Copyright Notice

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2003-2017, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Last updated: 7/24/2017
Contents

Welcome to the documentation for Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk version 2017.1 ................................................................. 9
Ivanti Endpoint Manager, powered by Landesk is the new name for Landesk Management Suite.Ivanti Endpoint Security for Endpoint Manager is the new name for Landesk Security Suite. ................................................................. 9
Where to go for more information ........................................................................ 9

What’s new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk
2017.1 .................................................................................................................. 10
What’s new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk
2016.3 SU3 .......................................................................................................... 11
What’s new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk
2016.3 .................................................................................................................. 12
What’s new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk
2016.1 .................................................................................................................. 13

Console ............................................................................................................ 14
Console overview ............................................................................................ 14
Understand the Network View ......................................................................... 18
View managed devices ...................................................................................... 29
Access console tools ......................................................................................... 36
Viewing data using the inspector ..................................................................... 44

User management ............................................................................................ 52
Role-based administration overview .............................................................. 52
Managing authentications ................................................................................. 56
Managing roles .................................................................................................. 58
Creating scopes ............................................................................................... 69
Create a team .................................................................................................... 72
Using remote control time restrictions ............................................................ 73

Core configuration .......................................................................................... 75
Running Ivanti® Endpoint Manager powered by Landesk setup .................... 75
Set up additional Endpoint Manager consoles ............................................. 76
Set up the Web console .................................................................................... 77
Activating the core server .............................................................................. 79
About the Core Server Activation utility ......................................................... 81
Manually activating a core or verifying the node count data ......................... 83
Configuring COM+ server credentials ............................................................ 83
Credential manager ........................................................................................ 84
Configuring the Workspaces database after core setup ................................. 85
Ivanti® Endpoint Manager powered by Landesk 2017 server certificate configuration ................................................. 87
Supported platforms and functionality ............................................................ 88
Endpoint Manager port usage ......................................................................... 89
Configuring services ....................................................................................... 89
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Center</td>
<td>99</td>
</tr>
<tr>
<td><strong>Core synchronization</strong></td>
<td>105</td>
</tr>
<tr>
<td>Core synchronization</td>
<td>105</td>
</tr>
<tr>
<td>Add servers to the core synchronization list</td>
<td>106</td>
</tr>
<tr>
<td>Synchronize items on demand</td>
<td>107</td>
</tr>
<tr>
<td>Automatically synchronizing items</td>
<td>108</td>
</tr>
<tr>
<td>Exporting and importing core sync items</td>
<td>109</td>
</tr>
<tr>
<td>Monitoring core synchronization status</td>
<td>110</td>
</tr>
<tr>
<td>Core sync conflict management</td>
<td>110</td>
</tr>
<tr>
<td>Change auto synchronization settings</td>
<td>111</td>
</tr>
<tr>
<td><strong>Agent configuration</strong></td>
<td>112</td>
</tr>
<tr>
<td>Configuring device agents</td>
<td>112</td>
</tr>
<tr>
<td>Agent security and trusted certificates</td>
<td>140</td>
</tr>
<tr>
<td><strong>Agent settings</strong></td>
<td>149</td>
</tr>
<tr>
<td>Agent Settings overview</td>
<td>149</td>
</tr>
<tr>
<td>Create change settings tasks</td>
<td>150</td>
</tr>
<tr>
<td>Create a task to install or update security components</td>
<td>151</td>
</tr>
<tr>
<td>Create a task to remove security components</td>
<td>154</td>
</tr>
<tr>
<td>Configure Windows Firewall settings</td>
<td>156</td>
</tr>
<tr>
<td>Generate security authorization codes</td>
<td>158</td>
</tr>
<tr>
<td>Adaptive settings</td>
<td>159</td>
</tr>
<tr>
<td>Available agent settings</td>
<td>165</td>
</tr>
<tr>
<td>Agent settings: Adaptive settings</td>
<td>187</td>
</tr>
<tr>
<td><strong>Agent Watcher</strong></td>
<td>319</td>
</tr>
<tr>
<td>Agent Watcher overview</td>
<td>319</td>
</tr>
<tr>
<td>Monitor services and files with Agent Watcher</td>
<td>319</td>
</tr>
<tr>
<td>Enable and configure Agent Watcher</td>
<td>320</td>
</tr>
<tr>
<td>Agent Watcher help</td>
<td>323</td>
</tr>
<tr>
<td><strong>Inventory</strong></td>
<td>326</td>
</tr>
<tr>
<td>Inventory scanning overview</td>
<td>326</td>
</tr>
<tr>
<td>Adding software and data items to inventory scans</td>
<td>347</td>
</tr>
<tr>
<td>Using custom data forms</td>
<td>362</td>
</tr>
<tr>
<td><strong>Queries/Directory manager</strong></td>
<td>369</td>
</tr>
<tr>
<td>Database queries</td>
<td>369</td>
</tr>
<tr>
<td>Query groups</td>
<td>369</td>
</tr>
<tr>
<td>Create a database query</td>
<td>369</td>
</tr>
<tr>
<td>Run a database query</td>
<td>370</td>
</tr>
<tr>
<td>Import and export queries</td>
<td>370</td>
</tr>
<tr>
<td>LDAP queries</td>
<td>370</td>
</tr>
<tr>
<td>Configure LDAP directories</td>
<td>371</td>
</tr>
<tr>
<td>Create an LDAP directory query</td>
<td>372</td>
</tr>
<tr>
<td><strong>Auditing</strong></td>
<td>373</td>
</tr>
<tr>
<td>Welcome to auditing</td>
<td>373</td>
</tr>
<tr>
<td>Configuring auditing</td>
<td>373</td>
</tr>
<tr>
<td>Sending auditing events to the Windows Event Viewer</td>
<td>376</td>
</tr>
</tbody>
</table>
### Viewing auditing events

Creating filters for auditing event queries

Archiving and restoring auditing data

**Reports**

- Using reports .................................................. 381
- Running reports .................................................. 400
- Running ad hoc reports ........................................ 409
- Organizing reports .............................................. 411

**Scheduling tasks** .............................................. 415

- Scheduling tasks .................................................. 415
- Assigning targets to a task .................................... 422
- Monitoring task status .......................................... 444

**Local scheduler** .............................................. 429

- About the local scheduler ...................................... 429
- Installing the local scheduler service on an unmanaged device .................................................. 429
- Adding a task with LocalSch.exe ............................... 430
- Create a local scheduler command ............................ 431
- Deleting a task with LocalSch.exe ............................. 433
- LocalSch.exe command-line parameters ...................... 433
- Local scheduler character parsing and the command line .......................................................... 434

**Remote control** .............................................. 436

- Using the remote control viewer ................................ 436
- Connect to Remote devices ...................................... 437
- Using the drawing tools on remote devices .................. 438
- Adjusting remote control settings ............................ 438
- Use alternate names .............................................. 439
- Using the mirror driver .......................................... 439
- Changing viewer hot key settings ............................. 440
- Optimizing remote control performance ...................... 440
- Interact with remote control device users .................. 441
- Changing device remote control security .................... 443
- Using remote control logging ................................. 443
- Customizing the viewer and remote control agents .......... 445
- Troubleshooting remote control sessions .................... 446

**HTML remote control** ....................................... 448

- HTML remote control ........................................... 448
- Starting an HTML remote control session .................... 450
- Using the HTML remote control clipboard to transfer text and files .......................................... 452
- Controlling devices that have multiple monitors with HTML remote control .................................... 453
- Configuring HTML remote control settings .................. 454

**Software distribution/Distribution packages/Delivery methods** .............................................. 457

- About software distribution ..................................... 457
- Understanding the available distribution delivery task types .......................................................... 469
- Assigning distribution return codes ............................ 477

