requirements. Instead of sending a package across the wire for each device, only one transfer is made for each subnet.

  Before using multicasting, make sure the multicasting components are in place on the subnet you're distributing to. Multicasting requires LANDesk Management Suite 6.62 or later agents and a LANDesk Management Suite 6.62 or later multicast domain representative.
- **Image uses SysPrep:** Indicates that you used Microsoft Sysprep to configure the OS image to be deployed. Selecting this option allows you to specify Sysprep file information and deployment options later in the wizard.
- **Use hardware-independent imaging:** Select this option to include the hardware-independent imaging tool in the imaging process. This tool lets you define a basic image that can be applied to multiple device models, and then injects drivers onto each device based on the device manufacturer and model. If you select this option, you also need to specify hardware-independent imaging options under the **Sysprep options** section.
- **Include profile migration:** Integrates both profile capture and restore processes as part of the image deployment job. Selecting this option allows you to specify profile migration options later in the wizard.
- **Continue with file capture errors:** Allows capture to continue, even if there are errors during the capture.

You can enter only one set of credentials that will be used to access both shares, so the shares must have matching credentials. The credentials must belong to a local user account on the device hosting the share.

- **Domain and user name:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password/Confirm password:** Enter and confirm the user's password.

About the deploy image dialog: Multicast discovery page

Use this page to configure the following basic targeted multicast options for an image deployment script:

- **Use Multicast domain discovery:** Searches for multicast domain representatives on subnets of your network prior to using Targeted Multicasting to deploy the image to devices across the network.
- **Use Multicast domain discovery and save results:** Searches for multicast domain representatives on subnets of your network prior to deploying the image, and saves the resulting data to help facilitate future Targeted Multicasting deployments.

  Only one discovery's results are saved at a time, so selecting this option for an image deployment script will replace the results of the previous discovery.
- **Use results of last Multicast domain discovery:** Uses the most recent list of discovered multicast domain representatives when deploying the image to devices.

  Select this option *only* if you've already saved the resulting data of a multicast domain representative discovery at least once.

- **Configure advanced Multicast options:** Allows you to further customize Targeted Multicasting behavior for a deployment script by configuring advanced Multicast options on the next page of the wizard.
- **Domain representatives can wake up managed devices:** Use this option if you want computers that support Wake On LAN technology to turn on so they can receive the multicast. You can use the Multicast Options dialog to configure how long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds.
- **Number of seconds to wait for Wake on LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

About the deploy image dialog: Advanced options page

Use this page to configure the following advanced targeted multicast options for an image deployment script:

- **Maximum number of Multicast Domain Representatives working simultaneously:** Controls the maximum number of multicast domain representatives that can actively deploy an image via Targeted Multicasting at the same time.
- **Number of days files stay in the managed device cache:** Controls the amount of time the image file being multicast can reside in the local cache on each target device. After this period of time, the file will be automatically purged.
- **Number of days files stay in the multicast domain representative cache:** Controls the amount of time the image file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions:** Controls the minimum amount of time to wait between sending out multicast packets. This value is only used when the multicast domain representative is not multicasting a file from its own cache. You can use this parameter to limit bandwidth usage across the WAN.

If this parameter is not specified, then the default minimum sleep time stored on the subnet's multicast domain representative will be used.

- **Maximum number of milliseconds between packet transmissions:** Controls the maximum amount of time to wait between sending out multicast packets.

About the deploy image dialog: Image type and path page

This page also appears in the capture image dialog. Use this page to specify the type of image you want to restore with this script, where the image is stored, and where the imaging tool is located:

- **Select the image type:** Identifies the file type (format) of the existing image file you want to deploy with this script, selected from the list of imaging tools.
- **Enter the UNC path to the desired image...:** Locates the server and share where the image file is stored, including the image filename. The image must be stored on a share accessible to devices.
- **Enter the UNC path to the imaging application...:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename.

- **Deploy image to this partition:** (Windows PE images only.) Lets you choose the partition on the managed device that you want the image deployed to. The partition you select becomes the C: drive.

Related topics

- Creating imaging scripts
- OS deployment overview
- Profile migration overview

About the deploy image dialog: Tool additional commands page

If you're using Powerquest as your imaging tool, you can add additional Powerquest commands on this page. The page is dimmed if you didn't select Powerquest as your imaging tool.

About the deploy image dialog: Pre-boot commands page

Use this page to customize the script by adding custom commands.

- **Enter commands to run before the device is rebooted and imaged:** You can add commands in this text box, one per line, as if you were typing at a command prompt. Commands are sent to devices one at a time. These commands are run before the device is rebooted and imaged.

About the deploy image dialog: Sysprep options page

Use this page to provide the following information about the Sysprep file (SYSPREP.INF) used by this script to modify the image being deployed:

- **Use existing SYSPREP.INF file as a template:** Uses an existing SYSPREP.INF file as a template for a new file and indicates where the existing file is stored. The new SYSPREP.INF file, containing the settings you specify in this wizard, overwrites the existing default Sysprep file. If you want OSD to base its SYSPREP.INF file on one you've already created, you can browse for that file. If you don't select an existing SYSPREP.INF, OSD creates a new one.

After you finish the wizard, you can edit the SYSPREP.INF associated with a script by right-clicking that script and clicking **Advanced Edit**.

- **Location of SYSPREP.INF in the image being deployed:** Locates where the SYSPREP.INF file was stored on the hard drive of the device where Sysprep was originally run. In other words, the device whose image is being deployed by this script.
- **SYSPREP.INF multiprocessor image support - Configure advanced multiprocessor options:** Allows you to configure an image to support multiprocessors (on Windows 2000 or Windows XP devices).

Only select this option if the processor count within your image is different than the processor count on any of your target devices.

About the deploy image dialog: Multiprocessors page

Use this page to configure the following multiprocessor settings for the image being deployed by this script:

- **Choose the operating system type for the image being deployed:** Specifies the OS that is part of the image being deployed, either Windows 2000 or Windows XP.

- **Specify the device type the image was created on:** Indicates whether the image being deployed was created on a uniprocessor or multiprocessor device, with either the APIC or MPS architecture.
- **Enter the location of the HAL-related .INF files inside your image:** Specifies the path to the HAL-related .INF file for the image being deployed by this script. By default, the wizard uses Microsoft's default .INF file paths for each OS. If you used the default paths when setting up your device for imaging, leave the information in this text box as is. Otherwise, type in the different path you used to the HAL-related .INF file.

Additional multiprocessor information

Uniprocessor and multiprocessor devices require different Windows 2000 and Windows XP kernels. Depending on your hardware configuration, you may be able to use your uniprocessor image on a multiprocessor device, or vice versa.

Devices that support advanced processor features typically have an Advanced Programmable Interrupt Controller (APIC). Devices that support advanced processor features can also have an Advanced Configuration and Power Interface (ACPI).

The support matrix for sharing an image between uniprocessor and multiprocessor devices is complex. You should refer to Microsoft's Sysprep documentation for more details.

As a general rule when considering sharing uniprocessor and multiprocessor images, remember that both the source and target devices must have either an ACPI APIC HAL or a non-ACPI APIC HAL. You can't use an ACPI APIC image on a non-ACPI APIC device, or vice versa.

Related topics

- OS image guidelines
- OS deployment overview

About the deploy image dialog: Image settings page

Use this page to specify the following generic settings for the SYSPREP.INF file used by this script to modify the image being deployed:

- **Time zone:** Indicates the time zone where the target devices are located.
- **Volume license key:** Specifies the license number for the OS that is being deployed.
- **Local administrator password for this image:** Provides the administrator's password for the device that was imaged.
- **Name:** Identifies the target devices with a name, such as a department name or geographic location.
- **Organization:** Identifies your organization with a name, such as a division or company name.

About the deploy image dialog: Network credentials page

Use this page to specify the following network settings you want to include in the SYSPREP.INF file for this image:

- **Workgroup:** Indicates that your target devices reside in a workgroup. If you select this option, enter the name of the workgroup in the text box.
- **Domain:** Indicates that your target devices reside in a domain. If you select this option, enter the name of the domain in the text box and provide the following domain account information:

- **Domain username:** Identifies the name of a user in the domain that has privileges to add a machine account to the domain.
- **Domain password:** Provides the user's password.
- **Add device to an Active Directory OU:** Allows you to specify the path (using LDAP path syntax) to a specific Microsoft Active Directory OU where you want to add the target devices being imaged.

About the deploy image dialog: Naming convention page

Use this page to assign the naming convention for target devices that will be imaged by the image deployment script:

- **First attempt to get and use existing computer names from the Inventory database:** Preserves existing Windows computer names if the targeted devices have already had the inventory scanner run on them. The image will attempt to use any computer names that already exist in the core database.
- **When necessary, use the following template to name target computers:** Provides a template that defines a naming convention to create unique names for target devices that do not currently have a device name assigned to them in the core database. This template is useful for LANDesk agent-discovered and PXE-booted devices. You can review the examples on the wizard page.

You can also create custom naming conventions. For details, see "Creating custom computer names" on page 571.

About the deploy image dialog: Hardware-independent imaging page

Use this page to configure the use of hardware-independent imaging (HII) in a script. The hardware-independent imaging tool (hiiclient.exe) lets you create a single provisioning template or deployment script that can be deployed to multiple device models. A base image is installed on the device, and the HII tool then injects drivers that are specific to the device model.

This option is only used in images based on the Windows preboot environment. After the OS is installed, but before the device reboots, the HII tool detects the device model and retrieves drivers for that model. The drivers are installed onto the device and their information is included in the registry. After a reboot, when the OS starts it configures the drivers.

- **Auto detect:** select this option to have the HII tool automatically select the manufacturer and model of the device you are imaging, based on the strings in the device's BIOS. You should select this option if you want to use the image for devices from multiple manufacturers.
- **Select manufacturer and model:** select this option *only* if you will use the image on the same device model every time. Select a manufacturer from the list, then select a model from the list. The device drivers associated with this model are listed for your reference.

For more information about hardware-independent imaging, see "Hardware-independent imaging" on page 216

About the deploy image dialog: LANDesk agent page

Use this page to provide the following information needed by the image to install LANDesk device software onto target devices:

- **UNC path to directory containing WSCFG32.EXE:** Specifies the UNC path (usually \\<corename>\LDLogon) to the core server or service center where WSCFG32.EXE (the LANDesk device setup file) resides.
- **LANDesk credentials to access core servers:** Provides a domain\username, password, and confirmed password to authenticate to the core server or service center, so that the image can install WSCFG32.EXE onto target devices.

About the Capture profile dialog: Storage UNC page

The options on this page also appear in the deploy image and restore profile dialogs' **Profile storage** page. Use this page to specify where to store the profile data and to provide authentication credentials:

- **UNC path to profile storage directory:** Specifies the UNC path to where the profile data will be stored. You can enter just the computer name in UNC format, then browse for the remainder of the path by clicking the Browse button.
- **Domain and user name:** Identifies a user with valid authentication credentials to the specified UNC path.
- **Password/Confirm password:** Specifies the user's password.
- **Force authentication using these credentials:** Forces an authentication (log out and log in using the credentials specified above) on devices that are scheduled for a profile migration IF the currently logged in user's credentials fail. If such a failure occurs, checking this option ensures that the device has sufficient rights to access and save data on the network share where the profile data will be stored.

About the Capture profile dialog: UMA command file

Use this page to specify the location of the UMA command file that is used to capture user profiles. This command file is an XML file that specifies what elements to include in the profile to be captured. This page also lets you edit the most common elements in the UMA command file, without opening the file and editing the XML code directly.

- **Select user migration assistant command XML file:** Click **Browse** and select the location of the XML file.
- **Edit:** Click this button to open the **Migration settings** dialog box. Select the UMA command file that you want to edit, and click the **Edit** button. Or, to create a new command file, click **New**.
  - **Save to:** Specify the name of the XML file.
  - **Desktop settings:** Select the check box for each desktop item that you want to capture in the profile.
  - **Application settings:** Select the check box for each application for which you want to capture user settings in the profile.
  - **Network settings:** Select the check box for each network and drive setting that you want to capture in the profile.

For more information about Profile migration and the UMA command file, see "Profile migration overview" on page 257

About the DOS task script editor: General page

Use this page to create a script that runs DOS commands (including application executable names) on target devices. The commands are sent to devices one at a time.

- **Name:** Identifies the script with a unique name. If the name you enter is already being used, you'll be prompted to replace the existing script. You should enter a name that helps you quickly and easily identify the script by its function or by the intended target devices on your network.
- **Description:** Additional text you can add to describe the script.
- **Enter the DOS commands to execute on this device:** DOS commands can be added to this box, one per line, as if you were typing at a DOS command prompt. You can enter as many commands as you like.
- **Abort this job if any command fails:** Causes the imaging job to abort if any of the DOS commands entered on this page fail. Applications (launched from the DOS command line) that generate a DOS errorlevel code when failing will also cause the imaging job to abort. If no errorlevel code is created when a command or application fails, the imaging job will continue.

Validating the OS deployment boot environments

The Linux PE boot environment is the only environment OS deployment supports that doesn't require additional validation. Before you can use the DOS or Windows PE* boot environments, OS deployment has to verify you have a license to use the files that the boot environment requires.

- DOS: License verification requires a Windows NT 4 server CD and a Windows 98 CD. This 7 MB image is the smallest one, reducing the network bandwidth used. It potentially is the slowest at creating and restoring images, and has lower hardware compatibility than the other imaging solutions.
- Windows PE: License verification requires a Windows PE 2005 CD and a Windows 2003 SP1 CD. This 120 MB image is the largest one. It has the best hardware compatibility and is potentially the fastest at creating and restoring images. The imaging speed benefits from 32-bit drivers and applications. This imaging environment also supports Microsoft's imaging tools.

*This product contains Windows software licensed from Microsoft Corporation and/or Microsoft Affiliate(s).

Adding additional drivers to the Windows PE image

If you have hardware on your devices that isn't supported by the standard Windows PE image, you can add drivers to the image. This dialog supports two main types of drivers:

- OEM storage drivers that include a txtsetup.oem file.
- Non-OEM drivers that include a .inf file.

To add drivers to the Windows PE image

1. In the **Operating System Deployment** pane, click the **Add additional drivers into the Windows PE image** toolbar button.
2. Browse for the Windows PE image file you want to update.
3. Click the type of driver you're installing and click **Next**.
4. Browse for the drivers .inf or txtsetup.oem file and associated files. Click **Next**.
5. Enter the amount of space you want to leave in the Windows PE image after resizing it.
6. Click **Next** when done.

Resizing the Windows PE image

If necessary, you can add space to a Windows PE image.

To add space to a Windows PE image

1. In the **Operating System Deployment** pane, click the **Resize the Windows PE image** toolbar button.
2. Browse for the Windows PE image file you want to update.
3. Enter the amount of space you want to leave in the Windows PE image after resizing it. You can enter a negative number to reduce the image size.
4. Click **OK** when done.

Changing the Windows PE image wallpaper

If necessary, you can change the Windows PE image wallpaper.

To add space to a Windows PE image

1. In the **Operating System Deployment** pane, click the **Change the wallpaper of the Windows PE image** toolbar button.
2. Browse for the Windows PE image file you want to update.
3. Browse for the wallpaper file you want to use. For best results, use a 24-bit 800x600 bitmap file.
4. Click **OK** when done.

Patch and Compliance help

The Patch and Compliance tool window (**Tools > Security > Patch and Compliance**) is where you perform security scanning, remediation, and related tasks. You can download and manage security content, configure security and compliance scans, configure remediation, customize and apply security scanner display/interaction settings, and view comprehensive security-related information for scanned devices.

The main section for "Patch and Compliance" on page 296 introduces this security management tool. In that section you'll find overview and security content subscription information, step-by-step instructions on how to use all of the tool's features, including a description of the tool's interface and functionality, see "Understanding and using the Patch and Compliance tool" on page 302.

This section contains the following online help that describes the Patch and Compliance dialogs. From the console interface, these help sections are accessed by clicking the **Help** button on their respective dialog.

- "Patch and Compliance tool window help" on page 649
- "Download security content updates help" on page 651
- "Definition properties help" on page 655
- "Detection Rule properties help" on page 658
- "Patch and Compliance tasks help" on page 666
- "Patch and Compliance settings help" on page 672
- "Patch and Compliance toolbar help" on page 680

Patch and Compliance tool window help

About the Select columns dialog

Use this dialog to configure data columns for item lists in the Patch and Compliance tool window. You decide which data columns are displayed so that you can sort through long lists of downloaded security definitions and quickly and easily find the information you need for a specific task or situation.

Using the CVE ID data column
LANDesk security products support the CVE (Common Vulnerabilities and Exposures) naming standard. With Patch and Compliance you can search for vulnerabilities by their CVE names, and view CVE information for downloaded vulnerability definitions. For more information about the CVE naming convention, LANDesk compatibility with the CVE standard, and how to use CVE identification to find individual vulnerabilities in Patch and Compliance, see "Using CVE names when searching for vulnerabilities" on page 331.

By adding and removing data columns, and moving them up and down in the list (to the left and to the right in the column view), you ensure that important, relevant information is front and center.

- **Available columns:** Lists the data columns that are currently not displayed in the Patch and Compliance tool window, but are available to add to the Selected Columns list.
- **Selected columns:** Lists the data columns that are currently displayed in the Patch and Compliance window. The data columns display in a downloaded security definition list from left to right in the same order as they appear here from top to bottom.
- **Defaults:** Restores the default displayed data columns.

About the Manage filters dialog

Use this dialog to manage filters you can use to customize the security content that displays in the Patch and Compliance window's item list. You can use filters to streamline a lengthy list.

- **New:** Opens the Filter Properties dialog where you can configure a new filter's settings.
- **Edit:** Opens the Filter Properties dialog where you can modify and save the selected filter.
- **Delete:** Removes the selected filter permanently from the database.
- **Use filter:** Applies the selected filter to the current item list. The applied filter persists when you click different groups in the tree view.

About the Filter properties dialog

Use this dialog to create or edit security content list filters. You can filter by operating system, security risk severity, or any combination of both.

- **Filter name:** Identifies the filter by a unique name. This name appears in the Filter drop-down list.
- **Filter operating systems:** Specifies the operating systems whose definitions you want to display in the item lists. Only those items associated with the operating systems you select are displayed.
- **Filter severities:** Specifies the severities whose definitions you want to display in the items lists. Only those items whose severity matches the ones you select are displayed.

Download security content updates help

About the Download Updates dialog

Use this dialog to configure settings for downloading security content updates, proxy server, patch file download location, spyware autofix, and antivirus updates and backups.

After you specify the types of content updates you want to download and the other options on the pages of the Download updates dialog:

- To perform an immediate download, click **Update Now**. If you click **Apply**, the settings you specify will be saved and will appear the next time you open this dialog. If you click **Close**, you'll be prompted whether you want to save the settings.
- To schedule a download security content task, click **Schedule update** to open the **Scheduled update information** dialog, enter a name for the task, verify the information for the task, and then click **OK** to add the task to Scheduled tasks.

To save your changes on any page of this dialog, click **Apply**.

The **Download updates** dialog contains the following pages:

- "About the Updates page" on page 651
- "About the Proxy settings page" on page 653
- "About the Patch location page" on page 653
- "About the LANDesk Antivirus page" on page 654

Security content downloading considerations

Security Suite content subscriptions

A basic LANDesk Management Suite installation allows you to download and scan for LANDesk software updates, and to create and use your own custom definitions. For all other security content types, such as platform-specific vulnerabilities, spyware, etc., you must have a LANDesk Security Suite content subscription in order to download the associated definitions.

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Task-specific settings and global settings

Note that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific.

However, all of the settings on the other pages of the Download updates dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global settings it is effective for all security content download tasks from that point on.

About the Updates page

- **Select update source site:** Specifies the LANDesk Security content server that is accessed to download the latest definitions, detection rules, and associated patches to your database. Select the server nearest your location.
- **Definition types:** Identifies which security content definitions are updated. Only those definition types for which you have a subscription are available. The more definition types you select, the longer the download will take.

After you've downloaded security content, you can use the **Type** drop-down list in the main Patch and Compliance tool window to determine which definition types are displayed in a list. For information on using the list options, see "Type drop-down list" on page 304. For information on how the security scanner works for each different type, see "How Patch and Compliance scans for different security risks" on page 333.

- **Languages:** Identifies the language versions of the selected definition types that are updated.

  Some vulnerability and other definition types, and any associated patches, are language neutral or independent, meaning they are compatible with any language version of the OS or application addressed by that definition. In other words, you don't need a unique language-specific patch to remediate those vulnerabilities because the patch covers all supported languages. For example, Linux and UNIX platforms use only language neutral definitions and patches. However, Microsoft Windows and Apple Macintosh platform vulnerability definitions and patches are nearly always language specific.

  When downloading content for any platform (with the appropriate security content subscription), all of the selected platform's language neutral vulnerability definitions are automatically updated by default. If you've selected a Windows or Mac content type, you must also select the specific languages whose definitions you want to update. If you've selected the Sun Solaris or a Linux platform, you do not have to select a specific language because their content is language neutral and will be updated automatically.
- **Download patches for definitions selected above:** Automatically downloads patch executable files to the specified download location (see Patch Location page), according to one of the following download options:
  - **For detected definitions only:** Downloads only the patches associated with vulnerabilities, security threats, or LANDesk updates detected by the last security scan (i.e., the definitions that are currently residing in the Detected group).
  - **For all downloaded definitions:** Downloads ALL of the patches associated with vulnerabilities, security threats, and LANDesk software updates currently residing in the Scan group.
- **Enable automatic patch deployment using Process Manager:** Lets you configure the LANDesk Process Manager database that is required for using the integrated automatic patch deployment feature.
- **LANDesk Process Manager:** Click the button to open the Automating Patch Deployment dialog describing the integrated capability between LANDesk Process Manager and the Patch and Compliance tool that allows you to create a workflow that automates patch deployment to target devices. You also have the option of viewing a tutorial that steps you through this procedure. LANDesk Process Manager includes online help that you can access any time for detailed information about its features and how to use them.
- **Put new definitions in Unassigned group (unless overridden by definition group settings):** Automatically places new definitions and associated detection rules in the Unassigned group instead of in the default Scan group. Select this option if you want to be able to manually move content in and out of the Scan group in order to customize the security scan.

  Note: Definitions that have dependency with another definition that already exists in a different group, such as the Scan or Do Not Scan group, are automatically placed in that group even if this option is selected. In other words, the dependency relationship overrides this option so that the most recently downloaded (new) definition is in the same group as the definition with which it has dependency.

  Note: Definitions that have already been selected to be placed in the Alert group (in the

Configure Alerts dialog) are automatically placed in the Scan group as well, even if this option is selected, so that the appropriate alerting takes place.

Note: For the blocked application type, the default download location is different. Blocked application definitions are downloaded to the Unassigned group by default, not the Scan group. Therefore you don't have to select this option if you're downloading only blocked application definitions.

- **Definition group settings:** Opens the Definition group settings dialog where you can create, manage, and select definition groups. You can use definition group settings to automate how security definitions (content) that match specified type and severity criteria are downloaded, their scan status, and the download location.

About the Proxy settings page

If your network uses a proxy server for external transmissions (such as Internet access), use this page to enable and configure the proxy server settings. Internet access is required for both updating vulnerability information, and for downloading patch files from appropriate Web services.

- **Use proxy server:** Enables the proxy server option (by default, this option is off). If you enable a proxy server, you must fill in the address and port fields below.
- **Server:**
  - **Address:** Identifies the IP address of your proxy server.
  - **Port:** Identifies the port number of your proxy server.
- **HTTP based Proxy:** Enables the proxy server, if it's an HTTP-based proxy (such as Squid), so that it will successfully connect to and download patches from FTP sites. (Patches hosted at some FTP sites cannot be downloaded through an HTTP-based proxy unless you first enable this option).
- **Requires login:** Allows you to enter a username and password if the proxy server is credentialed instead of a transparent proxy server.
  - **Username:** Enter a valid username with authentication credentials to the proxy server.
  - **Password:** Enter the user's password.

About the Patch location page

Use this page to specify where patch executables are downloaded.

- **UNC path where patches are stored:** Specifies where patch files are downloaded. The default location is the core server's \LDLogon\Patch folder. You can enter a different UNC path to download patches, but you must ensure access to that location by entering valid authentication credentials in the fields below.
- **Credentials to store patches:** Identifies a valid username and password for accessing a location other than the core server. If you're downloading patches to the default location on the core server, the username and password fields are not applicable.
- **Web URL where clients access patches:** Specifies a Web address where devices can access downloaded patches for deployment. The default location is the core server's \LDLogon\Patch folder. This location will normally be the same as the UNC path specified above.
- **Test settings:** Performs a connectivity test to the specified Web URL.
- **Reset to default:** Restores both the UNC path and the Web URL to the default location, which is the core server's \LDLogon\Patch folder.

About the LANDesk Antivirus page

Use this page to configure download options for LANDesk Antivirus virus definition files. Keep in mind this page applies only to actual virus definition files that are used by LANDesk Antivirus; it does not apply to the antivirus scanner detection content (Antivirus updates) that are available in the definition list on the **Updates** page.

For detailed information, see "About the LANDesk Antivirus page on the Download Updates dialog" on page 596.

Definition properties help

About the Definition properties dialog

Use this dialog to view properties for downloaded content definition types, including vulnerabilities, spyware, security threats, software updates, etc. You also use this page to create your own custom definitions.

This information is read-only for downloaded definitions. For custom definitions, the fields on this dialog are editable. You can enter identification, attribute, and detection rule details information for a custom definition by using the available fields on this dialog and on the detection rule properties dialog. For more information, see "Creating custom definitions and detection rules" on page 324.

Use the left and right arrow buttons (<, >) to view the previous or next definition's property information, in the order they are currently listed in the main window.

The Definition properties dialog contains the following pages:

- "About the Definition: General page" on page 655
- "About the Definition: Description page" on page 656
- "About the Definition: Dependencies page" on page 656
- "About the Definition: Custom Variables page" on page 656

About the Definition: General page

- **ID:** Identifies the selected definition with a unique, vendor-defined alphanumeric code (or user-defined in the case of a custom definition).
- **Type:** Identifies the selected item as a vulnerability, security threat, custom definition, etc.
- **Publish Date:** Indicates the date the selected definition was published by the vendor (or created by a user).
- **Title:** Describes the nature or target of the selected definition in a brief text string.
- **Severity:** Indicates the severity level of the definition. For downloaded content, this severity level is assigned by the vendor. For a custom definition, the severity is assigned by whoever created the definition. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown. Use this information to evaluate the risk posed by the definition, and how urgent scanning and remediation are for your network.
- **Status:** Indicates the status of the definition in the Patch and Compliance window. The three status indicators are: Scan, meaning the selected item is enabled for the next security scan; Don't Scan, meaning it won't be scanned; and Unassigned, meaning it is in a temporary holding area and won't be scanned. For more information about these three states/groups, see "Understanding and using the Patch and Compliance tool" on page 302.
- **Language:** Indicates the language of the platform identified by the definition. For custom definitions, INTL is the default value meaning the definition is language independent, and can't be edited.
- **Category:** Indicates a more specific category within an individual security content type (see above).
- **Detection Rules:** Lists the detection rules associated with the selected definition. Note that **Downloaded** indicates whether associated patch files are downloaded to the local repository, and **Silent Install** indicates whether the patch installs without user interaction.

You can right-click a detection rule to download its associated patch (or patches), disable/enable the detection rule for security scanning, uninstall its associated patches, or view its properties. You can also double-click a detection rule to view its properties.

If you're working with a custom definition, click **Add** to create a new detection rule; click **Edit** to modify the selected rule; or click **Delete** to remove the selected rule. For more information on custom definitions, see "To create custom detection rules" on page 326.

About the Definition: Description page

- **Description:** Provides additional details about the selected definition. This information is provided by vendor research and test notes (or by the user who created the custom definition).
- **More information at:** Provides a HTTP link to a vendor-specific (or user-defined Web page), typically a support site, with more information about the selected definition.
- **More information for CVE ID:** (Applies only to vulnerabilities) Provides the CVE ID (name) for the selected vulnerability, plus a link to the CVE Web page for that specific CVE ID. For more information, see "Using CVE names when searching for vulnerabilities" on page 331.

About the Definition: Dependencies page

This page displays only if the selected definition has an associated prerequisite definition, or if another definition depends on the selected definition before it can run. You can use this page to make sure your security scan task contains all the definitions necessary to operate properly before scanning devices.

A dependency relationship can exist only for the following security definition types:

- **Prerequisites:** Lists any definitions that have to be run BEFORE the selected definition can be checked for on devices. If any of the definitions in this list aren't included in your scan task, the selected definition won't be detected by the security scanner.
- **Dependencies:** Lists any definitions that won't be detected by the security scanner until AFTER the selected definition is run. Note that the selected definition will be scanned for even if these definitions aren't included in your security scan task. However, if you want your scan task to successfully detect a definition in this list, the selected definition must be run first.

About the Definition: Custom Variables page

This page displays ONLY if the selected security definition includes settings or values that can be modified. Some system configuration security threat definitions have variable settings that you can change before including them in a security scan. Typically, antivirus definitions also have custom variable settings.

With custom variables you can fine-tune security threat scanning by modifying one or more setting's values so that the scanner checks for conditions you define, and therefore determines a device to be vulnerable only if that condition is met (i.e., the value you specify is detected).

Edit Custom Variables right required
In order to edit custom variable settings, a LANDesk user must have the Edit Custom Variables role-based administration right. Rights are configured with the **Users** tool.

Every security definition with customizable variables has a unique set of specific values that can be modified. In each case however, the **Custom Variables** page will show the following common information:

- **Name:** Identifies the custom variable. The name can't be modified.
- **Value:** Indicates the current value of the custom variable. Unless the variable is read-only, you can double-click this field to change the value.

- **Description:** Provides additional useful information about the custom variable from the definition publisher.
- **Default value:** Provides the default value if you've changed it and want to restore it to its original value.

To change a custom variable, double-click the **Value** field, and either select a value if there's an available drop-down list, or manually edit the value, and then click **Apply**. Note that some variables are read-only and can't be edited (this is usually indicated in the description).

Custom variable override settings information can be viewed in the device's Inventory view.

Custom variable override settings
In some situations you may want to ignore a custom variable settings, or in other words create an exception to the rule. You can do this with a feature called custom variable override settings. Custom variable override settings let you decide which custom variables to essentially ignore when scanning devices so that they are not detected as vulnerable and are not remediated even if they meet the actual conditions of a definition's detection rules. You can create as many custom variable override settings as you like, and apply them to devices using a **Change settings** task. For more information, see "About the Custom variable override settings dialog" on page 677.

Detection Rule properties help

About the Detection Rule properties dialog

Use this dialog to view detection rule properties for downloaded security content, or to create and edit custom detection rules.

This information is read-only for detection rules belonging to downloaded definitions. For custom definitions, the fields on the pages of this dialog are editable. You can specify detection rule settings and configure the options on each page in order to create custom detection rules. Furthermore, if the custom detection rule allows remediation, you can add special commands that run during remediation (patch install or uninstall).

You can use the left and right arrow buttons (<, >) to view property information for the previous or next detection rule in the order they are currently listed in the main window.

The Detection rule properties dialog contains the following pages:

- "About the Detection rule: General information page" on page 658
- "About the Detection logic: Affected platforms page" on page 659
- "About the Detection logic: Affected products page" on page 659
- "About the Detection logic: Files used for detection page" on page 659
- "About the Detection logic: Registry settings used for detection page" on page 660
- "About the Detection logic: Custom script page" on page 660
- "About the Patch information page" on page 661
- "About the Detecting the patch: Files used for installed patch detection page" on page 662
- "About the Detecting the patch: Registry settings used for installed patch detection page" on page 662
- "About the Patch install commands page" on page 663
- "About the Patch uninstall commands page" on page 665

About the Detection rule: General information page

- **Name:** Displays the name of the detection rule.
- **State:** Indicates whether the detection rule is set to scan or not to scan. These two states correspond to the Scan and Don't Scan groups (under Detection Rules in the Patch and Compliance window).
- **ID:** Shows the ID of the definition associated with this rule.
- **Title:** Shows the title of the definition associated with this rule.
- **Description:** Shows the description of the definition associated with this rule.
- **Comments:** Provides additional information from the vendor, if available. If you're creating or editing a custom definition, you can enter your own comments.

Detection logic pages

The following pages refer to the detection logic used by the selected detection rule to determine whether the vulnerability definition (or other definition type) exists on a scanned device.

About the Detection logic: Affected platforms page

Identifies the operating systems the security scanner will run on to check for this rule's associated definition. In other words, only devices matching the selected platforms will attempt to process this rule. At least one platform MUST be selected. If a target device is running a different operating system, the security scanner quits.

About the Detection logic: Affected products page

- **Products:** Lists the products you want to check for with the detection rule to determine whether the associated definition exists on scanned devices.. Select a product in the list to view its name, vendor, and version information. You do not need to have a product associated with a detection rule. Associated products act as a filter during the security scan process. If none of the specified associated products are found on the device, the security scan quits. However, if no products are specified, the scan proceeds to the files check.

If you're creating or editing a custom detection rule, click **Configure** to open a new dialog that lets you add and remove products in the list. The list of available products is determined by the security content you've updated via the LANDesk Security service.

- **Name:** Provides the name of the selected product.
- **Vendor:** Provides the name of the vendor.
- **Version:** Provides the version number of the selected product.

About the Detection logic: Files used for detection page

- **Files:** Lists the file conditions (existence, version, date, size, etc.) that are used to determine whether the associated definition exists on scanned devices. Select a file in the list to view its verification method and expected parameters. If all the file conditions are met, the device is not affected. Said another way, if any of these file conditions are NOT met, the vulnerability is determined to exist on that device. If there are no file conditions in the list, the scan proceeds to the registry check.
  If you're creating or editing a custom detection rule, click **Add** to make the fields editable, allowing you to configure a new file condition and expected values/parameters. A rule can include one or more file conditions, depending on how complex you want to make it. To save a file condition, click **Update**. To delete a file condition from the list, select it and click **Remove**.
- **Verify using:** Indicates the method used to verify whether the prescribed file condition is met on scanned devices. For example, a detection rule can scan for file existence, version, date, size, and so on. The expected parameters that appear below the verification method are determined by the method itself (see the list below).

  If you're creating or editing a custom detection rule, select the verification method from the **Verify using** drop-down list. As stated above, the parameter fields are different for each verification method, as described in the following list:

  Note that the **Search for file recursively** option applies to all the file verification methods except for the MSI methods, and causes the scan to search for files in the specified path location and any existing subfolders.