**Portal Manager** .................................................. 482
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Portal Manager</td>
<td>482</td>
</tr>
<tr>
<td>Configuring the Portal Manager</td>
<td>483</td>
</tr>
<tr>
<td>Adding applications to the Portal Manager</td>
<td>484</td>
</tr>
<tr>
<td><strong>Application policy management</strong></td>
<td>485</td>
</tr>
<tr>
<td>About policy-based management</td>
<td>485</td>
</tr>
<tr>
<td>Configuring policies</td>
<td>486</td>
</tr>
<tr>
<td>Create a policy-based distribution</td>
<td>487</td>
</tr>
<tr>
<td>Adding policy targets</td>
<td>487</td>
</tr>
<tr>
<td>Understanding how scopes affect policy target visibility</td>
<td>488</td>
</tr>
<tr>
<td><strong>Software license monitoring</strong></td>
<td>489</td>
</tr>
<tr>
<td>Audit and compliance data in the dashboard</td>
<td>489</td>
</tr>
<tr>
<td>Monitoring software usage</td>
<td>503</td>
</tr>
<tr>
<td>Monitoring product license compliance</td>
<td>527</td>
</tr>
<tr>
<td><strong>Unmanaged device discovery</strong></td>
<td>550</td>
</tr>
<tr>
<td>Unmanaged device discovery overview</td>
<td>550</td>
</tr>
<tr>
<td>Use extended device discovery (with ARP and WAP)</td>
<td>554</td>
</tr>
<tr>
<td>Discover unmanaged devices with UDD</td>
<td>557</td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td>563</td>
</tr>
<tr>
<td>Provisioning overview</td>
<td>563</td>
</tr>
<tr>
<td>Creating templates</td>
<td>567</td>
</tr>
<tr>
<td>Schedule a provisioning task</td>
<td>577</td>
</tr>
<tr>
<td>Provisioning template variables</td>
<td>585</td>
</tr>
<tr>
<td>PXE-based deployment</td>
<td>617</td>
</tr>
<tr>
<td><strong>Hardware independent imaging</strong></td>
<td>624</td>
</tr>
<tr>
<td>Hardware-independent imaging overview</td>
<td>624</td>
</tr>
<tr>
<td>Creating a driver repository</td>
<td>625</td>
</tr>
<tr>
<td>Disabling HII drivers</td>
<td>626</td>
</tr>
<tr>
<td>Assigning HII drivers</td>
<td>626</td>
</tr>
<tr>
<td>Using hardware-independent imaging with provisioning templates</td>
<td>627</td>
</tr>
<tr>
<td><strong>LANDESK SmartVue</strong></td>
<td>629</td>
</tr>
<tr>
<td>Welcome to Ivanti SmartVue</td>
<td>629</td>
</tr>
<tr>
<td>Scheduling SmartVue data collection</td>
<td>630</td>
</tr>
<tr>
<td>Configuring SmartVue data sources</td>
<td>631</td>
</tr>
<tr>
<td>Configuring SmartVue locations</td>
<td>631</td>
</tr>
<tr>
<td>Using the SmartVue iOS app</td>
<td>632</td>
</tr>
<tr>
<td>Using the SmartVue web application</td>
<td>633</td>
</tr>
<tr>
<td>SmartVue architecture</td>
<td>634</td>
</tr>
<tr>
<td>Modifying SmartVue widgets</td>
<td>635</td>
</tr>
<tr>
<td>Making widgets active</td>
<td>637</td>
</tr>
<tr>
<td>About the SmartVue configuration dialog box</td>
<td>638</td>
</tr>
<tr>
<td><strong>Local accounts</strong></td>
<td>640</td>
</tr>
<tr>
<td>Local accounts overview</td>
<td>640</td>
</tr>
<tr>
<td>Manage local user groups</td>
<td>640</td>
</tr>
<tr>
<td>Manage local users</td>
<td>641</td>
</tr>
<tr>
<td>Assign users to groups</td>
<td>641</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Enroll devices</td>
<td>866</td>
</tr>
<tr>
<td>Device tasks</td>
<td>875</td>
</tr>
<tr>
<td>Use Mobility Manager with an Exchange server</td>
<td>883</td>
</tr>
<tr>
<td><strong>Alerting</strong></td>
<td>888</td>
</tr>
<tr>
<td>Alerts and monitoring overview</td>
<td>888</td>
</tr>
<tr>
<td>Configuring alert rulesets</td>
<td>895</td>
</tr>
<tr>
<td>About performance monitoring</td>
<td>910</td>
</tr>
<tr>
<td>View the global alert log</td>
<td>914</td>
</tr>
<tr>
<td>Managing Dell DRAC devices</td>
<td>919</td>
</tr>
<tr>
<td><strong>Intel vPro</strong></td>
<td>932</td>
</tr>
<tr>
<td>Provisioning Intel vPro devices</td>
<td>932</td>
</tr>
<tr>
<td>Discovering vPro devices</td>
<td>945</td>
</tr>
<tr>
<td><strong>Rollup cores</strong></td>
<td>954</td>
</tr>
<tr>
<td>Installing a rollup core</td>
<td>954</td>
</tr>
<tr>
<td>Configuring SQL server replication for rollup cores</td>
<td>954</td>
</tr>
<tr>
<td>Troubleshooting rollup replication errors</td>
<td>960</td>
</tr>
<tr>
<td><strong>Preferred servers and content replication</strong></td>
<td>963</td>
</tr>
<tr>
<td>Preferred servers and content replication overview</td>
<td>963</td>
</tr>
<tr>
<td>Configure sources and mirroring</td>
<td>967</td>
</tr>
<tr>
<td>Assign a replicator</td>
<td>969</td>
</tr>
<tr>
<td><strong>Cloud Services Appliance</strong></td>
<td>977</td>
</tr>
<tr>
<td>Configuring the Ivanti Cloud Services Appliance (Management Gateway)</td>
<td>977</td>
</tr>
<tr>
<td>Using the Cloud Services Appliance activity recorder</td>
<td>980</td>
</tr>
<tr>
<td><strong>Tenant management</strong></td>
<td>982</td>
</tr>
<tr>
<td>Tenant management overview</td>
<td>982</td>
</tr>
<tr>
<td>Creating a tenant</td>
<td>982</td>
</tr>
<tr>
<td>Create a tenant</td>
<td>983</td>
</tr>
<tr>
<td>Adding tenant devices</td>
<td>984</td>
</tr>
<tr>
<td>Add tenant devices</td>
<td>984</td>
</tr>
<tr>
<td>Deleting tenants and tenant devices</td>
<td>985</td>
</tr>
<tr>
<td>Delete a tenant or tenant device</td>
<td>985</td>
</tr>
<tr>
<td>Managing devices in a tenant</td>
<td>985</td>
</tr>
<tr>
<td><strong>Web console</strong></td>
<td>987</td>
</tr>
<tr>
<td>About the Web console</td>
<td>987</td>
</tr>
<tr>
<td>Using the health dashboard [Web console]</td>
<td>1003</td>
</tr>
<tr>
<td>Using remote control [Web console]</td>
<td>1005</td>
</tr>
<tr>
<td>Software distribution overview [Web console]</td>
<td>1012</td>
</tr>
<tr>
<td>Viewing the Real-time Inventory and Monitoring console [Web console]</td>
<td>1027</td>
</tr>
<tr>
<td>Using queries [Web console]</td>
<td>1034</td>
</tr>
<tr>
<td><strong>Ivanti Inventory Manager</strong></td>
<td>1048</td>
</tr>
</tbody>
</table>
Welcome to the documentation for Ivanti®
Endpoint Manager and Endpoint Security,
powered by Landesk version 2017.1

Ivanti Endpoint Manager, powered by Landesk is the new name for Landesk Management Suite.
Ivanti Endpoint Security for Endpoint Manager is the new name for Landesk Security Suite.

Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk consists of a wide variety of powerful and easy-to-use tools you can use to help manage and protect your Windows, Macintosh, mobile, Linux, and UNIX devices. Endpoint Manager and Security tools are proven to increase end user and IT administrator productivity and efficiency.

For information on what’s new, see "What’s new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk 2017.1" (10).

For release notes, installation instructions, and important additional information, make sure you visit the Endpoint Manager and Security announcement page on the Ivanti Community:

- [https://community.ivanti.com/docs/DOC-47663](https://community.ivanti.com/docs/DOC-47663)

Where to go for more information

Navigate the help topics in the Ivanti Help Center or perform a search using a specific key word or phrase to find the information you want.

The Ivanti User Community has user forums and best known methods for all Ivanti products and technologies. To access this valuable resource, go to:

- [The Ivanti User Community Home Page](https://community.ivanti.com/docs/DOC-47663)

The User Community is also your main resource for Endpoint Manager and Security installation and deployment information, such as:

- System requirements
- Installation instructions
- Activating the core server
- Ports used
- Upgrading from previous versions
- Installing add-on products

Copyright © 2017, Ivanti. All Rights Reserved. [Terms of Use](https://community.ivanti.com/docs/DOC-47663)
What's new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk 2017.1

- **Antivirus removal from the Mac agent configuration.** When altering the Mac configuration agent, you can prevent the antivirus component from being installed on Mac devices as part of the configuration agent. Previously, you could only disable the installation of the antivirus, though it would still be included as part of the configuration agent file. By disabling antivirus from the console, this removes the entire antivirus component from the configuration agent.

- **Windows Wi-Fi payload support.** Deliver Wi-Fi credentials directly to Windows smart devices. This functionality uses the same Mobile Connectivity dialog settings for payloads to iOS, Android, and Windows devices alike.