- **File Existence Only:** Verifies by scanning for the specified file. Parameters are: Path (location of the file on the hard drive), including the filename, and Requirement (must exist or must not exist).
- **File Version:** Verifies by scanning for the specified file and its version number. Parameters are: Path, Minimum Version, and Requirement (must exist, must not exist, or may exist).

Note that for the File Version, Date, and Size parameters, after specifying the file path and name, you can click the **Gather Data** button to automatically populate the appropriate value fields.

- **File Date:** Verifies by scanning for the specified file and its date. Parameters are: Path, Minimum Date, and Requirement (must exist, must not exist, or may exist).
- **File Size and/or Checksum:** Verifies by scanning for the specified file and its size or checksum value. Parameters are: Path, Checksum, File size, and Requirement (must exist, must not exist, or may exist).
- **MSI Product ID installed:** Verifies by scanning to ensure the specified MSI product is installed (a product installed by the Microsoft Installer utility). Parameters are: Guid (the product's global unique identifier).
- **MSI Product ID NOT installed:** Verifies by scanning to ensure the specified MSI product isn't installed. Parameters are: Guid.

About the Detection logic: Registry settings used for detection page

- **Registry:** Lists the registry key conditions that are used to determine whether the associated vulnerability (or other type) exists on a scanned device. Select a registry key in the list to view its expected parameters. If any of these conditions are NOT met, the vulnerability is determined to exist on that device.

Important: If there are no registry conditions in the list, AND there were no file conditions on the Files page, the scan fails. In other words, a detection rule must have at least one file or registry condition.

If you're creating or editing a custom detection rule, click **Add** to make the fields editable allowing you to configure a new registry key condition and expected parameters. A rule can include one or more registry conditions. To save a registry condition, click **Update**. To delete a registry condition from the list, select it and click **Remove**.

- **Key:** Identifies the registry key's expected folder and path.
- **Name:** Identifies the expected name of the key.
- **Value:** Identifies the expected value of the key.
- **Requirement:** Indicates whether the registry key must or must not exist on target devices.

About the Detection logic: Custom script page

Use this page if you want to write a custom VB script that checks for any other conditions on scanned devices. The security scanner's runtime properties that can be accessed with a custom script to report its results are: Detected, Reason, Expected, and Found.

Click the **Use editor** button to open your default script editing tool, associated with this file type. When you close the tool you're prompted to save your changes in the Custom Script page. If you want to use a different tool you have to change the file type association.

About the custom vulnerability's product properties: General information page

Use these dialogs when creating a custom vulnerability definition that includes a custom product.

You can enter a name, vendor, and version number, and then define the detection logic that determines the conditions for the vulnerability to exist.

These dialogs are similar to the properties dialogs for downloaded published vulnerability definitions. Please see the corresponding sections above.

This page includes the following options:

- **Affected products:** Lists products that are affected by this custom vulnerability definition.
- **Available products:** Lists all downloaded products.

- **Filter available products by affected platforms:** Restricts the list of available products to only those that are associated with the platforms you've selected on the Detection logic: Affected platforms page.
- **Add:** Opens the Properties dialog where you can create a custom product definition.

About the custom vulnerability's product: Detection logic page

The following pages refer to the detection logic used by the selected detection rule to determine whether the vulnerability definition (or other definition type) exists on a scanned device.

These dialogs are similar to the detection logic dialogs for downloaded known OS and application vulnerability definitions published by vendors that are described above. For information about the options, see the corresponding sections above.

About the custom vulnerability's product: Detection logic: Files used for detection page

See the Detection logic: Files used for detection page above.

About the custom vulnerability's product: Detection logic: Registry settings keys used for detection page

See the Detection logic: Registry settings used for detection page above.

About the custom vulnerability's product: Detection logic: Custom detection script page

See the Detection logic: Custom script page above.

About the Patch information page

Use this page to define and configure the rule's associated patch file (if one is required for remediation) and the logic used to detect whether the patch is already installed. You can also configure additional patch file install or uninstall commands for customized remediation.

This page and the ones under it refer to the patch file required to remediate a vulnerability. These pages are applicable only if the selected detection rule allows remediation by deploying a patch file. If the detection rule is limited to scanning only, or if the security content type doesn't use patch files for remediation, as in the case of security threats, or spyware, then these pages are not relevant.

- **Repaired by patch, or detection only:** Click one of these options to specify whether the detection rule will just check for the presence of the associated definition (detect only), or if it can also remediate that definition by deploying and installing the required patch.
- **Patch download information:**
  - **Patch URL:** Displays the full path and file name of the patch file required to remediate the selected definition if detected. The is location from where the patch file is downloaded.
  - **Auto-downloadable:** Indicates whether the patch file can be automatically downloaded from its hosting server. You can use this option with custom detection rules if you want to prevent patch files from being downloaded via the rule's shortcut menu. For example, you may need to prevent automatic patch download if there's a firewall that blocks access to the hosting server.
  - **Download:** If you're creating or editing a custom detection rule that performs remediation, and you've entered a patch filename and URL, you can click

Download to attempt to download the patch file at this time. You can download the patch file at a later time if you prefer.

- **Repair information:**
  - **Unique filename:** Identifies the unique executable filename of the patch file. Note that it is strongly recommended that when you download a patch file, you create a hash for the patch file by clicking **Generate MD5 Hash**. (Most, if not all, known vulnerability's associated patch files should have a hash.) The patch file must be downloaded before you can create a hash. A hash file is used to ensure the integrity of the patch file during remediation (i.e., when it's deployed and installed on an affected device). The security scanner does this by comparing the hash code created when you click the Generate MD5 Hash button with a new hash it generated immediately before attempting to install the patch file from the patch repository. If the two hash files match, remediation proceeds. If the two hash files do not match, indicating the patch file has changed in some way since being downloaded to the repository, the remediation process quits.
  - **Requires reboot:** Indicates whether the patch file requires a device reboot before completing its installation and configuration processes on the device.
  - **Silent install:** Indicates whether the patch file can complete its installation without any end user interaction.

Detecting the patch pages

The following pages refer to the detection logic used by the rule to check if the patch is already installed on devices.

Important: ALL of the specified conditions for BOTH files and registry settings must be met in order for the patch file to be detected as installed on a device.

About the Detecting the patch: Files used for installed patch detection page

This page specifies the file conditions used to determine whether the patch file is already installed on a device. The options on this page are the same as on the Files page for definition detection logic (see above). However, the logic works conversely when detecting patch installation. In other words, when checking for a patch installation, all of the file conditions specified on this page must be met in order to determine an installation.

About the Detecting the patch: Registry settings used for installed patch detection page

This page specifies the registry key conditions used to determine whether the patch file is already installed on a device. The options on this page are the same as on the Registry settings page for definition detection logic (see above). However, the logic works conversely in this case. In other words, when checking for a patch installation, all of the registry conditions specified on this page must be met in order to determine an installation.

Important: ALL of the specified conditions for BOTH files and registry settings must be met in order for the patch file to be detected as installed on a device.

Patch install and uninstall pages

The following pages let you configure additional commands that run when the patch is installed on or uninstalled from affected devices.

This option is available only for custom definitions that allow remediation.

These commands are useful if you need to program specific actions on target devices to ensure successful remediation. Additional commands aren't required. If you don't configure any additional commands, the patch file executes by itself by default. Keep in mind that if you do configure one or more additional commands, you must also include a command that executes the actual patch file with the Execute command.

About the Patch install commands page

Use this page to configure additional commands for a patch install task. The available commands are the same for patch install and uninstall.

- **Commands:** Lists commands in the order they will run on target devices. Select a command to view its arguments. You can change the order of commands with the **Move Up** and **Move Down** buttons. To remove a command from the list, select it and click **Remove**.
- **Add:** Opens a dialog that lets you select a command type to add to the Commands list.
- **Command Arguments:** Displays the arguments that define the selected command. An argument's values can be edited. To edit any argument, double-click its **Value** field, and then type directly in the field. For all the command types, you can also right-click in the **Value** field to insert a macro/variable into the argument.

The following list describes the commands and their arguments:

- **Copy:** Copies a file from the specified source to the specified destination on the hard drive of the target device. This command can be used before and/or after executing the patch file itself. For example, after extracting the contents of a compressed file with the Unzip command, you may want to copy files from one location to another.

  The arguments for the Copy command are: Dest (full path where you want to copy the file), not including the filename and Source (full path, and file name, of the file you want to copy).

- **Execute:** Runs the patch file, or any other executable file, on target devices.

  The arguments for the Execute command are: Path (full path, and file name, where the executable file resides; for the patch file, you can use the %SDMCACHE% and %PATCHFILENAME% variables), Args (command-line options for the executable file; note this field is not required), Timeout (number of seconds to wait for the executable to terminate before continuing to the next command in the list, if the Wait argument is set to true), and Wait (true or false value that determines whether to wait for the executable to terminate before continuing to the next command in the list).

- **ButtonClick:** Automatically clicks a specified button that displays when an executable file runs. You can use this command to program a button click if such interaction is required by the executable.

  In order for the ButtonClick command to work properly, the Wait argument for the preceding Execute command must be set to false so that the executable doesn't have to terminate before continuing to the button click action.

  The arguments for the ButtonClick command are: Required (true or false value indicating whether the button must be clicked before proceeding; if you select true and the button can't be clicked for any reason, remediation quits; if you select false and the button can't be clicked, remediation will continue, ButtonIDorCaption (identifies the button you want clicked by its text label, or its control ID), Timeout (number of seconds it takes for the button you want clicked appears when the executable runs), and WindowCaption (identifies the window or dialog where the button you want clicked is located).

- **ReplaceInFile:** Edits a text-based file on target devices. Use this command if you need to make any modifications to a text-based file, such as a specific value in an .INI file, before or after executing the patch file to ensure that it runs correctly.

The arguments for the ReplaceInFile command are: Filename (full path and name of the file you want to edit), ReplaceWith (exact text string you want to add to the file, and Original Text (exact text string you want to replace in the file).

- **StartService:** Starts a service on target devices. Use this command to start a service required for the patch file to run, or to restart a service that was required to be stopped in order for the patch file to run.

  The arguments for the StartService command are: Service (name of the service).

- **StopService:** Stops a service on target devices. Use this command if a service must be stopped on a device before the patch file can be installed.

The arguments for the StopService command are: Service (name of the service).

- **Unzip:** Unzips a compressed file on target devices. For example, you can use this command if remediation requires more than one file be run or copied on target devices.

  The arguments for the Unzip command are: Dest (full path to where you want to extract a compressed file's contents on a device's hard drive), and Source (full path and filename of the compressed file).

- **WriteRegistryValue:** Writes a value to the registry.

  The arguments for the WriteRegistryValue are: Key, Type, ValueName, ValueData, WriteIfDataEmpty

About the Patch uninstall commands page

Use this page to configure additional commands for a patch uninstall task. The available commands are the same for patch install and uninstall. However, the Patch uninstall commands page includes two unique options:

- **Patch can be uninstalled:** Indicates whether the patch file can be uninstalled from remediated devices.
- **Original patch is required for uninstall:** Indicates whether the original patch executable file itself must be accessible on the core server in order to uninstall it from scanned devices.

For information on the commands, see "About the Patch install commands page" on page 663.

About the Download associated patches dialog

Use this dialog to download patch executable files that are required to remediate the selected vulnerability but that are not currently available on the core server (or in some other specified patch repository location). Required patches must reside in the designated patch location in order for a managed device with a detected vulnerability to be remediated successfully.

- **Name:** Indicates the name of the patch executable file.
- **Definitions:** Indicates the vulnerability which is associated with this patch file.
- **Downloaded:** Shows whether the patch file has been downloaded or not.
- **Can download:** Indicates whether the patch can be automatically downloaded, or whether it has to be downloaded by a Patch and Compliance process.
- **Show currently required patches only:** Displays only those patch files that are required to remediate the selected vulnerability at this time. In other words, the list will include patches that have superseded earlier patches, not the earlier patches.
- **Show all associated patches:** Displays a comprehensive listing of all of the associated patches for the selected vulnerability, whether they have been superseded or not.
- **Download:** Click to download the patch files from the update source site.
- **Cancel:** Cancels the download operation.

Patch and Compliance tasks help

About the Create security scan task dialog

Use this dialog to create and configure a scheduled task that runs the security scanner on target devices.

IMPORTANT: LANDesk Script Writers group permission required
In order to create scheduled tasks and policies in the Patch and Compliance tool (for security and compliance scan tasks, and repair tasks), a user must have the LANDesk Script Writers group permission. In other words, they must be part of a group that has the LANDesk Script Writers permission assigned. For more information about role-based administration, see "Role-based administration" on page 44.

You can also run an immediate on-demand security or compliance scan on one or more target devices. Right-click the selected device (or up to 20 multi-selected devices), and either click **Security scan** and select a scan and repair settings, or click **Compliance scan**, and then click **OK**.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the security scan task.
- **Create a scheduled task:** Adds the security scan task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the security scan task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Scan and repair settings:** Specifies scan and repair settings used for the scan task. Scan and repair settings determine whether the security scanner displays on devices while running, reboot options, user interaction, and the security content types scanned. Select a scan and repair settings from the drop-down list to assign it to the security scan task you're creating. You can click **Edit** to modify the options for the selected scan and repair settings. You can also click **Configure** to create a new scan and repair settings. For more information, see "About the Configure scan and repair (and compliance) settings dialog" on page 672.

About the Create compliance scan task dialog

Use this dialog to create and configure a task that runs the security scanner to check target devices specifically for compliance with your security policy based on the contents of the Compliance group.

On-demand security and compliance scans
You can also run an immediate security or compliance scan on one or more target devices. Right-click the selected device (or up to 20 multi-selected devices), and either click **Security scan** and select a scan and repair settings, or click **Compliance scan**, and then click **OK**.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the compliance scan task.
- **Create a scheduled task:** Adds the compliance scan task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Target machines that have not reported since:** Limits the compliance scan to only those managed devices that haven't reported security scan results since the date you specify.
- **Start now:** Sets the scheduled scan task to begin as soon as the task is added to the Scheduled tasks window so that you don't have to manually configure scheduling options.

- **Create a policy:** Adds the compliance scan task as a policy to the Scheduled tasks window, where you can configure the policy options.

About the Change settings task dialog

Use this dialog to create and configure a task that changes the default settings on target devices for Patch and Compliance services, including:

- Scan and repair settings
- Compliance security settings (applies only to compliance security scans)
- Custom variable override settings

With a change settings task you can conveniently change a managed device's default settings (which are written to the device's local registry) without having to redeploy a full agent configuration.

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** As the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Scan and repair settings:** Specifies scan and repair settings used for security scan tasks. Scan and repair settings determine whether the scanner displays on devices while running, reboot options, user interaction, and the security content types scanned. Select one of the settings from the drop-down list. Click **Edit** to modify the options for the selected settings. Click **Configure** to create a new settings. For more information, see "About the Scan and repair (and compliance) settings dialog's pages" on page 672.
- **Compliance settings:** Specifies compliance settings used for compliance scan tasks. Compliance settings determine when and how a compliance scan takes places, whether remediation occurs automatically, and/or what to do when LANDesk Antivirus detects a virus infection on target devices.
- **Custom variables override settings:** Specifies custom variable override settings used on target devices when they're scanned for security definitions that include custom variables (such as security threats and viruses). Custom variable override settings let you specify values you want to ignore or bypass during a security scan. This is very useful in situations where you don't want a scanned device to be identified as vulnerable according to a definition's default custom variable settings. Select one of the settings from the drop-down list. From the drop-down list, you can also select to remove the custom variable override settings from target devices. The **Remove custom variable settings** option lets you clear a device so that custom variable settings are in full affect. Click **Edit** to modify the options for the selected settings. Click **Configure** to create a new settings. For more information, see "About the Custom variable override settings dialog" on page 677.

About the Create reboot task dialog

Use this dialog to create and configure a generic reboot task.

A reboot task can be useful when you want to install patches (without rebooting) as a single process and then reboot those remediated devices as another separate task. For example, you can run a scan or a patch install task during the day, and then deploy a reboot only task at a more convenient time for end users.

- **Task name:** Identifies the task with a unique name.
- **Create a scheduled task:** Creates a reboot task in the Scheduled tasks window when you click **OK**.
- **Create a policy:** Creates a reboot policy when you click **OK**.

- **Scan and repair settings:** Specifies which scan and repair settings' reboot configuration is used for the task to determine reboot requirements and action on target devices. Select a scan and repair settings from the drop-down list, or click **Configure** to create a new scan and repair settings.

About the Create repair task dialog

Use this dialog to create and configure a repair (remediation) task for the following definition types: vulnerabilities, spyware, LANDesk software updates, custom definitions, and security threats with an associated patch. The schedule repair option is not applicable to blocked applications.

This dialog includes the following pages:

- "About the Create repair task: General page" on page 668
- "About the Create repair task: Patches page" on page 669

About the Create repair task: General page

- **Task name:** Identifies the repair task with a unique name. The default is the name of the selected definition or the custom group. You can edit this name if you prefer.
- **Repair as a scheduled task:** Creates a security repair task in the Scheduled tasks window when you click **OK**.
- **Split into staging task and repair task:** (Optional) Allows you to create to separate tasks in the Scheduled tasks tool; one task for staging the required patch files in the target device's local cache; and one task for actually installing those patch files on the affected devices.
    - **Select computers to repair:** Specifies which devices to add to the scheduled repair task. You can choose no devices, all affected devices (devices where the definition was detected by the last security scan), or only the affected devices that are also selected (this last option is available only when you access the Schedule repair dialog from within a device Security and Patch Information dialog).
    - **Use Multicast:** Enables Targeted Multicast for patch deployment to devices. Click this option, and click **Multicast Options** if you want to configure multicast options. For more information, see "About the Multicast options dialog" on page 669.
- **Repair as a policy:** Creates a security repair policy when you click **OK**.
    - **Add query representing affected devices:** Creates a new query, based on the selected definition, and applies it to the policy. This query-based policy will search for devices affected by the selected definition, and deploy the associated patch.
    - **Download patch only from local peers:** Restricts patch deployment so that it will only take place if the patch file is located in the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, the patch file must currently reside in one of these two places.
    - **Download patch only (Do not repair):** Downloads the patch file to the patch repository but does not deploy the patch. You can use this option if you want to retrieve the patch file in a staging scenario for testing purposes before actual deployment.
- **Scan and repair settings:** Specifies which scan and repair settings is used for the repair task to determine whether the security scanner displays on devices when it is running. Select an scan and repair settings from the drop-down list, or click **Configure** to create a new scan and repair settings.

About the Create repair task: Patches page

Use this page to show either required patches only or all associated patches for the selected vulnerability. (**Note:** The fields on this page are the same as the fields on the "About the Download associated patches dialog" on page 665.)

To download patches directly from this page, if they have not already been downloaded and placed in the patch repository, click **Download**.

About the Multicast options dialog

Use this dialog to configure the following Targeted Multicast options for a scheduled security repair task:

- **Multicast Domain Discovery:**
  - **Use multicast domain discovery:** Select this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
  - **Use multicast domain discovery and save results:** Select this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
  - **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery that saved the results.
- **Have domain representative wake up computers:** Use this option if you want computers that support Wake On LAN technology to turn on so they can receive the multicast.
- **Number of seconds to wait after Wake on LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

The options below let you configure task-specific Targeted Multicast parameters. The defaults should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time.
- **Limit the processing of machines that failed multicast:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the Custom Job dialog would process no more than 20 computers at a time that failed the multicast. The Custom Job dialog will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the Custom Job dialog won't perform the distribution portion of the task for any computer that failed multicast.
- **Number of days the files stay in the cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged.
- **Number of days the files stay in multicast domain representative cache:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions (WAN or Local):** Minimum amount of time to wait between sending out multicast packets.

This value is only used when the domain representative isn't multicasting a file from its own cache. If this parameter isn't specified, then the default minimum sleep time stored on the subnet/domain representative computer will be used. You can use this parameter to limit bandwidth usage across the WAN.

- **Maximum number of milliseconds between packet transmissions (WAN or Local):** Maximum amount of time to wait between sending out multicast packets. For more information, see Minimum number of milliseconds between packet transmissions above.

About the Uninstall patch dialog

Use this dialog to create and configure an uninstall task for patches that have been deployed to affected devices.

- **Task name:** Identifies the task with a unique name. The default is the name of the patch. You can edit this name if you prefer.
- **Uninstall as a scheduled task:** Creates an uninstall patch task in the Scheduled tasks window when you click **OK**.
    - **Select targets:** Specifies which devices to add to the uninstall patch task. You can choose no devices, all devices with the patch installed, or only the devices with the patch installed that are also selected (this last option is available only when you access the Uninstall Patch dialog from within a device Security and Patch Information dialog).
- **If the original patch is required:**
    - **Use Multicast:** Enables Targeted Multicast for deploying the uninstall patch task to devices. Click this option, and click **Multicast Options** if you want to configure the multicast options. For more information, see "About the Multicast options dialog" on page 669.
- **Uninstall as a policy:** Creates an uninstall patch policy in the Scheduled tasks window when you click **OK**.
    - **Add query representing affected devices:** Creates a new query, based on the selected patch, and applies it to the policy. This query-based policy will search for devices with the selected path installed and uninstall it.
- **Scan and repair settings:** Specifies which scan and repair settings is used for the uninstall task to determine whether the security scanner displays on devices, reboot options, MSI location information, etc. Select an scan and repair settings from the drop-down list, or click **Configure** to create a new scan and repair settings.

About the Gather historical information dialog

Use this dialog to compile data about scanned and detected vulnerabilities on managed devices. This information is used for security reports. You can either gather the data immediately or create a task to collect the data for a specified period of time.

This dialog contains the following options:

- **Task name:** Identifies the gather historical information task with a unique name.
- **Keep historical data for:** Specifies the amount of time (in days) for which data will be collected. You can specify 1 day to 3,000 days.
- **Build report data for definitions published less than:** Restricts the report to data about vulnerabilities published within the specified time period.
- **Warn:** Displays a message on the core server console if a gather historical task has not run in the specified time period.
- **Gather now:** Immediately collects the current data for detected, scanned, and not scanned vulnerabilities.

- **Create task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Purge:** Completely removes the data about vulnerabilities collected to this point.

Patch and Compliance settings help

About the Configure scan and repair (and compliance) settings dialog

Use this dialog to manage your scan and repair (and compliance) settings. Once configured, you can apply settings to security scan tasks, compliance scan tasks, repair tasks, uninstall tasks, and reboot tasks.

This dialog contains the following options:

- **New:** Opens the settings dialog where you can configure the options pertaining to the specified settings type.
- **Edit:** Opens the settings dialog where you can modify the selected settings.
- **Copy:** Opens a copy of the selected settings as a template, which you can then modify and rename.
- **Delete:** Removes the selected settings from the database.

  Note: The selected settings may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that settings still have it and continue to use it until a new change settings task is deployed; scheduled tasks with that settings still run on target devices, as do local scheduler tasks with that settings, until a new configuration is deployed.
- **Close:** Closes the dialog, without applying any settings to the task.

About the Scan and repair (and compliance) settings dialog's pages

Use this dialog to create and edit scan and repair settings. Scan and repair settings determine whether the security scanner displays on devices while running, reboot options, user interaction, and the content types scanned.

Note on compliance scan settings
The information on this dialog can also apply to compliance scans, with the **Compliance** page taking the place of the **Scan** page. See the About the Compliance page section below for details about the specific settings that apply to compliance scans.

Note on reboot task settings
The settings on the **Reboot** page of this dialog can also be used for a reboot only task.

You can create as many scan and repair settings as you like and edit them at any time. For example, you can configure a scan and repair settings with a specific notification and reboot scenario for desktop devices, and another scan and repair settings with different reboot options for servers. Or, you can configure an scan and repair settings for Windows vulnerability scanning, and another one for spyware scanning, etc.

Once configured, you can apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks.

Scan and repair settings

- **Name:** Identifies the settings with a unique name. This name appears in the settings drop-down list on a security task dialog.

The settings dialog contains the following pages:

- "About the General settings page" on page 673
- "About the Scan options page" on page 673
- "About the Compliance settings page" on page 674
- "About the Repair options page" on page 674

About the General settings page

- **Show progress dialog:** Enables the security scanner to display information on end user devices while it is running. Select an option from the drop-down list (Never, Always, Only when repairing) to determine if and when you want to show scanner activity, and if you want to configure other display and interaction options in this dialog. If you select Never, none of the other options on this page are available to configure, and the scanner runs transparently on devices. If you select Always, you can configure the other options.
- **Hide if user is showing a presentation:** Does not display the security scanner on end user devices if the Microsoft Office PowerPoint application is running on the device.
- **Allow user to cancel scan:** Shows a Cancel button on the security scanner dialog on the end user device. Click this option if you want the end user to have the opportunity to cancel a scan operation. If this option is not checked, the dialog doesn't have a Cancel button and the end user can't stop the scan.
- **When no reboot is required:**
  - **Require end user input before closing:** For a scan or repair task that doesn't require a reboot in order to complete its full operation, click this option if you want the scanner to prompt the end user before its display dialog closes on the device. If you select this option, and the end user does not respond the dialog remains open which could cause other scheduled tasks to timeout.
  - **Close after timeout:** For a scan or repair task that doesn't require a reboot, click this option is you want the scanner's display dialog to close after the duration you specify.
- **CPU utilization when scanning:** Lets you fine-tune CPU usage by the security scanner in order to improve overall system performance. If several processes are running concurrently and maximizing CPU utilization on devices, you can reduce this setting for the security scanner.
- **Scheduled task status:** Indicates the level of information sent to the Scheduled tasks tool about the scheduled security scan task.

About the Scan options page

- **Scan for:** Specifies which content types you want to scan for with this scan task. You can select either a custom group (preconfigured) or specific content types. You can select only those content types for which you a LANDesk Security Suite content subscription. Also, the actual security definitions that are scanned for depends on the contents of the Scan group in the Patch and Compliance window. In other words, if you select vulnerabilities and security threats in this dialog, only those vulnerabilities and security threats currently residing in their respective Scan groups will be scanned for.
- **Immediately repair all detected items:** Indicates that any security risk identified by this particular group scan will be automatically remediated.
- **Enable autofix:** Indicates that the security scanner will automatically deploy and install the necessary associated patch files for any vulnerabilities or custom definitions it detects on scanned devices. This option applies to security scan tasks only. In order for autofix to work, the patch file must also have autofix enabled.

About the Compliance settings page

Compliance security scans
Keep in mind the options on the Compliance page apply to compliance security scans only.

- **Scanning:**
  - **Frequently scan the Compliance group:** Runs a frequent security scan based on the contents of the Compliance group. The basic frequent security scan is defined in the initial agent configuration, but you can override it with the options on this page. You can specify to run the compliance security scan only when a user is logged into the managed device.
  - **Scan after IP address change:** Performs a compliance security scan whenever the IP address changes on target devices. For example, if a laptop is reconnected to your network and receives a different IP address than before.
  - **Disable the frequent security scanner in Agent configuration:** Indicates that a frequent security scan set up via the device's agent configuration will be turned off, and the frequent scan settings defined here will be used for a compliance security scan instead.
- **Actions:**
  - **Enable autofix:** Indicates that the security scanner will automatically deploy and install the necessary associated patch files for any vulnerability definitions it detects on scanned devices. This option applies to security and compliance scan tasks only. In order for autofix to work, the must also have autofix enabled.
  - **Immediately repair all detected items:** All detected vulnerabilities are remediated, even if their associated patches do not have autofix enabled.
  - **Enforce 802.1X supported scan:** Ensures that 802.1X-enabled devices that are scanned for security compliance using this settings are either allowed access or quarantined based on their being compliant or non-compliant to the custom security policy.
- **If a virus cannot be removed or quarantined (LANDesk Antivirus only):** The following two options apply to LANDesk Antivirus only and provide a method for you to have an antivirus scan trigger or initiate a full security scan that checks target devices configured with this settings for compliance with your current security policy. In other words, whether the device is healthy or unhealthy. You can select one or both of the options below. The action described by these options occurs any time a virus is detected on the device and can't be removed or quarantined. (**Note:** As a prerequisite for performing this type of scan, you must first add the predefined AV-110 antivirus definition to the Compliance group. You should also add any other definitions you want to use to define your security policy to the Compliance group.)
  - **Immediately scan devices for compliance:** If a virus is detected and can't be removed or quarantined, a compliance security scan (by the security scanner, not the antivirus scanner) is initiated right away.
  - **Perform network access control check to determine if device is unhealthy:** If a virus is detected and can't be removed or quarantined, a network access control check is initiated immediately by LANDesk NAC.

About the Repair options page

- **Before repairing, installing, or uninstalling a patch:** Select whether you want the repair to begin immediately, or if you want a prompt to appear on the end user device with message and interaction controls as configured with the options below, or if you want to wait to perform the repair until the device is locked or the user is logged off.
- **Message:** Type a message in this box that will appear in the security scanner's display dialog on the end user device WHEN a security scan task detects any of the specified definitions on the scanned device. You can customize this message depending on the type of security scan you're running.

- **If no end user response:**
  - **Wait for user response before repair, install, or uninstall:** For a patch file operation prompt that doesn't receive a response, click this option if you want the scanner to continue waiting indefinitely.
  - **After timeout, automatically:** For a patch file operation prompt that doesn't receive a response, click this option if you want the scanner to automatically proceed and perform the patch file operation or close without performing the operation, after the duration you specify.
- **Start repair even if:**
  - **User is running a presentation:** Indicates that remediation will begin regardless of whether the Microsoft Office PowerPoint application is running on the device.
  - **Reboot is already pending:** Indicates that remediation will begin without waiting for the reboot operation.
- **Maximum bandwidth when downloading from source:** Specifies the bandwidth percentage you want to be used for the patch file download from the patch repository to scanned devices. You can use this settings to balance network traffic for large patch file deployments.
- **Maximum bandwidth when downloading from peer:** Specifies the bandwidth percentage you want to be used for the patch file download from a peer machine. You can use this settings to balance network traffic for large patch file deployments.

About the MSI information page

Use this page if a patch file needs to access its originating product installation resource in order to install any necessary supplemental files. For example, you may need to provide this information when you're attempting to apply a patch for Microsoft Office or some other product suite.

- **Original package location:** Enter the UNC path to the product image.
- **Credentials to use when referencing the original package location:** Enter a valid user name and password to authenticate to the network share specified above.
- **Ignore the /overwriteoem command-line option:** Indicates the command to overwrite OEM-specific instructions will be ignored. In other words, the OEM instructions are executed.
- **Run as Information: Credentials for running patches:** Enter a valid user name and password to identify the logged in user for running patches.

About the Reboot options page

- **When deciding whether to reboot:** Specify how you want the security scanner to act when a scan or repair task tries to reboot a device for any reason. You can select for the device to never reboot, reboot only if needed, or always reboot.
- **When rebooting:**
  - **Prompt user before rebooting:** For when a reboot occurs, click this option if you want the security scanner to prompt the end user. If you select this option, you can configure the accompanying reboot options below.
  - **If no one is logged in, reboot immediately without prompting or delay:** Ensures the reboot will occur automatically in the event no one is currently logged into the device.
  - **Allow user to defer reboot:** Shows a defer button on the reboot prompt on the end user device. Specify the deferral time span and the number of times the end user can defer the reboot. The deferral (or snooze time) begins with the next local scheduler poll. (Note that due to local scheduler operation the minimum snooze time is 10 minutes.)

- **Allow user to cancel reboot:** Shows a cancel button on the reboot prompt on the end user device.
- **Reboot message:** Type a message in this box that will appear in the security scanner's display dialog on the end user device WHEN a security scan task prompts the end user before attempting to reboot the device.
- **Wait for user response before rebooting:** For a reboot prompt that doesn't receive a response, click this option if you want the scanner to continue waiting indefinitely. If there's no response, the prompt remains open.
- **After timeout, automatically:** For a reboot prompt that doesn't receive a response, click this option if you want the scanner to automatically proceed and either reboot, snooze, or close the prompt without rebooting, after the duration you specify.

About the Network settings page

Use this page to identify an alternate core server that can be used for security scanning and remediation if the main core server is not available.

- **Communicate with alternate core server:** Enables communication with an alternate server.
- **Server name:** Enter the name of a valid, licensed LANDesk core server.

Note: The syntax for the servername field should be: <servername>:<port number> where port number is the secure port 443 for SSL transmission. If you enter only a servername, without specifying port 443, it defaults to port 80 which is the standard HTTP port.

About the Pilot configuration page

Use this page to create and configure a pilot group for testing security definitions before performing a wider deploying on your entire network.

- **Periodically scan and repair definitions in the following group:** Enables the pilot security scan features. Once you've checked this option, you need to select a custom group from the drop-down list.
- **Change settings:** Opens the Schedule scan dialog where you can define the parameters for the security scan. Click the **Help** button for details.

About the Schedule periodic pilot scan and repair dialog

This dialog is shared by several LANDesk management tasks. For details about the options on this dialog, see "About the Schedule dialog" on page 683.

About the Spyware scanning page

Use this page to replace (or override) spyware settings from a device's agent configuration.

Real-time spyware detection monitors devices for new launched processes that attempt to modify the local registry. If spyware is detected, the security scanner on the device prompts the end user to remove the spyware.

This page contains the following options:

- **Override settings from client configuration:** Replaces existing spyware settings on devices initially configured via an agent configuration. Use the options below to specify the new spyware settings you want to deploy to target devices.
- **Settings:**
  - **Enable real-time spyware blocking:** Turns on real-time spyware monitoring and blocking on devices with this agent configuration.

    Note: In order for real-time spyware scanning and detection to work, you must manually enable the autofix feature for any downloaded spyware definitions you want included in a security scan. Downloaded spyware definitions don't have autofix turned on by default.

- **Notify user when spyware has been blocked:** Displays a message that informs the end user a spyware program has been detected and remediated.
- **If an application is not recognized as spyware, require user's approval before it can be installed:** Even if the detected process is not recognized as spyware according to the device's current list of spyware definitions, the end user will be prompted before the software is installed on their machine.

About the Configure custom variable override settings dialog

Use this dialog to manage your custom variable override settings. Once configured, you can apply custom variable override settings to a change settings task and deploy it to target devices to change (or remove) their default custom variable override settings.

Custom variables overrides lets you configure exceptions to custom variable values. In other words, with custom variable override settings you can ignore or bypass a specific custom variable condition so that a scanned device is not determined to be vulnerable.