- **Windows SCEP for iOS.** Dynamically provision certificates as devices request them. By connecting to an existing SCEP server, you effectively protect Wi-Fi payloads. When connected to a SCEP server, Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk communicates with it through the CSA. The SCEP server should make any certificate requests to a certificate authority, which publishes the certificate to an access point. The certificate is then distributed on a device-by-device basis.

- **Mac standalone remote control agent.** Allow users to access and download the agent from the CSA, which they then simply connect to the server. The agent appears on an administrator page, which allows you to initiate a remote control session. After the session is complete, the device user can simply delete the file.

- **Credential manager.** New centralized tool for managing Endpoint Manager and Security credentials.
What's new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk 2016.3 SU3

- **Windows 10 MDM support.** Enroll both desktop and mobile devices using the Windows 10 operating system with Mobility Manager. Devices enrolled in this feature are treated as mobile devices, which means you can deploy mobile app packages, sync devices, and perform wipes.

- **Identity Server.** Identity Server is a Secure Token Service that delivers OAuth2 and OpenID Connect tokens. It acts as a login authorization service that replaces the logon policy for BridgeIT. Using this service, you can utilize single sign in and federated authentication. For new installations, this feature is already activated. However, for upgraded systems, you’ll need to configure this manually from the Configuration Center.
What's new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk 2016.3

- **Apple Device Enrollment Program (DEP).** Use Apple DEP to automatically enroll and install specific applications to new devices purchased through the Apple Store. Upon arrival, these devices are already part of your inventory and usable immediately.

- **Apple Volume Purchasing Program (VPP).** Distribute and retrieve software licenses through Apple IDs enrolled in the Volume Purchasing Program. By enabling VPP with Ivanti® Endpoint Manager powered by Landesk, administrators can view available licenses associated with their corporate Apple account and specify where each license goes.

- **Managing iMacs and Macbooks as mobile devices.** Mac device management is possible through Mobility Manager with the installation of an MDM Enroller app. These devices are then handled as mobile devices, and use the same packages for deploying software and other policy settings.

- **Android for Work.** Handle bring-your-own-device (BYOD) with Android for Work, which applies specific policies to work-related apps without interfering with the device owner’s existing privileges.

- **Standard, Profile Owner, and Device Owner restrictions.** Device restrictions are handled depending on the level of control desired for a device. Standard restrictions are applied throughout a device, typically for corporate-owned devices. Profile Owner restrictions protect work-related functions for devices enrolled with Android for Work. Device Owner restrictions handle enabling and disabling global access to device features like cameras, factory resets, and uninstalling apps.
What's new in Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk 2016.1

- **Mobile Device Management (MDM) integration:** Use the management console’s MDM capabilities to create and apply policies and packages to the appropriate mobile-device platforms.

- **Security administrator workspace:** Bridge the security/IT operations gap with a workspace that’s designed to identify the state of endpoint security and take action by applying a patching process.

- **Roll-out projects tool:** Automate staged roll-out projects to progress from smaller pilot groups to widespread enterprise distributions—perfect for maintaining Windows 10.

- **Enterprise Mac & Chromebook platform management:** Endpoint Manager 10 extends Mac and Chromebook management through the enterprise and includes patching for Linux.

- **New release for Mobile Security Suite:** Apply new mobile-device security features, such as app wrapping and secure email, along-side the new MDM capabilities in Endpoint Manager.

- **Simplified provisioning and distributions:** Endpoint Manager 2017 helps simplify complex provisioning and software distributions by providing flexible templates, conditional actions, and simplified workflows.

- **Xtraction enablement:** Use Ivanti Xtraction to leverage management and security data with quick executive views. Xtraction provides IT data enabled for add-on Xtraction dashboards. These business value dashboards can be created in a brief timeframe and are ideal for executives among others to see and modify views into multiple sets of IT and business data.

- **Management console dashboards:** You’ll find 100+ workspace-like charts and graphs inside the console, which is the same visual data shared in the Ivanti workspaces. Three of the 4 dashboards are security focused—one for patch, one for a comprehensive set of security data (AV, app control, etc.), and one for a subset of security, focused on security posture.

- **Discovery for rogue devices and lost assets:** Endpoint Manager 2017 automates the subnet-representative election process to reduce administrative overhead for passive discovery on each subnet.

- **Simplified advanced endpoint security:** This version of Endpoint Manager includes a large content database of trusted files and applications to improve workflows for application control, whitelisting, and blacklisting. Application control is simplified with file-reputation security updates.
Console

Console overview

The Ivanti Administrator console lets you perform network management functions from one location. 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.

A Console toolbar, B Layout menu, C Core Server menu, D Tools, E Tool groups, F Network view, G Results list, H Find bar, I Tool panel, J Tools toolbar, K Tool tabs, L Status bar

The help topics in this section describe how to navigate and use the console to view and organize devices; and how to access the various management tools.
Getting complete up-to-date installation and configuration information

You can have multiple core servers and databases to accommodate your specific network management needs. For information on installing a Ivanti® Endpoint Manager powered by Landesk core server and console, additional consoles, web console, and managing multiple core servers and databases, refer to the documentation hosted on the Ivanti User Community.

NOTE: The Ivanti User Community
The Ivanti User Community has user forums and best known methods for all Ivanti products and technologies. To access this valuable resource, go to: User Community Home Page

Console setup wizards

Wizards are available for several areas of Ivanti® Endpoint Manager powered by Landesk. These wizards proceed through a series of instructions as the user completes the outlined steps.

Wizards appear automatically on a new installation and can be accessed at any time from the Help menu. You can follow the steps in the wizard to learn more about the specific feature or functionality. Or you can check the Don’t show this wizard again check box to prevent the wizard from being shown automatically.

Getting started wizard

The Getting Started wizard helps you configure Ivanti® Endpoint Manager powered by Landesk 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
Discovering and installing agents wizard

The Discovering and Installing Agents wizard helps the user configure Ivanti® Endpoint Manager powered by Landesk to perform the following functions:

- Discovery: Looks for devices on the network that are unknown to the Ivanti® Endpoint Manager powered by Landesk. IP address ranges can be specified to scan on the network.
- Deploying an agent: Installs the Ivanti Management agent on devices to be managed.

Security updates wizard

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

The User Management 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.

Start the console

To start the console

1. Click Start > Programs > Ivanti > Endpoint Manager. (The actual program name may be different depending on the Ivanti product that's installed and the license used to activate your core server.)
2. Enter the 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 Endpoint Manager 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 Ivanti user. This might be an administrator user or some other type of user with restricted access (see "Role-based administration overview" (52)). The user must be a member of one of the Ivanti 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 an Ivanti 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.)
- **Core server:** Specifies the core server you want to connect to. This list is the same as the core server list available on the console toolbar.
Single Sign-on into the Ivanti console

With single sign-on, a user can log onto the Ivanti console without having to enter a username and password. If the user is the logged in user, the Windows credentials will pass through and the console will not prompt the user for login information.

To enable Single Sign-on

1. On the core server, click the Ivanti Management Console icon to open the Ivanti® Endpoint Manager powered by Landesk window.
2. In the User name field, enter the domain\username.
3. In the Password field, enter the password.
4. Click Log in to open the Ivanti console.
5. In the Ivanti console, click Configure | Services to open the Configure Ivanti Software Services window.
7. Click Apply.
8. Click [OK].

Understand the Network View

The Network View is the main window of the console and is the starting point for most administrative tasks. The Network View is where you view device 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 pane (A) shows a hierarchical tree view of the core server and 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 pane (B) in the Network View displays a detailed results 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.

**NOTE: 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 overview” (52).

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.

  **NOTE: 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 "no symbol" (circle with a slash through it) indicates that you can’t add the item to that group.

- **Public devices**: Lists devices an administrator (a user with the Ivanti 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 Ivanti agent automatically appear in the All devices group when they are scanned into the core database by the inventory scanner.

- Computers
- Mobile
- MDM managed
- Agentless
- Devices with older agents
- Hardware Password Manager

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.
Users

Virtual OS Hosts

The Virtual OS Hosts group shows VMWare ESX virtual host servers. 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 Endpoint Manager administrator has added from the All virtual OS hosts group. Users with the Ivanti 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 Ivanti Agent automatically appear in the All virtual OS hosts group/folder when they are scanned into the database by the inventory scanner.

- **User virtual OS hosts**: Lists all the virtual OS hosts in the database (organized by user subgroups). User subgroups are named with user login IDs (i.e., computer name\user account or domain\user account). Each user group contains the virtual OS hosts that appear in that user’s My Virtual OS Hosts group.

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 "Database queries" (369).

- **Public queries**: Lists queries that an administrator, or a user with the Public Query Management (PQM) right, has added. Only users with the Ivanti 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.

**Scopes**

The Network View includes a shortcut to view existing scopes, or to edit or create new scopes. You can also define the fields you want to display in the Network View. For details about creating and using Scopes, see "Create a scope" (70).