This dialog contains the following options:

- **New:** Opens the Custom variable override settings dialog where you can configure the options.
- **Edit:** Opens the settings dialog where you can modify the selected custom variable override settings.
- **Copy:** Opens a copy of the selected settings as a template, which you can then modify and rename.
- **Delete:** Removes the selected settings from the database.

  Note: The selected settings may currently be associated with one or more tasks or managed devices. If you choose to delete the settings, devices with that settings still have it and continue to use it until a new change settings task is deployed; scheduled tasks with that settings still run on target devices, as do local scheduler tasks with that settings, until a new configuration is deployed.
- **Close:** Closes the dialog, without applying any settings to the task.

About the Custom variable override settings dialog

Use this dialog to create exceptions to custom variable settings. Some system configuration security threat definitions have variable settings that you can change before including them in a security scan. Typically, antivirus definitions also have custom variable settings.

With custom variables you can fine-tune security threat scanning by modifying one or more setting's values so that the scanner checks for conditions you define, and therefore determines a device to be vulnerable only if that condition is met (i.e., the value you specify is detected). Custom variables are a global settings, so when you scan for a security definition that includes a custom variable it will always be determined to be vulnerable if that custom variable condition is met.

Edit Custom Variables right required
In order to edit custom variable settings, and configure custom variable override settings, a LANDesk user must have the Edit Custom Variables role-based administration right. Rights are configured with the **Users** tool.

Custom variable override settings information can be viewed in the device's Inventory view.

About the Definition group settings dialog

Use this dialog to create, edit, and select settings that control how and where security definitions are downloaded based on their type and/or severity.

This dialog contains the following options:

- **Definition type and severity filters:** Lists definition group settings.
- **Type:** Shows the definition type for the selected group settings.
- **Severity:** Shows the definition severity for the selected group settings.
- **Status:** Shows the status (Do not scan, Scan, and Unassigned) for definitions that match the group settings when they're downloaded. Status corresponds to the group nodes in the tree view. Unassigned is the default status.
- **Group(s):** Shows the group or groups where the security definitions matching the type and severity criteria specified above are placed. You can add and delete as many custom groups as you like.
- **Autofix:** If you've specified that downloaded security definitions are set to Scan status (placed in the Scan group), select this option if you want the vulnerabilities to have autofix enabled.

About the Definition filter properties dialog

Use this dialog to define a definition group settings. These settings control how and where security definitions are downloaded based on their type and/or severity.

This dialog contains the following options:

- **Filter:** Defines which security content (definitions) will be place in the group or groups selected below.
  - **Definition type:** Select the definition type you want to download with your desired status and location.
  - **Severity:** Select the severity for the specified definition type. If the type matches but the severity does not, the definition will not be filtered by this settings.
- **Action:** Defines what you want to do with the downloaded definitions and where you want them placed.
  - **Set status:** Select the status for the downloaded definitions. Options include: Do not scan, Scan, and Unassigned.
  - **Set autofix:** Select autofix if the status is Scan and you want the security risk to be fixed automatically upon detection.
  - **Put definition in custom groups:** Select one or more groups with the Add and Delete buttons. You can select any of the custom groups you've created, the Alert group, the Compliant group, and several of the available security industry groups.

About the Alert settings dialog

Use this dialog to configure security-related alerting for scanned devices, including both vulnerability and antivirus alerting.

The Alert settings dialog contains the following pages:

Definitions page

Use this page to configure security alerting. If you've added security definitions to the Alert group, Patch and Compliance will alert you whenever any of those definitions is detected on any scanned device.

- **Minimum alert interval:** Specifies the shortest time interval (in minutes or hours) in which alerts for detected vulnerabilities are sent. You can use this settings if you don't want to be alerted too frequently. Set the value to zero if you want instant, real-time alerting to occur.
- **Add to Alert group:** Indicates which vulnerabilities, by severity level, are automatically placed in the Alert group during a content download process. Any definition placed in the Alert group is also automatically placed in the Scan group by default (in order to include those definitions in a security scan task).

Antivirus page

Use this page to configure antivirus alerting.

- **Minimum alert level:** Specifies the shortest time interval (in minutes or hours) in which alerts for detected viruses are sent. You can use this settings if you don't want to be alerted too frequently. Set the value to zero if you want instant, real-time alerting to occur.
- **Alert on:** Indicates which antivirus events generate alerts.

About the Rollup core settings dialog

Use this dialog to enable and configure automatic forwarding of the latest security scan results to a rollup core server on your network. Security scan data forwarding allows you to view real-time vulnerability status for all of your managed devices in a large, distributed enterprise network without having to manually retrieve that data directly from the primary core server.

Every time the security scanner runs it writes a scan results file to a folder called VulscanResults on the core server and notifies the LANDesk Security web service, which adds the file to the core database. If the rollup core settings are enabled and a valid rollup core is identified, the rollup core reads the scan results file into its own database, providing faster access to critical vulnerability information.

The Rollup core settings dialog contains the following options:

- **Send scan results to rollup core immediately:** Enables immediate forwarding of security scan results to the specified core server, using the method described above.
- **Use default rollup URL:** Check this box if you want the default URL to be used when the scan results file is sent from the core server to the rollup core. Enter the name of the core server, and then check this box to automatically insert the script and Web address in the **Rollup URL** field.
- **Rollup core name:** Identifies the rollup core you want to receive the latest security scan results from the core database.
- **Rollup URL:** Specifies the Web address of the rollup core receiving the security scan results and the destination folder for the scan results file on the rollup core. The rollup URL can either be automatically inserted by checking the **Use default rollup URL** checkbox, or you can manually edit the field by clearing the checkbox and entering the URL you want.

Patch and Compliance toolbar help

About the Purge patch and compliance definitions dialog

Use this dialog to completely remove definitions (and their associated detection rules) from the core database.

Requires the LANDesk Administrator right
A user must have the LANDesk Administrator right in order to perform this task.

You may want to remove definitions if they have become obsolete, are not working properly, or if the related security risk has been totally resolved.

This dialog contains the following options:

- **Platforms:** Specifies the platforms whose definitions you want to remove from the database. If a definition is associated with more than one platform, you must select all of its associated platforms in order for the definition and its detection rule information to be removed.
- **Languages:** Specifies the language versions of the selected platforms whose definitions you want to remove from the database. If you've selected a Windows or Macintosh platform, you should specify the languages whose definition information you want to remove. If you've selected a UNIX or Linux platform, you must specify the Language neutral option in order to remove those platform's language independent definition information.
- **Types:** Specifies the content types whose definitions you want to remove.
- **Purge:** Completely removes definition and detection rule information for the types you've selected that belong to the specified platforms and languages you've selected. This information can only be restored by downloading the content again.
- **Close:** Closes the dialog without saving changes and without removing definition information.

About the Security scan information view

Use this dialog to view detailed patch deployment activity and status for scanned devices on your network.

You can view scan results for:

- Computers not recently reporting
- Computers with no results
- Computers needing patches by selected severity type

About the Threshold settings dialog

Use this dialog to define time periods for security scan (patch deployment) results that appear in the **Security scan information** dialog.

- **Threshold for not recently scanned:** Indicates the maximum number of days to check for devices that haven't been scanned for patch deployment.

About the Security and Patch Information dialog

Use this dialog to view detailed security information for selected devices. You can view a device's scan results, detected security definitions, missing and installed patches (or software updates), and repair history.

Use the **Clear** button to remove all scan information from the database for the selected devices.

You can also right-click a vulnerability (or other security content type) in this view and directly create a repair task, or enable/disable the autofix option for applicable security content types.

Displayed information is based on the selected security content type

The group names and information fields that display on this page are dynamic, depending on the security content type you select from the **Type** drop-down list. For example, if you select vulnerabilities, the following information fields display:

- **Missing Patches (Vulnerabilities Detected):** Lists all of the vulnerabilities detected on the device by the last scan.
- **Installed Patches:** Lists all of the patches installed on the device.
- **Repair History:** Shows information about the remediation tasks attempted on the device. This information is helpful when troubleshooting devices. To clear this data, click **Purge Repair History**, specify the devices and time range settings, and then click **Purge**.
- **Vulnerability Information:**
    - **Title:** Displays the title of the selected vulnerability.
    - **Detected:** Indicates whether the selected vulnerability was detected.
    - **First detected:** Displays the date and time the vulnerability was initially detected on the device. This information can be useful if you've performed multiple scans.
    - **Reason:** Describes the reason why the selected vulnerability was detected. This information can be useful in helping you decide whether the security risk is serious enough to prompt immediate remediation.
    - **Expected:** Displays the version number of the file or registry key the vulnerability scanner is looking for. If the version number of the file or registry key found on the scanned device matches this number, the vulnerability does not exist.
    - **Found:** Displays the version number of the file or registry key found on the scanned device. If this number is different than the Expected number above, the vulnerability exists.
- **Patch Information:**
    - **Patch Required:** Displays the file name of the patch executable required to remediate the selected vulnerability.
    - **Patch Installed:** Indicates whether the patch file has been installed.
    - **Last action date:** Displays the date and time the patch was installed on the device.
    - **Action:** Indicates whether the last action was an install or an uninstall.
    - **Details:** Indicates whether the deployment/installation was successful. If an installation failed, you must clear this status information before attempting to install the patch again.
    - **Clear:** Clears the current patch installation date and status information for the selected device. Clearing this information is necessary in order to attempt to deploy and install the patch again.

Scheduled tasks help

About the Schedule task dialog

Access this dialog from the **Scheduled tasks** window (**Tools > Distribution > Scheduled tasks**). In the **Scheduled tasks** window, click the **Create software distribution task** toolbar button, or from the shortcut menu of the task you want to configure, click **Properties**.

Use this dialog to set the start time for the task and whether to make it a recurring task and how often. This dialog also shows the task targets. Depending on the task type you're scheduling, you may also see options for delivery methods and distribution packages.

About task copying

You can also create groups for your common tasks to categorize them. Other users will see groups only if their RBA scope allows them to see a task in that group. If you try deleting a group that contains tasks, you won't be able to delete the group if there are tasks in the group that your scope doesn't allow you to see.

About the Overview page

This page lets you pick an owner for the task and summarizes the choices you've made in the Scheduled tasks dialog. If you want to modify any of your choices, click **Change** beside that choice. If you want the task to appear in the **Scheduled tasks** window's **Common tasks** group, rather than the **My tasks** group, click **Show in common tasks**.

About the Distribution package page

Use this page to select the distribution package you want to deliver. Once you select a **Package type**, the **Distribution package** list shows the packages of that type that you can distribute. The packages in the list correspond to the packages you can see under that type in the **Distribution packages** window for the current user and the public user. Click the **Distribution package** you want.

Push-based software distribution tasks can include a preliminary package and a final package. When using multiple packages, the packages are installed in order one at a time. The previous package must return a successful task status before the next package begins installing. For more information, see "Using multiple distribution packages in a task" on page 153.

About the Delivery method page

Use this page to select the delivery method to use for the package you're delivering. Once you select a **Delivery type**, the **Delivery methods** list shows the delivery methods of that type that you can use. The delivery methods in the list correspond to the delivery methods you can see in the **Delivery methods** window for the current user and the public user. Click the **Delivery method** you want.

About the Target devices page

Use this page to view target devices for the task you're configuring. You can't add targets on this page. You can add targets later by dragging and dropping them into the task in the **Scheduled tasks** window. Targeted devices can be in these categories:

- Targeted devices
- Targeted LDAP objects
- Targeted queries
- Targeted LDAP queries
- Targeted device groups

You can also check the **Wake up devices** option on this page. This option wakes up a powered-down computer for the selected task by using Wake On LAN. When the task is complete, the computer shuts itself down again. This feature only works on computers with BIOS versions that support Wake on LAN technology. Selecting this option will make tasks take longer, since the task waits for devices that just woke up to boot. Don't mark this option for pull distribution packages.

About the Schedule task page

Use this page to configure when the task runs and how retries should work:

- **Leave unscheduled:** Adds the task to the Scheduled tasks window but doesn't schedule the task. Use this option if you want to preserve a task configuration but you don't want it to run.
- **Start now:** Starts the task as soon as the dialog is closed. There can be a delay of up to a minute before the task actually starts.
- **Start later:** Starts the task at the specified time and date.
- **Date and time:** Runs a task on selected date. Type the date using MM/DD/YY format, or click the drop-down list to pick the date off a calendar.
- **Repeat every:** Schedules the task to recur periodically. Select Day, Week, or Month from the drop-down list to choose how often the task repeats. It repeats at the time set above.
- **Deploy packages in this task even if they were previously deployed:** Reinstalls packages in the task if the packages were already installed.
- **Schedule these devices:** For the first time a task runs, you should leave the default of **Schedule these devices**. For subsequent runs, choose from **All**, **Devices that did not succeed**, or **Devices that did not try to run the task**. These options are explained in more detail below.

When rescheduling a task, you can limit the devices the task runs on. You may want to do this if the task failed on a large number of devices and you don't expect the failed device state to change, for example. Limiting the task this way would help the task complete more quickly because the scheduler wouldn't keep trying devices that won't process the task. You can choose to run tasks on devices in these states:

- **Waiting or currently working:** This is the default and should be used the first time a task runs. If you're rerunning the task, this option targets devices that succeeded the previous time you ran the task.
- **All:** Select this if you want the task to run on all devices, regardless of state. Consider using this option if you have a task, especially a repeating one, that needs to run on as many devices as possible.
- **Devices that didn't succeed:** Select this if you only want the task to run on all devices that didn't complete the task the first time. This excludes devices that have a **Successful** state. The task will run on devices in all other states, including **Waiting** or **Active**. Consider using this option if you need the task to run on as many unsuccessful devices as possible, but you only need the task to complete successfully once per device.
- **Devices that didn't try to run the task:** Select this if you only want the task to run on devices that didn't complete the task and didn't fail the task. This excludes devices that were in an **Off**, **Busy**, **Failed**, or **Canceled** state. Consider using this option if there were a lot of target devices that failed the task that aren't important as targets.

About the Schedule dialog

Several Management Suite agents have features that you can schedule using the local scheduler agent that is installed on managed devices. Use this dialog to configure that schedule.

You can also use the local scheduler to schedule your own tasks to run periodically on devices. Once you create a local scheduler script or customize the schedule for a device agent, you can deploy it to devices by using the **Scheduled tasks** window.

To configure a local scheduler task, in the **Managed scripts** window (**Tools > Distribution > Managed scripts**), from the **My scripts** shortcut menu, click **New local scheduler configuration script**.

All criteria in this dialog that you configure must be met before the task will execute. For example, if you configure a schedule that repeats every day between 8 and 9 o'clock with a **Machine state** of **Desktop must be locked**, the task will only execute if it's between 8 and 9 o'clock AND the machine is locked.

These options are available in the **Schedule** dialog:

The Schedule dialog's "Events" section

The events section is dimmed unless you're configuring a local scheduler script from the **Manage scripts** tool.

- **Run when user logs in:** Check this option to run the task whenever a user logs in. When a user logs in, the local scheduler will run the task directly.
- **Run whenever the machine's IP address changes:** Check this option if you want the task to run if the device's IP address changes or is renewed through DHCP. For example, you can use this option to trigger an inventory scan when the IP address changes, keeping the IP address in the Management Suitedatabase synchronized.

The Schedule dialog's "Time" section

Use this section to configure times for the task to run. If you launched this dialog from the agent configuration tool, you can specify a random delay on the agent configuration page you came from. The random delay interval you specify is a time range during which the task may run. For example, if you have a large number of users who log in at the same time, this delay allows tasks that run on login to not all run at the same time, assuming your delay interval is long enough. The default delay is one hour.

- **Start:** Click this option to display a calendar where you can select the day you want the task to start. Once you pick a day, you can also enter a time of day. These options default to the current date and time.
- **Repeat after:** If you want the task to recur, click the list box and select **minutes**, **hours**, or **days**. Then in the first box enter the length you want for the interval you selected. For example, 10 days.
- **Time range:** If you want the task to run between certain hours, select the start and end hours. The hours are in 24-hour (military) time format.
- **Weekly between:** If you want the task to run between certain days of the week, select the start and end days.
- **Monthly between:** If you want the task to run between certain dates of the month, set the start and end dates .

The Schedule dialog's "Run filters" section

When configuring local scheduler commands, you can specify the minimum bandwidth criteria necessary for the task to execute. The bandwidth test consists of network traffic to the device you specify. When the time comes for the task to execute, each device running the local scheduler task will send a small amount of ICMP network traffic to the device you specify and evaluate the transfer performance. If the test target device isn't available, the task won't execute.

When specifying bandwidth criteria for devices that may be connecting to the core through a LANDesk Management Gateway, you should put the Management Gateway's IP address in the **to** field. This allows the bandwidth test to complete and the task can then execute.

You can select these **Minimum bandwidth** options:

- **RAS:** The task executes if the device's network connection to the target device is at least RAS or dialup speed, as detected through the networking API. Selecting this option generally means the task will always run if the device has a network connection of any sort.
- **WAN:** The task executes if the device's connection to the target device is at least WAN speed. WAN speed is defined as a non-RAS connection that's slower than the LAN threshold.
- **LAN:** The task executes when the device's connection to the target device exceeds the LAN speed setting. LAN speed is defined as anything greater than 262,144 bps by default. You can set the LAN threshold in agent configuration (**Tools > Configuration > Agent Configuration, Bandwidth detection** page). Changes won't take effect until you deploy the updated configuration to devices.

The run filters section has these options:

- **Minimum bandwidth:** If you want task execution criteria to include available bandwidth, select the minimum bandwidth you want and enter the device name or IP address that will be the target for the bandwidth test between the target and device.
- **Machine state:** If you want the task execution criteria to include a machine state, select one of these states: **Screen saver or desktop locked**, **Desktop must be locked**, **Machine must be idle**, **User must be logged in**, or **User must be logged out**. The criteria for the **Machine must be idle** state are: the OS is locked, the screen saver is active, or the user is logged out.

The Schedule dialog's other options

- **Additional random delay once all other filters pass:** If you want an additional random delay, use this option. If you select a random delay that extends beyond the time limits you configured for the task, the task may not run if the random value puts the task outside the configured time limits.
- **Delay up to:** Select additional random delay you want.
- **And at least:** If you want the task to wait at least a certain number of minutes before executing, select this option. For example, if you're scheduling an inventory scan, you could enter a five here so a computer has time to finish booting before the scan starts, improving the computer's responsiveness for the user.
- **Command:** Enter the program you want to run locally. Include the full path to the program or make sure the program is in a folder that's in the device's path. This path must be the same on all devices you deploy this script to.
- **Parameters:** Enter any command-line parameters you want passed to the program.

Software distribution help

Using the Distribution package dialog

The **Distribution package** dialog (**Tools > Distribution > Distribution package**) stores information in the database that describes the package that you want to distribute. The data contains the settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, installation options, and so on. Once created, this information is called a "distribution package."

Before using this dialog, put the package on your distribution server. You'll need to browse for the package and provide information on any package prerequisites or additional files. Once you've created a distribution package for your package, you can associate it with a delivery method (**Tools > Distribution > Delivery methods**) to deploy it to devices.

About the Package information page

Use this page to enter the package name and your package's primary file. If your package consists of a single file, add it here. If your package has multiple files, add the main file in your package, for example, the file that starts the install. You can add supporting additional files on the **Additional files** page.

To use the file browser, type a Web share or file path in the box next to the **Go** button. Clicking **Go** displays the destination in the **Primary file** box. You can continue navigating there. When browsing for the file, double-click the file you want to be the primary file. This adds the filename to the package path next to the Go button.

- **Name:** The name you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer descriptions.
- **Description to show end users on download:** The description you enter here appears in the **Distribution packages** and **Delivery methods** Windows and the Software Deployment Portal.
- **Primary file:** The main file in this package.
- **Go:** Starts browsing the path you entered next to the Go button.
- **Up:** Goes up one folder level from the current location you're browsing.

Using environment variables

Support for putting the environment variable directly into the package path isn't supported in Management Suite, though expansion will still work with previously created custom scripts. To support environment variables for the new SWD architecture, the " PreferredPackageServer" registry value should be set to the environment variable to be used. This environment variable will then be expanded to define the server from which the package should be retrieved.

About the Install/Uninstall options page

Use this page to specify the package type. You have several options depending on the package you're deploying. Not all package types have these options.

- **Install:** Specifies that you want to use an installation package to install software.
- **Uninstall:** Specifies that you want to use an installation package to remove software. When this flag is set, the script removes everything that was installed with the installation script.
- **Command line:** (Not available for SWD, Macintosh, or Linux packages). The command line you want passed to the primary file you specified. Software distribution automatically adds the basic parameters for the type of package you're distributing. For more information, see Using package command lines.

MSI install/uninstall options

MSI distribution packages have additional install/uninstall options when you select **Use Windows Installer to install and control installation (MSIexec)**.

- Display options:
    - **Quiet mode, no user interaction:** Runs the installation with no notification on the managed device (silent install).

  - **Unattended mode, progress bar only:** Displays only a progress bar during install with no cancellation or deferral options.

- Sets user interface level:
  - **No UI:** Runs a completely silent installation.
  - **Basic UI:** Displays a full size window with a progress bar and a [Cancel] button. A message box is displayed at the end of the installation. If you cancel the installation, a message box is not displayed.
  - **Reduced UI:** Displays a message box at the end of the installation.
  - **Full UI:** Displays a full size window with a progress bar and a [Cancel] button. A message box is displayed at the end of the installation.
- Restart options (Not recommended. Set reboot options on Delivery Method please):
  - **Do not restart after the installation is complete:** Does not perform a reboot even if an installation has been hard coded to require it.
  - **Prompts the user to restart if necessary:** Prompts the user to reboot if the installation file requires it.
  - **Always restart the computer after installation:** Performs a reboot after install is complete.
- **Log File Name:** Specifies the location and file name to store a Windows Installer log file based on the results of the installation after completion.
- **Logging Options:** Enables the creation of the log file after the location has been specified.
- **Enter command line or select options above and edit command line for MSI package:** (Not available for SWD packages) Displays the command line that will be passed to the primary file specified. Software distribution automatically adds the basic parameters here to change default behaviors. Command line fields can also call up values from the inventory using database macros. Specify the inventory item encapsulated in the % symbol for example:

  %Device_Name.Computer%

  This displays the device name with the underscore used instead of a space and the computer at the top of the inventory tree.

About the Additional files page

If your package consists of multiple files, you can add them on this page. To use the file browser, type a Web share or file path in the box next to the Go button. Pressing the Go button displays the destination in the **Available** files box. You can continue navigating there. Select files in the **Available files** box and click **>>** to add them to the **Additional files** list. This adds them to the package.

- **Auto detect:** This option is available for MSI packages. It parses the primary MSI file for external file references and adds those automatically.
- **Arrows:** These arrows add and remove selected files from the **Additional files** list.
- **Go button:** Starts browsing the path you entered next to the Go button.
- **Up button:** Goes up one folder level from the current location you're browsing.

Using the Dependent packages page

Dependent packages are packages that must already be on the device in order for the package you're configuring to install. If they're not on the device, dependent packages are installed automatically. MSI and SWD packages are detected automatically through the appropriate registry keys on the device. For other package types, the package detection method depends on what you select on the detection page.

If you add an existing package with a dependency as a dependant package to the package you're creating, that existing dependency will also be added to the new package.

- **Available packages:** Lists the public packages you have created using the **Distribution package** window. Only public packages can be dependent. Select the packages you want to be dependent and click **>>**.
- **Dependent packages:** Lists the packages you've selected to be dependent.
- **Arrows:** These arrows add and remove selected files from the **Additional files** list.
- **Up** and **Down** buttons: Dependent packages are applied in the order they appear in the **Dependent packages** list. Use the **Up** and **Down** buttons to change the dependent package order.

Understanding Linux software dependencies

When you click **Save** in a Linux package's **Distribution package-properties** dialog, software distribution parses the primary RPM and any dependent RPMs you selected for dependencies those RPMs require. These dependencies then appear in the **Missing libraries** dialog. Checking a dependency in this dialog tells software distribution to not prompt you about it again. You can check dependencies you know are installed on managed devices. This dialog is for your information only. If a dependency is missing on a target device and you didn't specifically include that dependency as a dependent package, the RPM probably won't install successfully.

Using the Prerequisites page

The prerequisites page allows you to specify prerequisites for package installation. You can do this through a query or through an additional file/program that runs on devices and returns an errorlevel code. A non-zero code prevents the package from installing.

Prerequisites run on devices in the target list. If a device on the target list fails a prerequisite, the package won't be installed on it. The failure details are in the distribution task's log.

Prerequisites are especially useful in organizations where one person creates packages and another person distributes them. The distributor might not be aware of package system requirements that the creator does know about. In cases like these, the package creator can create a query that includes package requirements like operating system or amount of memory.

For the additional file option, you can select a file that's in the package's additional files list. You can then specify a command line you want the file to run with.

- **Choose a query:** Select an existing query that you want to use to filter targeted devices. You can also click **Create query** to create a new query.
- **Run additional file:** If you want to run a file on devices, check this option.
- **Choose an additional file:** Enter the file you want devices to run. This file is run before any other package files.
- **Command line:** If the file you specified needs a command line, enter it here.

Using the Detection page

Use the Detection page configure how software distributions detects if a package is already deployed. The Detection page is only available for executable packages, batch file packages, and Virtualized Application packages. A match on one or more criteria prevents dependent packages from installing.

The following detection methods can be used:

- **Detect by:** Determines that the package is already installed and therefore bypass the installation if one of the following items exists the managed device.

  - File exists
  - File version
  - File size and/or checksum
  - File date
  - Registry key exists
  - Registry value exists
  - Matching registry value
- **File path:** Specifies the location and name of the item to detect.
- **Search for the file recursively:** Cascades a search through subdirectories of the directory specified in the 'File path' field.

Multiple criteria can be added by specifying the criteria and clicking the **Add** button.

The MSI and SWD packages deploy GUIDs with their installations. These are used to detect if a package is already installed. The detection option isn't available on these package types.

Using the Accounts page

Use the Accounts page to select the type of user account to use to distribute the package.

- **LocalSystem account:** The account of the device.
- **Current user's account:** The account of the current user. A user must be logged into the device, or the distribution package task will fail.

Using the Uninstall Association page

Use the Uninstall association page to associate an uninstall package to a software deployment policy package. This will automatically uninstall the software from the client when the machine or user is removed from the target list or query. **Note:** Uninstall packages are only used with policy-based deployment.

- **Type:** Select the type of package you want to use to uninstall the package. The Available distribution packages list will display only the packages of the type you specify.
- **Current:** The currently selected package.

Using the Assign return codes page

Use the **Assign return codes** page to configure distribution package status messages that appear in the console based on whether or not a distribution task was successful.

The **Assign return codes** page contains the following options:

- **Package information:** Contains a summary of properties for the distribution package.
  - **Package name:** Displays the name of the distribution package.
  - **Package type:** Displays the type of package (MSI, exe, bat, etc.).
  - **Assigned template:** Displays the return code template that has been associated with the distribution package.
- **Return code template information:** Displays the name, description, and date modified for all available templates. To associate a specific template to associate with distribution package click on the template then click the **Assign** button.
- **Modify:** Modifies the template and launches the Package return code mappings window.
- **Assign:** Associates the currently selected template with the distribution package.

Using the Return code template manager

Use the **Return code template manager** to add, modify, delete, import, and export return code templates. You can display this dialog box from the Distribution packages tool by clicking the **Return code template manager** toolbar button. The **Return code template manager** dialog box contains the following options:

- **Return code template information:** Lists all existing templates by name, description, type and date modified.
- **Template filter type:** Filters the list of templates to display All, MSI or Other.
- **Template name:** Displays the name to be assigned to the new template.
- **Template description:** Displays the description to assigned to the new template.
- **Template filter type**: Displays the group to assign the new template to for filtering options. Choose from: MSI or Other.
- **Add:** Opens the New Return Code Mapping Template window. The following Information must be entered to create a new template.
- **Modify:** Opens the Package Return code Mappings window to enable a user to modify the selected template.
- **Delete:** Removes the selected template.
- **Import:** Allows for importing of a template from a designated location (.xml format).
- **Export:** Allows for export of a template to a designated location (.xml format).

Using the Package return code mappings dialog box

The Package return code mapping window contains the following options:

- **Return code template information:** Lists general properties of the template.
  - **Template name:** Displays the name of the template that was assigned in the Return code template manager.
  - **Template description:** Displays the description of the template that was assigned in the Return code template manager.
- **Default behavior:**
  - **State:** Assigns a success or failure state.
  - **Message:** Enters a custom message that will display should a package send back the selected return code.
- **Return code mappings:** Assigns new or removes existing return codes by using the [Add] or [Delete] buttons (right hand side). Return codes added in the manner will be created in numerical order.
- **Edit return code mapping:** Enters the number(s) for the return codes to be created. Click the [Apply] button after making additions and modifications in this section.
  - **Single:** Allows for the assignment of a single return code number that can then be assigned to a state and custom message.
  - **Range:** Allows for the assignment of a range of return code numbers that can then be assigned the same state and custom message.
- **Message:** Displays the custom message when the package sends back the return code.
- **State:** Sets the return code to indicate success or failure.

Using the SWD package options page

Use this page to set what happens when an SWD package is already installed on a device. If you have applications that aren't responding to a normal package heal, the full reinstall option might work better. Healing tends to take less time than a full reinstall.

When you create an SWD package, you can create it with or without a package installation interface that users see. If the package has an interface, you can choose whether the package installation status dialog appears on top of their existing applications or whether there should be a solid blue installation background that masks the desktop while the package is installing.

- **Heal (repair) the package:** This option only updates registry keys and replaces program files that the agent detects as different than those in the installation package.
- **Perform a full reinstall of the package:** This option completely reinstalls the package, replacing all files and recreating all registry keys.
- **When feedback is enabled, override the above setting and let the user decide:** Allows users to choose between heal or reinstall. You can enable feedback in the **Delivery method properties** dialog's **Feedback** page.
- **When feedback is enabled, display the background screen:** Displays the solid blue background screen. You can enable feedback in the **Delivery method properties** dialog's **Feedback** page.

Using the Delivery methods dialog

The **Delivery methods** dialog (**Tools > Distribution > Delivery methods**) defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Options include Targeted Multicast and push or policy-based distributions. Don't create a delivery method every time you want to distribute a package. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.

Before using this dialog, create the distribution package (**Tools > Distribution > Distribution packages**) that you want to deliver.

About the Description page

Use this page to describe the delivery method you're creating and to set the number of devices you want to distribute to simultaneously.

- **Name:** The name for your delivery method.
- **Owner:** The name of the person who originally created the package. You can't change this field.
- **Description of delivery method:** The description you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer descriptions.
- **Number of computers for distribution:** Controls the maximum number of devices that can simultaneously receive the software distribution.

About the Network usage page

Use this page to control how the package and package files are sent to managed devices. You have these options:

- **Use multicast to deploy files:** Uses targeted multicast to send files to multiple devices simultaneously.
- **Use run from source to deploy files:** Doesn't copy files locally before installing them. Instead, the primary package file is executed directly from the package download location. This option works with all package types on UNC package shares. For HTTP shares, this option only works with SWD and MSI package types. You can use this option with application installs that require a specific folder structure. This option will use preferred servers, but it won't try running the package from a peer.
- **Use download from source to deploy files:** Each device downloads package files from the package server before using them. This option doesn't take advantage of Targeted Multicast.

About the Bandwidth page (under the Network usage page)

Use this page to control the network bandwidth that the package requires for deployment. You don't have to select any of these options if you want all selected devices to receive the package regardless of their bandwidth.

Bandwidth control is important for devices that have a slow WAN or a dialup connection. You usually won't want to deploy a multi-megabyte package to devices on slow links. Choose from the following options:

- **Require a non-RAS network connection:** This option enables the bandwidth requirement. Select one of the following:
    - **Allow any non-RAS network connection:** This option enables WAN and LAN devices to receive the package.
    - **Only allow a high-speed network connection:** This option enables only LAN devices to receive the package.
- **Limit remote downloads (per subnet) to one device at a time:** Use this to reduce the network bandwidth consumed on a subnet.
    - **Maximum percentage of bandwidth to use:** When you've selected limit remote downloads, you can further limit bandwidth by adjusting the maximum percentage of the target device's network bandwidth to use for the distribution.

If you're using PDS to detect network connection speed, high-speed and low-speed connections return the same information. For accurate detection of high-speed network connections, you need to use ICMP.

ICMP sends ICMP echo requests of varying sizes to the remote computer and uses the round trip time of these echo requests/responses to determine the approximate bandwidth. However, not all routers or computers support forwarding or responding to ICMP echo requests. ICMP also distinguishes between LAN (high speed) and WAN (slow, but not dialup) connections.

If your network isn't configured to allow ICMP echo requests, you can select PDS. If you're using PDS, the **Only allow a high-speed network connection** option won't give you accurate control.

About the Bandwidth usage page (under the Network usage page)

Use this page to configure bandwidth throttling and packet delays.

- **Peer download (only install from cache or peer):** Only allow packages to download if they are in the local cache or on a peer in the same multicast domain. This option conserves network bandwidth, but for the package installation to be successful, the package must be in one of these two places.
- **Bandwidth used from core or preferred server (WAN):** Adjusts the priority of this specific task over other network traffic. The higher the percentage slider is set, the greater the amount of bandwidth being used by this task over any other traffic. WAN connections are usually slower, so it is most often recommended to set this slider at a lower percentage.
- **Bandwidth used peer-to-peer (Local):** Adjusts the priority of this specific task over other network traffic. . The higher the percentage slider is set, the greater the amount of bandwidth being used by this task over any other traffic. LAN connections are usually faster than WAN connections so it is most often recommended to set this slider at a higher percentage than that of the WAN.

About the Multicast domains page (under the Network usage page)

This page appears only when you've selected Multicast as the distribution type. Use this page to configure multicast options.

- **Use multicast domain discovery:** Use this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
- **Use multicast domain discovery and save results:** Use this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
- **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery and save the results.
- **Domain representatives wake up devices:** Use this option if you want computers that support Wake On LAN* technology to turn on so they can receive the multicast. You can use the Multicast Options dialog to configure how long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds.
- **Number of seconds to wait for Wake On LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

About domain discovery

Domain discovery is only necessary on networks with subnets that can see each other's multicast traffic. If your subnets don't see each other's traffic, you can save time by first saving the results of a domain discovery and then selecting **Use results of last multicast domain discovery** so Targeted Multicast doesn't do a domain discovery before each job.