**Configuration**

The Configuration group contains the following configuration subgroups.

- **PXE holding queue**: Lists PXE holding queues and the devices that are waiting in the PXE holding queue.
- **Bare Metal Devices**: Lists bare metal devices that have been created for provisioning tasks.
- **PXE Provisioning (Windows PE)**: Lists devices targeted for Microsoft Windows PE provisioning tasks.
- **Multicast domain representatives**: This item only applies for devices with agent versions older than 9.6. Lists configured multicast domain representatives that can be used for software distribution load balancing. For more information, see "Using self-organizing multicast with software distribution" (475).
- **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 overview" (550).
- **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).

**Inspector results**

When you use the Ivanti Inspector to view data, you can double-click a chart in the Inspector window and view the details in the Inspector Results window.

Viewing the results this way makes the data actionable. For example, in the Scheduled tasks inspector a chart can show how many devices have failed a task. If you double-click the chart, you’ll see the individual devices listed in the Inspector results folder. You can then apply an action to those devices (such as restarting the task) or view a report with that data to follow up.
Data in the Inspector results folder changes every time you double-click on a chart in an inspector window.

**Network View icons**

Note that in the Network View, an icon appears next to each item in the results list, to identify the type of device. Depending on whether the agent is installed, the device is currently connected, the health status, etc., a tiny overlay may also appear on or next to the device icon after you have clicked on it.

<table>
<thead>
<tr>
<th>Icons</th>
<th>Overlays</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Server" /></td>
<td>LANDesk agent is present</td>
</tr>
<tr>
<td><img src="image" alt="Workstation" /></td>
<td>Remote control agent is present</td>
</tr>
<tr>
<td><img src="image" alt="Laptop" /></td>
<td>Device status unknown</td>
</tr>
<tr>
<td><img src="image" alt="Mobile device" /></td>
<td>Device status unavailable; not connected</td>
</tr>
<tr>
<td><img src="image" alt="Apple device" /></td>
<td>Device with alert ruleset reporting a critical state</td>
</tr>
<tr>
<td><img src="image" alt="VMWare virtual host" /></td>
<td>Device with alert ruleset reporting warning state</td>
</tr>
<tr>
<td><img src="image" alt="VMWare virtual guest" /></td>
<td></td>
</tr>
</tbody>
</table>

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 "Configure agent discovery" (32).

**NOTE:** *Icon display quality*

These high-color icons 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.

**Create groups in the Network View**

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 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, can’t 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.

Configure 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 Ivanti 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.

**Create 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. You can specify the attributes you want to include, when creating or editing a column set.

![Network View with columns](image)

**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 “Specify the qualify option with software components” (28).

7. Click **OK** to save the column set.
Columns display

If after defining certain inventory attributes, you decide you want to hide a column or change its position in the Network View, you can use the shortcut menu to display the Select columns dialog.

To change or hide displayed columns

1. Right-click any device in the results list of the Network View.
2. Select Columns...
3. Use the Add ->, <-Remove, Move up, or Move down buttons to arrange the columns.
4. Click OK.

You can also return to the original columns display configuration by clicking Defaults.

Apply 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 Report
- Export as CSV
- Copy
- Delete
- Rename
- Properties
- Info
- Export
- Copy to other core(s)
- Auto sync
- Columns

**Specify 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, select a value from the list of available primary key values, and click **OK**.

**About the Column Configuration dialog**

This dialog contains the following options:

- **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 "Specify the qualify option with software components" (28).

- **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.

### View managed devices

Devices running Ivanti 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 and its inventory report has been sent to 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” (112).

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 "Viewing a summary inventory" (328).
When connected to a particular core server, the administrator can see every device managed by that core server. Other users 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 overview” (52).

**View 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**.

![Device Properties dialog](image)

**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.

**About the Inventory tab**

The **Inventory** tab contains a summary of the device's inventory data. For more details, see “Viewing a summary inventory” (328).

**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 Server 2012.

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.

About the 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 Ivanti 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.

Inventory data

More detailed information about the device is available in its inventory data. You can view extensive inventory information by double-clicking the device name in the results panel of the Network View.
Configure agent discovery

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

- **The standard Ivanti agent**: Enables the PDS (ping discovery service). If the standard Ivanti 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 Ivanti agent discovery with TCP/IP. Endpoint Manager looks for the standard Ivanti 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: 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.

The agent discovery defaults are to do discovery for only the selected device. You can adjust the discovery options by following the steps below.

**To configure agent discovery options**

1. Click Configure > Agent status options.
2. Select the discovery and refresh options you want. For more information, see the next section.
3. Click OK.

**Configure 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 email 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 email or an SNMP trap, or run an executable on the core when the alert is received. (You need to define each action, such as specifying where to send email 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.

**Monitor 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 email 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:** Closes the dialog without saving your changes.
Viewing device diagnostics and logs

Ivanti® Endpoint Manager powered by Landesk 9.6 SP1 added a new device diagnostics and logs viewer. You can access it by right-clicking a device and clicking Scheduled tasks and diagnostics.

The **Diagnostics and logs** window has the following features:

- Individual client logs (real-time) shown in the log viewer
- Get all client-side logs and upload to core or additional console as a zip file
- View core-side logs
- CSV export of devices
- Real-time PDS ping discovery (mismatches shown in red)
- Inventory
- HTML5 remote control
- Remote event viewer
- Remote file system
- Synchronize policies
- Searching the web for highlighted log content or the current return code
- Searching in any column

**Viewing device logs**

The integrated log viewer has the following features:

- Integrated log viewer (allows up to 50K of log information, option to use an external editor)
- Automatically shows failure log if available for the selected task
- Syntax highlighting
• Searching (max 200 matches)
• View client local scheduler tasks (real time)
• View client task history (real time)
• View client inventory change history (real time)
• Option to search the web for highlighted text
• Auto scroll to end of the log

You can view the following client logs:

• Agent install
• AV (install, Ldav, Ldav_scan, and Ldav_update)
• Current downloads
• Gather products
• Local scheduler
• Policy sync
• Proxy host
• Service host
• Reboot
• Software installer (sdclient)
• Status dialog
• Vulnerability scanner (vulscan)

You can view the following core logs:

• Console
• LDAP (schedldapresolver)
• Policy task handler
• Provisioning
• Queries (schedquery)
• Vulnerability core

**Access console tools**

Console tools are available through both the Tools menu (A) and the Toolbox (B). To enable the Toolbox, click **View > Toolbox**. To save space in the console, however, you may choose not to enable the Toolbox, and just select tools from the Tools menu.
Tools menu, Toolbox pane

Endpoint Manager administrator sees all of the tools in both the Tools menu and the Toolbox. Other Endpoint Manager users will see only the tools and features that are allowed by their assigned rights. Tools dependent on rights that a user hasn’t been granted don’t appear 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, below the Network View.

Tool windows can be resized, docked, floating, hidden, and closed. You can have multiple tool windows open at the same time, docked or floating. For more information, see "Move and resize tool windows" (38).

Favorites

If you find you use certain tools more often than others, you can quickly set up a Favorites toolbox by right-clicking any tool in the toolbox and selecting "Show in Favorites". You can then access your Favorites from the Favorites button in the bottom of the Toolbox panel.

Show/Hide image
Move and resize tool windows

The console lets you open as many 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 "Save console layouts" (42).

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.

Dock tool windows

You can "dock" a tool window, by 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 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.
**Float tool windows**

You can also undock the tools window and drag it (using its title bar) so it can "float" to another location inside or outside of the console. Floating tools can be dragged or resized to move them temporarily out of the way to give you more room to work on other tasks. When you drag the tools window, the tabs for any other currently-opened tools also float with it. To return the tool to its docked or default location, simply double-click it. Or you can drag it back to its position and release it when you see the gray docking rectangle in the correct location.

**Show/Hide image**

![Image](image.jpg)

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 tool windows**

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 panel also supports the auto hide feature.
Search for items with the Find bar

The Find bar 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 Find bar is included in that view to facilitate locating a specific item in the corresponding list.

An example may be helpful. Consider an organization that 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 find the exact entry among the 10,000 entries in a second or two.

![Find bar example](image)

**Step 2** Find text box, 3 In Column list, 4 Search button

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** 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.

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.

![Toolbar options](image)

**Console toolbar 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.

**Status bar**

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

```
5/48 item(s) selected  |  Agent Status: Cycle Ended  |  User: SJENSEN-2008VM\sjensen
```

**Status bar elements**

- Number of selected items in a listing
- Current job name and status
- Name of the currently logged-in user

**Console themes**

The console has several color themes that you can select. Select a theme from the **Theme** drop-down list in the console toolbar. The default is “Expression Dark.” Try some of the other options if you want something else.