If your network subnets do see each other's multicast traffic, you can help Targeted Multicast work faster by pre-discovering your domains with the multicast_domain_discovery.ini script included in the ManagementSuite\Scripts folder. This script doesn't do anything on target devices. Run this script from the **Scheduled tasks** window against a target list that spans your network. This will save the domain discovery results for future use. You may want to run this script periodically before large sets of multicast distributions.

If you selected **Use cached file** in **Configure > Services > Multicast**, Targeted Multicast will go through a discovery process even if you selected **Use results of last multicast domain discovery**. Targeted Multicast needs to do this to find out which potential multicast domain representatives have the file in their cache.

About the Multicast limits page (under the Network usage page)

Use this page to configure job-specific Targeted Multicast parameters. The defaults in this dialog should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time. The default is 5.
- **Maximum number of devices that failed multicast to process simultaneously:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the scheduled task handler would process no more than 20 computers at a time that failed the multicast. The scheduled task handler will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the scheduled task handler won't perform the distribution portion of the task for any computer that failed multicast. The default is 240.

- **Number of days the files stay in the device's cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged. The default is 2.
- **Number of days the files stay in cache on multicast domain representatives:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged. The default is 14.

About the Reboot page

Use this page to configure whether the computer is rebooted after the software has been installed or removed. You have three options:

- **Never reboot:** Devices won't reboot after a package installation. If you select this setting and your package requires a reboot, devices may encounter errors running the application until they do reboot. If the package is an SWD package, this option overrules any settings in the package. If the package is a generic executable or an MSI package, the package setting may overrule this option.
- **Reboot only if needed:** Devices will reboot it the package requires it.
- **Always reboot:** Devices will reboot regardless of whether the package requires it or not.

About the Feedback and timing page

Use this page to help determine how much the user sees during the installation or removal of the software. You have these options:

- Package progress UI:
  - **Hide all feedback from user:** Hides the installation from the user as much as the software distribution package allows. This option is dependent upon whether or not the software distribution package was created to be silent.
  - **Display progress to user:** Enables the software installation notification message box and system tray icon animation during software installation. It also enables the following options:
- **Run the package immediately:** Installs the package immediately without allowing any deferral options.
- **Allow the user to delay running the package:** Enables deferral options so users can delay package installations. This can help users who are in the middle of a task that a package installation might interfere with.
  - **Delay until next login automatically:** When checked, package installation is delayed until the next login without prompting users. After the next login, users will see the deferral dialog if you check **User selects how long to delay**.
  - **Prompt user before downloading package:** Notifies the user before a managed device initiates download of the package. This option is particularly useful for mobile users if used with deferral options to prevent a user from being forced to download a large application over a slow connection.
  - **Prompt user before running package:** Prompt user before running package: Displays a message prior to starting installation after the package is downloaded to the local distribution cache.
- **Allow user to cancel:** This option enables the user to cancel the action: either an installation or removal. Generally, for application policies, this isn't recommended.
- **Display full package interface:** This option controls whether the package installs silently (disabled) or if it prompts the user for feedback when necessary (enabled).
- **Show successful or failed status to end user:** When checked, displays a dialog after the package installs that shows whether the install succeeded or failed.

About the More deferral options page (under the feedback and timing page)

Use this page to configure package deferral limits and timeout options. The options on this page are enabled by clicking **User selects how long to delay** on the **Feedback and timing** page. You have these options:

- **Amount of time user can defer the package:** Select the number of hours, minutes or seconds that packages will be deferred if the user clicks **Wait** in the deferral dialog.
- **User deferral is limited:** When checked, limits the number of times users can click **Wait** when the deferral dialog appears.
  - Number of times user can delay: The delay limit.
- **Wait for user response before continuing:** When selected, the deferral dialog appears and waits for user response, regardless of the deferral time you specified. If users wait too long to respond or nobody is at the computer, the task can time out and fail.
- When user feedback is expected you will be able to choose the default action to take from a dropdown list. Click the radio button beside the dropdown list and select **Cancel**, **Run the package**, or **Delay**. You can then enter the amount of time the deferral dialog waits for a response before completing the action you selected.
  - **Amount of time before install/removal starts automatically:** The amount of time before the dropdown list's action is completed.

About the custom message page (under the feedback and timing page)

Use this page if you want to configure a custom message for the deferral dialog. This dialog only appears if you allow deferrals. The HTML page source for the deferral pages is on the core server in the LDLogon\html\ folder.

- **Use customized HTML pages:** Uses the HTML pages in the core server's LDLogon\html\ folder.
- **Include a custom message on the deferral dialog:** Adds text you enter (including HTML formatting) to the deferral dialog, replacing the standard text that normally gets inserted. The dialog can still show the **Wait**, **Cancel**, and **Install now** buttons with text describing what clicking each button does.

About the Deployment timing page

Use this page to control when the package is deployed after arriving at the device. You don't have to select any of these options if you want the package to be deployed as soon as you have scheduled it.

If you want your devices to have some control, you have these options:

- **Delay installation/removal until next login:** This option delays the deployment until the next time any user logs in to the computer.
- **Allow end user to delay installation/removal:** This option enables the user to delay the task. You can customize this option by configuring the following:
- **Use custom message:** If you enable this option, you can specify a custom delay message.
- **Amount of time before install/uninstall starts automatically:** This option enables you to specify how long to wait for the user to enter a delay time. The default is to wait for 60 seconds. If the user fails to interact with the request for a delay time within this specified time, the deployment begins.

About the Type and frequency of policy page

This page appears for policy-based delivery types and affects how target devices act when they receive the policy:

- **Required:** The policy-based delivery agent automatically applies required policies without user intervention. You can configure required policies to run silently. Any UI that appears on the device while a required task is installing should be non-blocking; in other words, the application being installed shouldn't require user input.
- **Recommended:** Users have the choice of when to install recommended policies. Recommended policies are selected by default on the device UI.
- **Optional:** Users have the choice of when to install optional policies. Optional policies aren't selected by default on the device UI.

You can also configure how frequently a policy can run:

- **Run once:** Once a policy successfully runs on a device, the device won't run that policy again.
- **As desired:** Can be installed by users at any time.
- **Periodic:** When a recommended or optional policy is specified as being periodic, it will be removed from the UI when it's successfully processed and will be shown again in the UI after the specified interval has elapsed.

About the downgrade page

Use this page to configure the distribution behavior when either the target operating system or the target device agents don't support the delivery methods you've chosen. For example, if you have older Management Suite agents on devices, they may not support multicast or peer download.

OS downgrade options:

- **Downgrade functionality to level of operating system:** Allows jobs to continue, though all of the delivery method options you selected may not be active.
- **Fail if operating system cannot handle default functionality:** Job fails if the operating system doesn't support the delivery method options you selected.

Device downgrade options:

- **Downgrade functionality to level of agent:** Allows job to continue though all of the delivery method options you selected may not be active.
- **Fail if agent cannot handle default functionality:** Job fails if the agents don't support the delivery method options you selected.

About the discovery page

This page allows you to choose options for device discovery. Before the scheduled task handler can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

Discovery options:

- **UDP:** Selecting UDP uses a Ping Discovery Service (PDS) ping via UDP. Most Management Suite device components depend on PDS, so your managed devices should have PDS on them. PDS is part of the standard LANDesk agent. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping retries and timeout.
- **TCP:** Selecting TCP uses an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.

- **Number of retries:** How many discovery attempts to do.
- **Discovery timeout:** How long to wait for a response with each discovery attempt.
- **Timeout for subnet broadcasts:** How long to wait for a response to subnet broadcasts.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast. When selected, this will result in a subnet directed broadcast being sent via UDP using PDS.
- **DNS/WINS:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

About the Multicast software distribution status window

This window appears on the core when there's an active Targeted Multicast distribution happening. This window shows the following information:

- **Package URL or UNC address:** This is the location of the package you're currently attempting to distribute. This line will be updated with the current file that is being transferred.
- **Status:** A real-time report on how the distribution is proceeding or, if the distribution is complete, how well the job completed.
- **Multicast domains:** The field on top shows all of the subnets and the multicast domain representatives that are being used in the distribution. When you highlight each domain representative, the lower window displays all of the computers that are receiving their distribution from that domain representative.
  Each computer in the lower window contains information on how the distribution completed on that computer. There are several information fields on the far right of each computer listed, including Packets Missed, Resend Requests, and Slowdown Requests. These fields do not contain any information until after the distribution is complete.
- **Packets missed:** Shows the number of packets that the device wasn't able to obtain from the subnet representative. If this number wasn't 0, then the distribution failed.
- **Resend requests:** Shows the number of times the device had to request that packets be resent from the subnet representative. This is a good way to gauge, for example, how busy the device was when dealing with other processes during the distribution.
- **Slowdown requests:** Shows the number of times the device had to ask the subnet representative to slow the packet stream. In this case, high numbers usually indicate that a computer is having some hardware problem that is slowing the distribution. If you have a large number of computers that have a high number of slowdown requests, you should check the Delay/Packet number on the subnet representative. There's often a correlation between the Delay/Packet number and the number of slowdown requests.

This window closes automatically after 10 seconds. If you'd like the window to remain open during the entire distribution, click **Keep dialog open** and the window will stay open until you close it manually. Keeping the dialog open will stop script execution, so make sure you close the dialog when you're done.

Creating custom scripts

If you want to create a custom script from a generic template, you can use the **Create custom script** option.

To create a custom script

1. Click **Tools > Distribution > Manage scripts**.
2. In the **All other scripts** shortcut menu, click **Create custom script**.
3. Enter a **Custom script name**. Click **OK**.

4. Your default text editor opens with a document named after the Custom script name you entered. Enter the script you want and save the document in the default path (LDMAIN\scripts).

Creating file deployment scripts

If you just want to copy files to devices, you can use a file deployment script. You can transfer any type of file, including text files, to a directory you specify on the device. File deployment scripts support Targeted Multicast.

To distribute files

1. Click **Tools > Distribution > Manage scripts**.
2. In the **All other scripts** shortcut menu, click **Create file deployment script**.
3. Enter a **Script name** and **Destination directory**. Click **Next**.
4. Enter the Multicast Domain Options you want. Click Next.
5. Select the files you want to deploy by selecting a **Web path** or a **File share path**, entering the path, and adding the files you want to the list box. Click **Next**.
6. Read the **Finished** page summary and click **Finish**.

The following sections describe the pages and options in the **Create file deployment script** wizard.

About the Download options page

Use this page to configure bandwidth throttling and packet delays.

- **Peer download (only install from cache or peer):** Only allow packages to download if they are in the local cache or on a peer in the same multicast domain. This option conserves network bandwidth, but for the package installation to be successful, the package must be in one of these two places. One way of using this option is to first copy the package to a device on each subnet with the **Only cache the file(s) on the computer using multicast** option earlier in the wizard.
- **Dynamic bandwidth throttling:** Specifies that the network traffic a device creates has priority over distribution traffic. If you select this option and leave the **Minimum available bandwidth percentage** at 0, once the device initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops. This option forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted. If you're reinstalling or repairing an ESWD package or an MSI package, you may not want to use the **Dynamic bandwidth throttling** option because these package types normally only download the files they need.
- **Minimum available bandwidth percentage to use on client:** Specifies how much dynamic bandwidth throttling to apply. You can enter values of up to 50 percent of the total network bandwidth available to the device. For example, if there were one other application consuming network bandwidth on the device during a distribution and you set the bandwidth percentage to 50 percent, the distribution job would take 50 percent and the device application would take 50 percent. In practice, this percentage is variable because the operating system automatically allocates much of the network bandwidth depending on the number of applications needing bandwidth and their priority.
- **Delay between packets (peer):** This option specifies the delay between packets for peers on the same subnet. You can use this delay to force distributions to be faster or slower. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.

- **Delay between packets (source):** Specifies the delay between the package source and device destination. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.

About the Job options page

Use this page to configure how this distribution will be deployed. If you're distributing an MSI file or generic executable, you have the option to enter any command-line options that need to be passed to the file after the multicast.

- **Script uses default distribution limit:** You can limit the number of computers Targeted Multicast distributes to simultaneously. This option uses the default value you set in the **Configure > Services** dialog's **Custom Jobs** tab under **Distribute to X computers simultaneously**.
- **Script uses custom distribution limit:** Use this option to override the default for the current job by specifying a different value.
- **Only install from cache or peer:** This option prevents target computers from going beyond their subnet to install a package. Computers will first look in their multicast cache directory and if the package isn't there, they'll check with peers on their subnet for the package. If no peers have the package, the distribution fails. This option minimizes network traffic across subnets. You can use this option after you've copied a package to each subnet with the Create Scripts page's **Only cache the file(s) on the computer using multicast** option.
- **Verify file before client install:** Generates a hash (CRC) for the package you're distributing once you finish the wizard. Devices can then use this hash value to make sure the package/file they receive isn't corrupt. Depending on the size of the package/file you're distributing, you may have to wait several minutes for the hash calculation.
- **Do not attempt task completion:** Use this option to not use the task completion feature to retry failed jobs. Normally, when task completion is installed on devices, failed jobs will be retried the next time task completion runs. Failed jobs will still be logged if you use this option.

About the Multicast domain options page

This page appears only when you've selected multicast as the distribution type. Use this page to configure multicast options.

- **Use multicast domain discovery:** Use this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
- **Use multicast domain discovery and save results:** Use this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
- **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery and save the results.
- **Domain representatives wake up computers:** Use this option if you want computers that support Wake On LAN* technology to turn on so they can receive the multicast. You can use the **Multicast options** dialog to configure how long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds.
- **Advanced multicast options:** Use this option to set advanced options. The defaults are fine for most jobs.

About domain discovery

Domain discovery is only necessary on networks with subnets that can see each other's multicast traffic. If your subnets don't see each other's traffic, you can save time by first saving the results of a domain discovery and then selecting **Use results of last multicast domain discovery** so Targeted Multicast doesn't do a domain discovery before each job.

If your network subnets do see each other's multicast traffic, you can help Targeted Multicast work faster by pre-discovering your domains with the multicast_domain_discovery.ini script included in the LDMAIN\Scripts folder. This script doesn't do anything on target computers. Run this script from the **Scheduled tasks** window against a target list that spans your network. This will save the domain discovery results for future use. You may want to run this script periodically before large sets of multicast distributions.

If you selected **Use cached file** in **Configure > Management Suite Services > Multicast**, Targeted Multicast will go through a discovery process even if you selected **Use results of last multicast domain discovery**. Targeted Multicast needs to do this to find out which potential multicast domain representatives have the file in their cache.

About the Multicast options dialog

The file deployment script wizard has a **Multicast options** dialog where you can configure job-specific Targeted Multicast parameters. The defaults in this dialog should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time.
- **Limit processing of machines that failed multicast...:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the **Custom job** dialog would process no more than 20 computers at a time that failed the multicast. The **Custom job** dialog will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the **Custom job** dialog won't perform the distribution portion of the task for any computer that failed multicast.
- **Number of days the files stay in the client cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged.
- **Number of days the files stay in multicast domain representative cache:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions (WAN or Local):** Minimum amount of time to wait between sending out multicast packets. This value is only used when the representative isn't multicasting a file from its own cache. If this parameter isn't specified, then the default minimum sleep time stored on the subnet/domain representative computer will be used. You can use this parameter to limit bandwidth usage across the WAN.
- **Maximum number of milliseconds between packet transmissions (WAN or Local):** Maximum amount of time to wait between sending out multicast packets. For more information, see Minimum number of milliseconds between packet transmissions above.
- **Number of seconds to wait after Wake On LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120

seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

About the Select files to deploy page

The **Select files to deploy** page appears in the file transfer script wizard.

- **Web path:** Click for packages stored on a Web server. You must include http:// in the URL.
- **File share path:** Click for packages stored on a null-session share on a file server. This path must follow the UNC path convention, \\servername\sharename\.
- **Browse:** Click **Browse** to browse for the path. If you clicked **Web path**, a small browser window opens. If you clicked **File share path**, a standard browse dialog opens. If you want to browse a Web server directory in the Select Package Location browser window, you must include a trailing slash on your URL (/), otherwise the browser window displays an error.
- **Add:** Click **Add** to add a program directly from the path edit box once you've entered the full path and filename.
- **Remove:** Select a file you've added and click **Remove** to remove a file from the list.

About the Finished page

This page summarizes the actions you've selected for deploying the package. Before continuing, make sure your managed devices meet all the requirements listed in the warning section.

If you click **Set as Default**, the configuration options you've selected will be set as the default values for this wizard.

Click **Finish** and you can schedule the script for distribution.

Software license monitoring help

About the Product details dialog

The Product details dialog displays information about products that are designated for monitoring. This information may come from the database provided with this product, or may have been added as a custom definition. The following fields are included in this dialog:

- **Name**: The product name. Similar products may have the same name with a number in brackets to distinguish different versions.
- **Manufacturer**: The company that produced the product. Click the arrow to view the list of normalized manufacturer names from the database.
- **Product type**: The type of license associated with the product.
  - **Single**: The product is licensed uniquely by one name and one version number.
  - **Dynamic**: More than one version of the product can be used with the same license. The list below this field shows the product names and version numbers that can be run with the same license. In the version field, use a wildcard character (*) to indicate which version numbers use the same license. For example, type **9.*** for a license that includes versions 9.0, 9.01, 9.2, and 9.5.
  - **Suite**: The product license includes rights to run multiple individual products sold as a suite. The list below this field shows the product names and version numbers that are included in the suite license.
- **Version**: The number used to identify the version of the product to customers.
- **Status**: The product super group with which the product is currently associated.

    - **Monitored**: The product is being monitored in software license scans.
    - **Ignored**: The product is not monitored in software license scans.
- **Tracking**: The files that are used to track the use of this product on managed devices. There may be one executable file or a combination of files that uniquely identify the product.
    - **Installation**: Files listed here define when the product is installed on the device. You can choose to require a match with any of the listed files or with all files to determine that the product is being used on the device. The files are listed by filename, with the version number (as given in the file's properties) and the file size (in bytes).
    - **Usage**: Files listed here define when the product is being used. The scanner checks for these files to be executed and reports the product as having been used. The files are listed by filename, with the version number (as given in the file's properties) and the file size (in bytes).
- **Add**: Click this button to add another file under the Tracking list. To do this, you must complete the following three fields:
    - **Filename**: The name of the file, including file extension.
    - **Version**: The complete version number of the file as given in the file properties.
    - **Size**: The size of the file, in bytes, as given in the file properties. This number is identified as "Size" in the Windows Properties dialog, not as "Size on disk."

About the Add file dialog

This dialog lets you add details about specific files to be used for software monitoring.

- **Filename**: The name of the file, including file extension.
- **Version**: The complete version number of the file as given in the file properties.
- **Size**: The size of the file, in bytes, as given in the file properties. This number is identified as "Size" in the Windows Properties dialog, not as "Size on disk."

About the Add product group dialog

The **Add product group** dialog displays a product group that you define, including all products that you want to include in the group. You can create groups to view related types of software, to help you organize in whatever way you want.

For example, you can define a group of software products that are used by a specific group of employees, such as all graphic design software used by your Marketing team. Another example is that you might define a group of software products that are all ordered through one vendor, so that when you track license usage you can see at a glance which product licenses need to be adjusted with the vendor.

When you define a group you use the following fields:

- **Name**: Type a descriptive name for the group. This name is displayed in any of the product super groups (Monitored, Ignored, and Discovered) that contain the products in your custom group. For example, if the group you create includes only products that you are monitoring, it only appears in the Monitored group. If it contains both monitored and ignored products, then it appears in both the Monitored and Ignored groups.
- **Product list**: Add or remove products from the list by clicking the plus (+) or minus (-) buttons under the list. Products are identified by name, version, and manufacturer.
- **Plus (+) button**: To add products to the list, click this button and select products from the **Select product** dialog. First, select an item from the **Manufacturer** list. Then click individual products or use Ctrl+Click or Shift+Click to select multiple products.

- **Minus (-) button**: To remove products from the list, select the products and click this button.

About the Add computer group dialog

The **Add computer group** dialog displays a computer group, which is a list of managed computers based on a LANDesk Management Suite query or device group. To define a computer group in the software license monitoring console, you must have first defined a query or device group in the Management Suite console. (Queries and device groups are defined in the network view pane in the Management Suite console.)

You can define a computer group to more easily manage licenses for a specific subset of your managed devices. For example, you can define a group that includes a division within your organization, or you can define a group of devices that all have a similar hardware profile.

When you define a group you use the following fields:

- **Name**: Type a descriptive name for the group. The name will appear under **All computer groups**, displayed in bold.
- **Source**: Select either Query or Device group depending on which one will define this group of computers.
- **Definition**: The name of the Management Suite query or device group that is the basis of this computer group.
- **Browse**: When you click this button, select the query or group by drilling down in the tree. The options here are based on the queries or groups that you have defined in the Management Suite console.

About the Add license/Edit license dialog

The Add license dialog displays information about a license that your organization has purchased. You do not need to enter information in every field, but there must be at least a name and, if you want to monitor compliance, at least a primary product specified.

When you define a license you use the following fields:

- **Name**: The name of the license, which may be the same as the product name. In the case of a suite license, the license name can be for the suite and the product name can identify a product in the suite.
- **Vendor**: The vendor from whom you purchased the license. This may be the same as the manufacturer. You can select from the list, which displays all vendors currently in the database, or you can enter a new vendor name.
- **Computer group**: If the license was purchased for a specific group of computers, you can specify the group here. This group must exist in the Computers view of the software license monitoring console, and so it must have been created in the Management Suite network view. Select **All** when the license can be used for any computer in your organization. Select **None** when the license is not specific to individual computers, such as a site license.
- **Location**: A notation that helps you identify where the licenses are being used in your organization.
- **License quantity**: The number of licenses allowed in the purchase agreement. (Depending on the type of license consumption, this can be per computer or per application.)
- **Price**: The price paid for the purchase of the license.
- **Manufacturer**: The manufacturer of the software product. You can select from the list, which displays all manufacturers currently in the database.
- **Primary product**: The main product associated with the license. You can select from the list, which displays products from the manufacturer you selected. If the license applies to multiple product versions, this should be the current product version.

- **Secondary product**: A product that is also associated with the license, such as an earlier version that can "borrow" licenses from the primary product.
- **License key**: The key provided by the manufacturer to activate the license.
- **Serial number**: The manufacturer's serial number associated with the license.
- **Purchase date**: The date the license was purchased and is valid. Click the calendar icon to select the date, or type the date in the text box (it will be formatted in your default numeric format, such as mm/dd/yyyy).
- **Expiration date**: The date the license expires. This date is important when you want to track licenses that must be renewed. Click the calendar icon to select the date, or type the date in the text box (it will be formatted in your default numeric format, such as mm/dd/yyyy).
- **Manufacturer invoice #**: The invoice number issued by the software manufacturer. This is useful for tracking the software within your purchasing process.
- **Purchase order #**: Your organization's purchase order number used to purchase the software. This is useful for tracking the software within your purchasing process.
- **Consumption**: The method used to calculate license usage.
    - **One per application**: License usage is counted one time for each instance that the application is installed on a given computer.
    - **One per computer**: License usage is counted one time for each computer that has the software installed, regardless of how many additional installations there may be on that computer.
- **Compliance type**: The type of license, in terms of the license compliance as specified by the manufacturer.
    - **Calculated**: The license usage is calculated to ensure that it is in compliance with the terms of the sale. This can include the following license types: New product, Competitive upgrade, OEM license, Product upgrade, Volume license, or Unknown.
    - **Not calculated**: License usage does not need to be calculated to be in compliance. This can include the following license types: Freeware, Public domain, Shareware, Floating license, Site license, and Enterprise agreement.
- **Supporting documents**: A notation that describes where supporting documentation is found for your license assets. This can indicate a network location or URL or any description you want to use.
- **Notes**: Type any additional notes related to the license. These notes are saved in the database.

About the License group dialog

The **License group** dialog displays a license group that you define, including all licenses that you want to include in the group. You can create groups to view related licenses and organize licenses in whatever way you want. For example, you can define a group of licenses that are owned by a division in your organization.

When you define a license group you use the following fields:

- **Name**: Type a descriptive name for the group. This name is listed under **All license groups**, displayed in bold.
- **License list**: Add or remove licenses from the list by clicking the plus (+) or minus (-) buttons under the list. Licenses are identified by name and vendor.
- **Plus (+) button**: To add licenses to the list, click this button and select products from the **Select license** dialog. You can select a license from the list, or to view only licenses from one vendor, select an item from the **Vendor** list. Use Ctrl+click or Shift+click to select multiple licenses.

- **Minus (-) button**: To remove licenses from the list, select the licenses and click this button.

Unmanaged Device Discovery help

The LANDesk Unmanaged device discovery (UDD) tool is accessed from the main LANDesk console (**Tools > Configuration > Unmanaged Device Discovery**). This tool provides a way for you to find devices on your network that haven't submitted an inventory scan to the LANDesk core database. UDD has multiple ways of finding unmanaged devices. This tool also provides Extended device discovery (XDD), which relies on a device agent that listens for network ARP and WAP broadcasts. The extended device discovery agent on a device then checks discovered devices for the LANDesk agent. If the LANDesk agent doesn't respond, extended device discovery displays the device in the **Computers** list. Extended device discovery is ideal in situations involving firewalls that prevent devices from responding to the normal ping-based UDD discovery methods.

The "Unmanaged device discovery" on page 191 chapter introduces this tool. In that chapter you'll find overview information, as well as step-by-step instructions on how to use all of the tool's features.

This chapter contains the following online help sections that describe the Unmanaged device discovery tool's dialogs. From the console interface, these help sections are accessed by clicking the **Help** button on their respective dialogs.

About the Scanner Configuration dialog

Use this dialog to customize and launch unmanaged device scans. To access this dialog, at the **Unmanaged device discovery** tool windows, click the **Scan network** toolbar button.

- **Saved configurations:** Shows the saved scanner configurations. Save a configuration by changing the settings you want, clicking **New**, naming the configuration, and with your new configuration selected, clicking **Save**.
- **More >>:** Expands the dialog to show discovery options.
- **Network scan:** Discovers devices using an ICMP ping sweep. This is the most thorough and recommended discovery method.
  - **IP OS fingerprinting:** An additional level of discovery that uses packet responses to try and determine the installed OS on a discovered device.
  - **Use SNMP:** An additional level of discovery that uses SNMP for device detection.
- **Discover devices with LANDesk CBA installed:** Discovers devices with the CBA agent running. If your devices have CBA, this is the fastest discovery method.
  - **Discover devices with LANDesk PDS2 installed:** Discovers devices using the older LANDesk PDS2 agent. You can only select this option if you select **CBA discovery** first.
- **Discover devices using NT domain:** Discovers devices in a Windows NT domain. This option uses the NT domain account information and doesn't require an IP address range, though you can specify one. Selecting this option and clicking **Configure** shows the **NT domain configuration** dialog where you can customize the NT domain discovery settings.
- **Filter by IP range** (for both NT domain and LDAP): Filters NT domain and LDAP discovery by the IP ranges specified in **Starting IP** and **Ending IP**.
- **Discover devices using LDAP:** Discovers devices in an LDAP directory. Selecting this option and clicking **Configure** shows the **LDAP configuration** dialog where you can customize the LDAP discovery settings.

- **Discover IPMI-enabled devices:** Looks for servers enabled with Intelligent Platform Management Interface, which allows you to access many features regardless of whether the server is turned on or not, or what state the OS may be in.
- **Discover Intel vPro AMT devices:** Looks for Intel Active Management Technology-enabled devices. AMT devices appear in the **Intel AMT** folder.
- **Discover virtual hosts:** Looks for servers running the VMware ESX Server.
- **Starting IP:** Enter the starting IP address for the range of addresses you want to scan.
- **Ending IP:** Enter the ending IP address for the range of addresses you want to scan. UDD automatically updates this field as you type the **Starting IP**, but you can change the ending IP address manually. **Ending IP** is calculated using the value of **Subnet mask** + what is typed in **Starting IP**.
- **Subnet mask:** Enter the subnet mask for the IP address range you're scanning.
- **Add** and **Remove:** Adds or removes your IP address ranges from the work queue at the bottom of the dialog.
- **Schedule task:** Schedules the scan based on your settings. You can customize the start time in the **Scheduled tasks** window. Scheduled scans originate from the core server.
- **Scan now:** Starts the scan immediately based on your settings. Scans started here originate from the console you're at. Once you start the scan, a **Scan status** dialog appears showing the total number of devices found, how many existing devices were updated, and how many new unmanaged devices were added.

About the NT domain configuration dialog

Use this dialog to configure how you connect to the domain you want to scan.

- **Domain:** Enter the domain you want to scan.
- **Log in as current user:** Select this if you're logged in as a user with access to the domain you're scanning.
- **Log in as:** Select this if you aren't logged in as a user with access to the domain you're scanning. Also enter a **User name** and a **Password**.
- **Use domain info:** Uses information from the domain about the detected device OS.
- **Add** and **Remove:** Add each domain you configure and want to scan to the work queue by clicking **Add**. Click **Remove** to delete the selected domain from the work queue.

About the LDAP configuration dialog

Use this dialog to configure how you connect to the LDAP directory you want to scan.

- **LDAP://:** Enter the LDAP directory you want to scan.
- **Log in as current user:** Select this if you're logged in as a user with access to the directory you're scanning.
- **Log in as:** Select this if you aren't logged on as a user with access to the directory you're scanning. Also enter a **User name** and a **Password**.
- **Select individual OUs:** Select the OUs that you want to scan. Click **Add** to add them to the work queue. Click **Remove** to delete the selected OU from the queue.
- **Active directory path:** Shows the active directory path, if applicable.

Configuring SNMP scans

Network scan discoveries can use SNMP. Depending on your network's SNMP configuration, you may need to enter additional SNMP information in UDD. Clicking **Configure** next to the **SNMP** option shows the **SNMP configuration** dialog, which has these options:

- **Retries:** How many times UDD retries the SNMP connection.

- **Wait for response in seconds:** How long UDD should wait for an SNMP response.
- **Port:** What port UDD should send SNMP queries to.
- **Community name:** The SNMP community name UDD should use.
- **Configure SNMP V3:** UDD also supports SNMP V3. Click this button to configure SNMP V3 options in the **SNMP V3 configuration** dialog.

The **SNMP V3 configuration** dialog has these options:

- **User name:** The username UDD should use to authenticate with the remote SNMP service.
- **Password:** The password for the remote SNMP service.
- **Authentication type:** The authentication type SNMP is using. Can be **MD5**, **SHA**, or **None**.
- Privacy **Type:** The encryption method the SNMP service is using. Can be **DES**, **AES128**, or **None**.
- Privacy **Password:** The password to use with the specified privacy type. Not available if you selected a privacy type of **None**.

About the ARP (or WAP) Discovery Settings list dialog

Use this dialog to manage your ARP and WAP settings that are used for extended device discovery. Once configured, you can apply XDD settings to scan tasks.

This dialog contains the following options:

- **New:** Opens the settings dialog where you can configure the discovery method options.
- **Edit:** Opens the settings dialog where you can modify the selected setting.
- **Copy:** Opens a copy of the selected setting as a template, which you can then modify and rename. This is useful if you want to make minor adjustments to settings and save them for a specific purpose.
- **Delete:** Removes the selected setting from the database.

  Note the selected setting may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that setting still have it and continue to use it until a new agent configuration task is deployed; scheduled tasks with that setting still run on target devices, as do local scheduler tasks with that setting, until a new configuration is deployed.

- **Close:** Closes the dialog, without applying a setting to the task.

About the Configure ARP Discovery Settings dialog

Use this dialog (**Configure extended device discovery** toolbar button > **Configure ARP discovery settings**) to customize ARP-based extended device discovery scan settings.

- **Configuration name:** Identifies the setting with a unique name. This name appears in the settings drop-down list on the settings list dialog.
- **Duration ARP entry stats cached (in seconds):** How long devices with the extended device discovery agent keep an address in the ARP table. Devices in the ARP cache won't be pinged after the initial discovery ping. The default is 24 hours (86,400 seconds). The minimum value is 900 seconds.
- **Maximum delay before pinging an unknown device for the LANDesk agent (in seconds):** When a new ARP is recognized by a device with the extended device discovery agent, the device waits two minutes for the detected device to boot and then waits a random amount of time within the value you specify here. The agent with the shortest random wait will ping first and then UDP broadcast to the subnet that it took care of the ping for that device. If you have multiple extended device discovery agents

installed, this prevents devices from generating excess traffic by all pinging at the same time. If you set this too high, unmanaged devices may leave the network before they can be pinged. If you set this too low, multiple agents may ping and report the same device. The default is one hour (3,600 seconds).

- **Frequency the cached ARP table is refreshed (in seconds):** How often the device writes the ARP cache to disk so the data isn't lost in case the device shuts off, crashes, or reboots. The default value is five minutes (300 seconds).
- **Logging level:** The local extended device discovery logging level for errors (1), warnings (2), everything (3). The default level is 1- errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xddclient.log.
- **Force logging level:** Overrides the log level setting from the core server. If you clear this option, you can set the log level manually on a particular device. This can be useful for troubleshooting a particular device without having to change the log level on all devices. This is enabled by default.

About the Configure WAP Discovery Settings dialog

Use this dialog (**Configure extended device discovery** toolbar button > **Configure WAP discovery settings**) to configure WAP-based extended device discovery scan settings.

This dialog contains the following options:

- **Configuration name:** Identifies the setting with a unique name. This name appears in the settings drop-down list on the settings list dialog.
- **Frequency of WAP scan (in seconds):** Specifies how often the extended device discovery agent scans for WAP points.
- **Logging level:** The local extended device discovery logging level for errors (1), warnings (2), everything (3). The default level is 1- errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xddclient.log.
- **Force logging level:**Overrides the log level setting from the core server. If you clear this option, you can set the log level manually on a particular device. This can be useful for troubleshooting a particular device without having to change the log level on all devices. This is enabled by default.

About the ARP discovery history dialog

Use this dialog (**Configure ARP discovery history** toolbar button) to configure how the core server maintains the ARP discovery history. This history data is used for generating extended device discovery reports. The options in this dialog don't affect the discovered devices you see in the main unmanaged device discovery window. This history only applies to devices that were discovered through ARP discovery and that don't have LANDesk agents on them.

- **Maintain history for this period of days:** Clicking this option allows you to specify how many days of ARP discovery history data you want to save in the database. ARP discovery history data older than the number of days you specify will be deleted from the database during maintenance.
- **Clear entries manually:** This is the default. The ARP discovery history won't be deleted during maintenance.
- **Clear all entries now:** Click this button to immediately delete the ARP discovery history from the database.