You can only select from the list of available themes. You can’t customize an existing theme or create your own.
Save console 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 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 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.

### Change 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** list located on the right side of the console toolbar. Or, enter a core server name in the **Core** text box and press **Enter**.

   ![Core List](image.png)

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

2. Enter your 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** list in the toolbar.

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

### Ivanti Service Desk integration

If you have Ivanti Service Desk installed in your environment, you can configure the Endpoint Manager console to launch it from a Network View object's shortcut menu. The Service Desk shortcut menu items are disabled by default. You have to edit an XML configuration file to activate them. Once you edit this file and restart the console, the Service Desk menu items will appear.

When you right-click a user or device in the Network View, the following Service Desk shortcut menu options are available:

- Incident management
- Change management
Problem management
Request management

Selecting one of these choices will launch a Service Desk session in your default browser for the device or user you selected. Depending on your Service Desk configuration, you may be prompted to log in to Service Desk first. The URL in the launched session is based on data the XML configuration file. If the Service Desk session isn’t launching correctly, double-check your configuration there.

To enable Service Desk integration

1. On the core server that you want to have Service Desk integration, open C:\Program Files\LANDesk\ManagementSuite\ServiceDeskUrl.xml in your text editor.
2. Change <Enable>false</Enable> to <Enable>true</Enable>.
3. In the URL for each item, replace <SDhostname> with your Service Desk server's hostname.
4. Save your changes and restart the management console.

Viewing data using the inspector

The Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk inspector displays details about items in the Ivanti console. Use the inspector to quickly find information about managed devices, groups, queries, security configurations, and many more items.

Inspectors are defined for many standard items. For example, you can inspect managed devices, scheduled tasks, vulnerabilities, and the core server.

User rights required to view the inspector

To view the inspector, a user must have the correct right assigned in Role-based administration. The Inspector right has only one option, View, that can be enabled for a user. If a user doesn’t have this right, the Auto inspector and context-menu option for the inspector are not visible.

For information about Role-based administration, see “Role-based administration overview” (52).

Opening an inspector window

There are two ways to view data in an inspector window:

- Turn on the Auto inspector (click View > Auto inspect). This opens one window that displays data any time you click on an item. Each time you click another item, that item's data appears in the Auto inspector window.
- Right-click an item and select Inspect. A new inspector window opens with data for that item.

Inspector windows open separately from the console.
Viewing inspector data

Inspector windows contain different tabs and data. Items are displayed based on the XML file defined for that item. For example, a default inspector is provided for managed devices. When you click a managed device, you see the following tabs in the inspector window:
You can resize the window to view data. You can act on some items, such as the list of processes running on a managed device. From the inspector window, you can click the *Processes* tab, right-click a process in the list, and kill the process.
Similarly, you can stop or start services running on a device by clicking the **Services** tab and right-clicking a service in the list.

### Viewing inspector results

Some data items in an inspector window are displayed as charts. To view the details of a chart, double-click on the chart. The data details are displayed in the network view in the **Inspector results** list.

Each chart shows a summary of data when you point to a portion of the chart.
Double-click the chart to view the associated data in list format.
Viewing the results this way makes the data actionable. For example, in the Scheduled tasks inspector a chart can show how many devices have failed a task. If you double-click the chart, you’ll see the individual devices listed in the **Inspector results** folder. You can then apply an action to those devices (such as restarting the task) or view a report with that data to follow up.

Data in the **Inspector results** folder changes every time you double-click on a chart in an inspector window. In the example above, you would click on the "No anti-virus" section of a chart to see a list of devices without an antivirus application. If you click the “Anti-virus installed” section of the chart, the list changes to display devices with an antivirus application.

### Real-time data in inspectors

Some inspector data can be updated in real time. This can only happen if you have deployed a device agent that includes the Real-time inventory and monitoring component.

**To check whether a device has the real-time inventory and monitoring agent**

1. In the network view, right-click the device and select **Properties**.
2. Click the **Agents** tab.
Default inspectors

The following predefined inspectors are included when you install the inspector add-on:

- Column sets
- Computer queries
- Console users
- Console user groups
- Core servers
- Delivery methods
- Distribution packages
- Queries
- Roles
- Scheduled tasks
- Scopes
- Scripts
- Teams
- Vulnerabilities

Creating custom inspectors

You can create an XML file that defines inspector parameters for items in the Ivanti Management Console. To do this, you’ll need to be familiar with XML conventions and you’ll need to understand how data is managed in the database your core server uses.

For instructions on creating a custom inspector, see the "Creating a custom inspector" document in the Ivanti Community.

NOTE: Inspector help on the Ivanti User Community

The Ivanti User Community has technical documents and user forums for the inspector. To access the community, go to: https://community.landesk.com

Auto-inspect items

Use the Auto-inspect feature to display detailed information about any item you click. Each time you click a new item, the contents of the inspector window change to show the new item.

1. Click View > Auto Inspector.
2. Click an item in a list, such as a managed device, a scheduled task, or a vulnerability.
Unlinking an auto-inspector window

If you want to keep the data in an auto-inspector window, unlink the inspector.

1. Click the Unlink button 📊.

This keeps the current data in an inspector window, and you can then click other items that open in a new auto-inspector.

For example, you might unlink the data if you want to compare more than one item side by side. You would unlink the first data window and then click a new item to open a second inspector window.

Manually inspect items

If you don’t use Auto-inspect, you can inspect any item by right-clicking it. Each time you manually inspect an item, a new inspector window opens with the new data.

1. Right-click a list item (such as a managed device).
2. Select Inspect.

Unlinking dynamic content

Data in the inspector window can be dynamic. Some data items will refresh on a regular basis (if a device has the real-time inventory component).

To keep the data currently displayed in an inspector

1. Click the Unlink button 📊.

Refreshing data in an unlinked window

After you unlink an inspector window, you can’t re-link the data to make the data dynamic again. The data in the window stays the same unless you change the refresh setting.

To refresh data in an inspector

1. Click the Change refresh rate button 🔄.
2. The text next to the button indicates the current refresh setting. Click the button again to change the setting, which can be 10 seconds, 30 seconds, or 10 minutes.
User management

Role-based administration overview

Ivanti® Endpoint Manager powered by Landesk 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 Endpoint Manager is placed into the LANDESK Administrators group.

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.

NOTE: If you've upgraded from Endpoint Manager 8, setup creates a log file called ..\LANDesk\Management Suite\RBASetup.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 Endpoint Manager console users" (53)
- "Managing authentications" (56)
- "Managing roles" (58)
- "Understanding rights and states" (60)
"Creating scopes" (69)
"Using teams" (73)

Role-based administration workflow

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

1. Create roles for console users.
2. Use the Windows Local Users and Groups tool to add console users to the appropriate Windows LANDESK groups.
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. Optionally use teams to further categorize console users.

Adding Endpoint Manager console users

Endpoint Manager 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 Endpoint Manager installation is automatically placed into the Windows Ivanti Administrators user 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.

Endpoint Manager setup creates several local Windows groups on the core server. These groups control file system permissions to the Endpoint Manager and Security 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 Endpoint Manager 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 provisioning won't work correctly for users in this group because both those features use scripts.
- 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 Endpoint Manager 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.
The Users tool’s **Users and groups** tree shows the list of authorized console users. You can see the last time a console user logged in, their group, role, scope, remote control time restriction status, and team. You can also use this tree to see if users are in the LANDESK local Windows groups. Users won’t be able to log in until you’ve added them to one of the LANDESK groups described in this section.

Users are stored in the database by unique security IDs (SIDs). If a user’s active directory account name changes, for example if they got married, their SID should remain the same and their Endpoint Manager permissions will still apply.

---

**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.

---

### Add Endpoint Manager console users

Endpoint Manager 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 Endpoint Manager installation is automatically placed into the Windows **LANDESK Administrators** user 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.

**To add users to a LANDESK group from the Windows Computer Management dialog box**

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 box, click **Add**.
4. In the **Select the users and groups** dialog box, select the desired users (and groups) from the list and click **Add**.
5. Click **OK**.

**To add a Endpoint Manager console user or group**

1. Click **Tools > Administration > User management**.
2. In the **Users and groups** tree, right-click the authentication source containing the user or group you want, and click **New user or group**.
3. In the authentication source directory, select the user or group you want to add and click **Add**. If you want to select individual users within a group, right-click the group and click **Select users to add**. You can then select the users you want and click **Add selected users**.
4. In the dialog box reminding you to manually add the user or group you selected to the appropriate local LANDESK Windows group, click **OK**.
5. Click **Close**.
6. If you haven’t already, use the Windows Local Users and Groups tool to add the new user or group to the appropriate local LANDESK Windows group as described earlier in this section.

7. Assign roles and scopes to the new user or group.

Delete users

You can also use the Users and groups tree to delete console users or groups. When you delete a user or group, 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 or group that you select. Note that deleting a user or group only deletes that user or group from the Endpoint Manager user database. You’ll need to also manually remove the user or group from local LANDESK Windows groups they are members of. If you don’t do this, the deleted user will still be able to log into the console.

To delete a console user

1. Click Tools > Administration > User management.
2. In the Users management tree, click Users and groups.
3. Select the user or group 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/group or team and click the user, group, or team you want to receive the objects and click OK.
6. Remove the user from the local LANDESK Windows group or Active Directory group that gives them console access.

Viewing user or group properties

In the Users and groups tree, you can right-click a user or group in the right pane and click Properties. This properties dialog box shows all the properties and effective rights for that user. The properties dialog box has the following pages:

- **Summary**: Summarizes that user’s/group’s roles, scopes, teams, group membership, and effective rights.
- **Effective rights**: Shows a more detailed view of the user’s/group’s effective rights.
- **Roles**: Shows explicit and inherited roles. You can select which explicit roles apply to that user or group.
- **Scopes**: Shows explicit and inherited scopes. You can select which explicit scopes apply to that user or group.
- **Teams**: Shows explicit and inherited teams. You can select which explicit teams apply to that user or group.
- **RC time restrictions**: Allows you to apply and modify RC time restrictions. For more information, see "Using remote control time restrictions" (73).
- **Group membership**: Shows which groups that user is a member of.
- **Group members**: Shows the members of a group if a group is selected. Shows the group a user is a member of if a user is selected.

If you make changes to the editable pages, you need to click OK to apply them. You can then re-open the properties dialog box if necessary.

**Managing authentications**

Use the User management tool to define credentials for Active Directory groups that will have console access. These credentials only need to let Endpoint Manager 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 an Ivanti 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 Endpoint Manager:

- Active Directory is fully integrated with DNS and TCP/IP (DNS) is required. 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 Endpoint Manager 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 Endpoint Manager console users” (53).
- 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 “Configuring COM+ server credentials” (83).

If the account password for an authentication changes, you will have to log into the console and change the password in the authentication dialog box 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 has been corrected in the Users tool.
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, the user inherits the RBA rights for that group.
- If a user is a member of an Active Directory group, which is a member of a higher level group, the user inherits the RBA rights of the upper level group.
- Groups can be nested and inherit the appropriate rights according to the usual Active Directory rules.

Add an active directory authentication

Use the User management tool to define credentials for Active Directory groups that will have console access. These credentials only need to let Endpoint Manager 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 when assigning console group permissions.

To add an authentication

1. In the User management tool, right-click Users and groups and click New authentication source.
2. In the Authentication source dialog box, enter credentials that give access to the Active Directory.
3. Click OK.

Adjusting the directory query frequency

A utility called Resolveusergroups.exe runs periodically (every 20 minutes) to refresh the list of Ivanti® Endpoint Manager powered by Landesk console users.

Once the user list is resolved, it is placed in cache and used until Resolveusergroups.exe runs again. In some Active Directory environments, if the TTL values are too small, some of the resolved user accounts may have crossed the TTL threshold before all of the accounts are resolved. This causes the cache to be refreshed again and again, and the console loads very slowly.

If this happens in your environment, change the default TTL settings for Resolveusergroups.exe. You can run Resolveusergroups.exe /? to see its usage. The TTL values are in seconds. This is a specific example that sets the TTL values to the maximum:

```
Resolveusergroups.exe /verbose /TTL 600 /LDTTL 60
```

Any changes to the TTL values are written to the KeyValue table in the database (GroupResolutionTTL and LocalLDGroupResolutionTTL), so they are persistent.
Managing roles

Use the Roles tree to define and maintain administrative roles and their associated console rights. Console rights are based on Endpoint Manager 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 users or groups. Once you create a role, you associate it with a user or group in the Group Permissions tree.

Since you can assign multiple roles to users or groups, 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.

You can assign multiple roles to a user or 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. You can see the effective rights for a user or group by opening the properties for it and viewing the Effective rights page.

Generally, you should avoid assigning a role to the default local groups: LANDESK Management Suite and LANDESK Administrators. Assigning a role 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. The LANDESK Administrators group already has a default role of Administrator, which you can’t restrict further.

Changes to a logged-in user’s rights won’t take effect until the next time they log in.

For more information, see “Understanding rights and states” (60) and “Understanding the default roles” (60).
Create and assign a role

Use roles to define and maintain administrative roles and their associated console rights.

To create and assign a role

1. In the User management tool, right-click Roles and click New role.
2. In the Role properties dialog box, 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. In the tree click Users and groups and select the users and groups that will have the new role.

To assign an existing role to users and groups

1. In the User management tool, right-click Roles and click Properties. You can also double-click a role to edit its properties.
2. On the Users and groups page, select the groups you want to have that role.
3. Click OK.
Understanding the default roles

There are a number of default roles under the Roles tree. You can edit or delete any of these default roles, except for Ivanti Administrator.

- Auditing Configuration
- Auditor
- Inspector Viewer
- IT Help Desk
- Ivanti Administrator
- Patch Management
- Power Management
- Provisioning
- Security
- Software distribution
- Software licensing

**IMPORTANT:** Ivanti 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. Additionally, only users with the Administrator right can configure Ivanti services running on the core.

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 "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.

Console rights reference

Console rights provide access to specific Endpoint Manager 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:

- Administrator
- Agent configuration
- Alerting
- Basic Web console
- Content replication
- 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
- Inspector
- Link management
- OS provisioning
- Power management
- Public query management
- Refresh scopes
- Remote control tools
  - Chat
  - Execute programs
  - Reboot
  - Remote control
  - Transfer files
- Reporting
  - Report designer
  - Reports
- Security
  - Patch and compliance
  - Security configurations
- Software distribution
  - Delivery methods
  - Directory management
  - Distribution packages
  - Link management
  - Manage scripts
- Software license monitoring
- User administration
- vPro

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

**NOTE: 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).

**Endpoint Manager Administrator**

The Endpoint Manager 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 Endpoint Manager Administrator permission provides users the ability to:
• Manage users with the Users tool.
• See and configure product licensing in the **Configure** menu.
• Configure Ivanti services.
• **IMPORTANT:** Perform ALL of the Endpoint Manager 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.

**Content replication**
• 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.
• 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.

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.

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.

Device power control

- 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.
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.

Inspector
- No rights: Can’t see the Inspector tool.
- View: Can open the Inspector tool and view any item.

OS provisioning
- No rights: Can’t see the OS provisioning 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

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

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.

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

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.

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.

Reporting

Report designer
• No rights: Can’t open the designer.
• View: Not applicable.
• Edit: Can open the designer and create or edit reports.
• Deploy: Not applicable.
• Edit public: Not applicable.
Reports

- No rights: Can’t see the tool.
- View: Can see this tool and can view reports. Can run reports. Can’t change anything.
- Edit: Can see reports and change report properties. This right alone doesn’t allow access to the designer; the Report designer edit right is required to access the designer.
- Deploy: Can schedule and publish reports.
- Edit Public: Can move reports into the Public group.

Security

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.

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. Access 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.
- 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.
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.

Directory management
- 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.

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.

Link management
- No rights: Can’t see the Link management 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.

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.
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.

vPro
- No rights: Can’t view or change vPro information and settings.
- View: Not applicable.
- Edit: Can view and change vPro information and settings.
- Deploy: Not applicable.

Additional information about scheduled tasks
- If someone has “Deploy” rights for a tool that uses tasks that can be scheduled, 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.

Creating scopes

A scope defines the devices that can be viewed and managed by a Endpoint Manager and Security 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

Endpoint Manager and Security role-based administration includes one default scope: "All machines." 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 box 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 “Database queries” (369).

- **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 box 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 box. 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 Endpoint Manager 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 Endpoint Manager 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 effect 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).

Create a scope

A scope defines the devices that can be viewed and managed by a Endpoint Manager 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.

**To create a scope**

1. Click **Tools > Administration > User Management**.
2. Right-click **Scopes** and click **New Scope**.
3. In the **Scope Properties** dialog box, 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 box, 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 (you can browse the directory by clicking **Browse directories**), and then click **OK**.

Click on the plus (+) and minus (-) signs to expand and collapse nodes in the directory tree. 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 box.

**To create a scope based on an existing query**

1. Right-click **Scopes** and click **New scope from query**.
2. Select the query you want and click **OK**.
3. A copy of the query will be made and a new scope appears in the tree with a name based on the source query name.

NOTE: You can quickly create a scope from an existing query by dragging a query from the Network view and dropping it onto the scopes tree.

NOTE: Scopes use a copy of the query they are based on. Changes to the source query in the Network view won’t affect existing scopes.

**About the Scope properties dialog box**

Use this dialog box to create or edit a scope. You can access this dialog box 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 box where you can define and save a query. This is the same query dialog box 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 box where you can select locations from inventory data. 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. If you click Browse directories, you can browse and select devices from the actual LDAP directory tree for directories you’ve configured.
  • **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 box 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 box where you can change query parameters and statements.

**Create a team**

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.

**To create a team**

1. In the User management tool, right-click Teams and click New team.
2. Enter a team Name.
3. Select the Users and Groups that you want in the team.
4. Click OK.
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.

Using remote control time restrictions

Remote control time constraints limit the hours and days console users can initiate remote control sessions. You can specify the days of the week and the starting and ending time (in UTC format) 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.

By default no remote control time restrictions are active.

Note that RBA rights are additive. If a user is a member of multiple roles, you could unintentionally allow remote control when you intended to restrict it.

For example, if a user is a member of a remote control role that includes time restrictions and that user is also a member of a security role that doesn't include time restrictions, that user won't have any remote control time restrictions.

To ensure remote control time constrictions are applied in the way you intend, you may want to make sure users with time restrictions have only one role applied to them.
Assign remote control time restrictions

Remote control time constraints limit the hours and days console users can initiate remote control sessions.

To use remote control time restrictions

1. In the User management tool (Tools > Administration > User management), right click a user or group in the Users and groups tree and click Properties.
2. In the left pane click RC time restrictions.
3. Check Use time constraints.
4. Check the days you want enabled.
5. Enter the UTC time range that you want to allow remote control.
6. Click OK when done.
Core configuration

Running Ivanti® Endpoint Manager powered by Landesk setup

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

For release notes, installation instructions, and important additional information, make sure you visit the Ivanti® Endpoint Manager powered by Landesk 2017 announcement page on the Ivanti Community:

- https://community.landesk.com/docs/DOC-42261

For more information on supported platforms and system requirements, see this document in the Ivanti user community:

- https://community.landesk.com/docs/DOC-23848

The Indexing service and Windows Search service must both be disabled prior to installation of Ivanti® Endpoint Manager powered by Landesk; failure to disable these services could cause the installation to fail.

Also make sure that the server you’re installing to doesn’t have Microsoft’s Windows Server Update Service installed on it. If this service is active you will have problems logging into the console.

Because each environment has different needs, we recommended that you contact Ivanti Professional Services, your reseller, or your Expert Solution Provider (ESP) about Certified Ivanti Deployment.

For more information visit the following web site:

- http://www.landesk.com/services/implementation-services/

Endpoint Manager setup will open ports in the Windows Firewall on the core server. Normally, Endpoint Manager setup and agent configuration will configure these ports automatically. If you’re using a different firewall, you will need to configure the ports manually. For more information on the ports Endpoint Manager uses, see the following URL:

- Ports used by Ivanti® Endpoint Manager powered by Landesk- full list: https://community.landesk.com/support/docs/DOC-1591
To install Ivanti® Endpoint Manager powered by Landesk with the built-in SQL Express database

1. From your installation media, launch Setup.exe.
2. In the main welcome screen, select an installation language and then click Continue.
3. Accept the license agreement and then click Continue.
4. On the What do you want to install page, make sure Core server is selected and then click Continue.
5. On the Prerequisites page, make sure your server passes the prerequisites check. If it doesn’t, install the missing prerequisites and click Continue.
6. On the How should Ivanti configure your database page, click Configure a new 2016.4 database and then click Continue.
7. On the Database application page, select SQL Express (Bundled) and then click Continue.
8. On the Where do you want to install page, click Continue to accept the default installation path (C:\Program Files\LANDesk\ManagementSuite\).
9. On the Secure Client Management page, click Enable Client Certificate-based Security if this the first time Endpoint Manager has been installed in your environment. Otherwise, read “Client certificate-based security” (144). Click Continue.
10. On the Ready to install page, click Install.
11. When setup finishes, click Reboot now.
12. After you reboot, wait five minutes for all of the services to start.
13. Activate your core as described in "Activating the core server" (79).
14. Launch the console and log in with the Windows credentials of the user logged in during Endpoint Manager 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 Endpoint Manager. It’s important that you complete these steps. After you’ve done this, see “Configuring device agents” (112) and the Ivanti User Community at https://community.landesk.com for more information about agent deployment.

Set up additional Endpoint Manager consoles

The Endpoint Manager console is automatically installed on the core server. This console should be installed on Ivanti administrator’s machines that need full functionality or access to all the Endpoint Manager tools. The console is used to interact with the various Endpoint Manager features, for example, 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. (Ivanti doesn’t charge extra for additional consoles.)
For more information on supported platforms, see this document in the Ivanti user community: https://community.landesk.com/support/docs/DOC-7478.

**To install an additional console**

1. From your installation media, launch Setup.exe.
2. In the main welcome screen, select an installation language and then click **Continue**.
3. Accept the license agreement and then click **Continue**.
4. On the **What do you want to install** page, make sure **Additional Console** is selected and then click **Continue**.
5. Follow the remaining installation prompts.

**Set up the Web console**

The Web console offers a subset of the Endpoint Manager 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.

**Console and Web console functionality comparison**

The following table lists the capabilities of the Endpoint Manager console and the Endpoint Manager Web console.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Console</th>
<th>Web Console</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Configuration</td>
<td>Yes</td>
<td>Minimal</td>
<td>Scheduled Agent Deployments and Update tasks are visible and controllable by Web console users with rights to Agent Configuration.</td>
</tr>
<tr>
<td>Alerting</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Column Set Configuration</td>
<td>Yes</td>
<td>Yes</td>
<td>In the Web Console access under Preferences on the Custom Columns tab.</td>
</tr>
<tr>
<td>Configure Services</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Connection Control Manager</td>
<td>Yes</td>
<td>Minimal</td>
<td>Scheduled deployments are visible and controllable by Web console users with rights to CCM.</td>
</tr>
<tr>
<td>Capability</td>
<td>Console</td>
<td>Web Console</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom Data Forms</td>
<td>Yes</td>
<td>No</td>
<td>Tab located under Distribution in Web console.</td>
</tr>
<tr>
<td>Delivery Methods</td>
<td>Yes</td>
<td>Yes</td>
<td>Vastly different behavior – the only overlapping function is to run an inventory scan (on Web “Scan Device”).</td>
</tr>
<tr>
<td>Device right-click</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Directory Manager</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Display Manager</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Distribution Packages</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Host Intrusion Prevention</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>LaunchPad Link Manager</td>
<td>Yes</td>
<td>Minimal</td>
<td>Scheduled LaunchPad Link Deployments are visible and controllable by Web console users with rights to Software Distribution.</td>
</tr>
<tr>
<td>Logs</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Manage Scripts</td>
<td>Yes</td>
<td>Partial</td>
<td>From Scripts, existing scripts can be scheduled and grouped.</td>
</tr>
<tr>
<td>Power Management</td>
<td>Yes</td>
<td>Minimal</td>
<td>Scheduled power policy tasks are potentially visible and controllable by Web console users.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>PXE Boot Menu</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Query Capability</td>
<td>Yes</td>
<td>Partial</td>
<td>The Web console allows use of a Count feature which is not in the Windows console. Queries can't be viewed as reports in the Web console.</td>
</tr>
<tr>
<td>Remote Control</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>Yes</td>
<td>Yes</td>
<td>The reporting console launches in a separate browser window.</td>
</tr>
<tr>
<td>Scheduled Tasks</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Scopes</td>
<td>Yes</td>
<td>Partial</td>
<td>Existing scopes can be added to a user, but new scopes can't be created.</td>
</tr>
<tr>
<td>Capability</td>
<td>Console</td>
<td>Web Console</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security and Patch Manager</td>
<td>Yes</td>
<td>Minimal</td>
<td>Scheduled scans and repair tasks are visible and controllable by Web console users with Patch Manager rights.</td>
</tr>
<tr>
<td>Software License Monitoring</td>
<td>Yes</td>
<td>Partial</td>
<td>In the Web console product usage data is not visible, individual product and group compliance reports are not available, and you can’t ignore or group products.</td>
</tr>
<tr>
<td>Unmanaged Device Discovery</td>
<td>Yes</td>
<td>Minimal</td>
<td>Scheduled unmanaged device discovery scans are visible and controllable by Web console users with rights to UDD.</td>
</tr>
<tr>
<td>Users</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Windows CE Agent Configuration</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Windows CE CAB Creator</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Activating the core server**

Ivanti® Software uses a central licensing server to help you manage your core server’s product and node licenses. To use Ivanti products, you must obtain from Ivanti 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 Ivanti 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 Ivanti Software programs you’re using (collectively, the “node count data”)
- General feature usage statistics

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

You can install additional Ivanti products under your 45-day evaluation license by using the installation media'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 Ivanti 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 Ivanti username and password.

There are two types of licenses, client and server. Any time you install Endpoint Manager agents on a server operating system, such as Windows 2012 Server or Windows 2008 Server, that installation consumes a Endpoint Manager 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 Ivanti, 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 Ivanti with the node count data. Once you send the node count data, Ivanti 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 Endpoint Manager 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.

**Participating in the Ivanti Customer Experience Improvement program**

Ivanti is committed to using Customer Experience Improvement Program data to improve Ivanti software for its customers. You may participate in the Ivanti Customer Experience Improvement Program to contribute your individual experience to the overall feedback affecting the development of Ivanti software products. Participation in the Customer Experience Improvement Program is strictly voluntary.

For more information on this program, see the following PDF document:

The participation option is in the activation utility. You can change your participation status from there, even if you've already activated your product.

**To change your participation status**

1. Launch the activation utility by clicking **Start > Ivanti > Core Server Activation**.
2. On the **Activation** tab, select or clear **Participate in the Ivanti Customer Experience Improvement Program**.
3. Click **Activate**. It may take a few minutes for the activation process to complete.

**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 > Ivanti > Core Server Activation**. If your core server doesn't have an Internet connection, see "Manually activating a core or verifying the node count data" (83).

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 Ivanti account.

Periodically, the core server generates node count verification information in the "\Program Files\Ivanti\Authorization Files\LANDESK.usage" file. This file gets sent periodically to the Ivanti 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 Ivanti licensing server.

The core communicates with the Ivanti 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 an Ivanti account**

Before you can activate a new server with a full-use license, you must have an account set up with Ivanti that licenses you for the Ivanti 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 Ivanti sales representative.
To activate a server

1. Click Start > Ivanti > Core Server Activation.
2. Click Activate this core server using your Ivanti 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 Ivanti 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 Ivanti 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 > Ivanti > 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 Ivanti 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 Ivanti 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 > Ivanti > Core Server Activation.
2. Click Update this core server using your Ivanti 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\Ivanti\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. Ivanti will process the message attachment and reply to the mail address you sent the message from. The Ivanti message provides instructions and a new attached authorization file.
3. Save the attached authorization file to the "\Program Files\Ivanti\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.

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 Endpoint Manager 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, Endpoint Manager 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.

Credential manager

Use the credential manager tool (Tools > Configuration > Credential manager) to centrally manage credentials for the following:

- Agentless scanner
- SQL servers
- Preferred servers

These credentials can still be configured elsewhere in many cases, but the credential manager provides a central location.

Some components allow you to specify multiple credentials. In these cases you can also specify the order credentials will be tried by that component. Use the arrows to change the credential ordering.
Configuring the Workspaces database after core setup

If you want to use Ivanti Workspaces with Ivanti Management and Security 2016.3, you’ll need to configure a database that Workspaces can use.

After you run the 2016.3 setup on the core server and reboot, the core checks for existing Workspaces database connection information. If it can't find that information, the Ivanti Configuration Center will launch in a web browser so you can provide it. Depending on your server configuration, you may have to click through an HTTPS security warning for this page to load.

If you don’t want to configure a Workspaces database at this time, click Cancel to close the dialog box. The dialog box will reappear the next time you launch Configuration Center.
To configure the Workspaces database instance

1. If you haven’t already, open SQL Server and create an empty database for Workspaces.

2. In Configuration Center, enter the connection details for the Workspaces database you created. These details are for the new empty Workspaces database, not the LDMS database.
   - If your database requires more connection information than our interface provides, use the Specify as connection string option.
   - If you want to use Windows credentials for a Windows user that has SQL permissions to configure the database, select the Integrated Security check box. The User Name and Password boxes will disappear and the logged-in Windows user credentials will be used for authentication.

     When using integrated security, you need to modify some IIS application pool identities so the database configuration can complete. Follow these steps here: Configuring IIS application pool identities for integrated security.

3. Click Test Connection to make sure the connection details work.

4. Click Configure Database to configure the database. This may take a few minutes.

5. After the database configuration completes, click Close.
NOTE: If you've configured the database but users can't log in to Workspaces, try doing an IIS reset.

Configuring IIS application pool identities for integrated security

Follow these steps if you're using integrated security.

1. In IIS Manager, change the ConfigurationCenter application pool identity to the database user.
2. In Ivanti Configuration Center, configure the database.
3. In IIS Manager, change the ConfigurationCenter application pool identity back to LocalSystem.
4. In Ivanti Configuration Center, edit the My AppPool1 application pool in the My instance, and change the identity to the database user.

Ivanti® Endpoint Manager powered by Landesk 2017 server certificate configuration

This topic contains information about configuring Trusted Root Certification Authorities.

The problem

For Microsoft Internet Information Services (IIS) to properly handle client certificate-based authentication, it's important that the certificates in the Trusted Root Certification Authorities container be properly configured. The certificates contained in this container should all be self-signed certificates. If non-self-signed certificates are installed on this container, it can cause certificate-based authentication for IIS to fail with HTTP error 403. For a description of the HTTP 403.16 and 403.7 errors, see this website:

- [https://support.microsoft.com/en-us/kb/2802568](https://support.microsoft.com/en-us/kb/2802568)

Resolution

Part 1: Remove non-self-signed certificates from Trusted Root Certification Authorities

This issue can be addressed by removing all non-self-signed certificates from the Trusted Root Certification Authorities in Certificate Manager (certmgr.msc) and moving them to the appropriate location instead, such as Intermediate Certification Authorities. Make these changes with caution, because other software may be affected; you'll need to run software tests to ensure everything still works properly.
Part 2: Change the SCHANNEL Settings in the Windows Registry

On some systems, it may be necessary to change the following registry keys that affect how certificates are trusted:

1. Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL, Value name: ClientAuthTrustMode, Value type: REG_DWORD, Value data: 2
2. Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL, Value name: SendTrustedIssuerList, Value type: REG_DWORD, Value data: 0 (False, or delete this key entirely)

For information about the SCHANNEL registry key and its uses, see these websites:


**Supported platforms and functionality**

For more information on the operating system versions and languages that Endpoint Manager supports (for the core server, managed devices, and Ivanti tools and features), see the following Ivanti User Community documents:

- [Supported Platforms and Compatibility Matrix for Endpoint Manager](#)
- [Supported Client Languages for Endpoint Manager](#)
Endpoint Manager port usage

When using Endpoint Manager 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 documents on the Ivanti User Community identify the ports that Endpoint Manager uses on your core server and managed devices.

- Ports used by Ivanti Endpoint Manager - Full List: https://community.landesk.com/support/docs/DOC-1591

**IMPORTANT:** Typically, during the installation process Endpoint Manager setup and agent configuration will configure these ports automatically in the Windows Firewall. However, if you’re using a different firewall product, you will need to configure the ports manually.

Configuring services

Many of the most integral and fundamental functions provided by Ivanti 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 Ivanti Software Services** applet that you can launch from the **Ivanti** Start menu program group (or from the management console, click **Configure > Services**).

**NOTE:** Configuring services is restricted to only Ivanti Administrators
Only a user with the Ivanti 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 topic to learn about:

- "Selecting a core server and database" (89)
- "Configuring the Inventory service" (90)
- "Resolving duplicate device records in the database" (93)
- "Configuring the scheduler service" (95)
- "Configuring the Custom jobs service" (97)
- "Configuring the Multicast service (pre-9.6 agents only)” (98)
- "Configuring OS virtualization credentials" (99)

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 General tab

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

The Reporting database user credentials let you connect to the database with a different user account when using the Reports tool. For example, you can create a user account for the database with read-only rights, then use that account so that reporting users can read from, but not modify, the database.

- **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.
- **Reporting database user**: Specify the user name and password for the account that you want the Reports tool to access the database with. This account must have already been created with specific access rights to the 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.
- **FIPS 140-2**: Enables FIPS 140-2, a US government security standard that defines an allowable set of cryptographic functions. For more information, see About FIPS 140-2 Support.
- **Single Sign-on**: Enables the user to log onto the Ivanti console without having to enter a username and password. For more information, see Single Sign-on into the Ivanti console.
- **Refresh settings**: Restores the settings that were present when you opened the dialog box.

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 Ivanti Software Services **Inventory** tab can’t restart the Inventory service on a clustered core.

**About the 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 box. 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 box. Configure when the software scans run and how long to save the inventory history.
- **Attributes**: Opens the **Select attributes to store** dialog box, which lets you limit the number of scan attributes that get stored in the database. This can reduce database size and speed up scan insertion time.
- **Manage duplicates**: Opens the **Duplicate devices** dialog box, where you can configure how duplicate devices are handled.
- **Manage duplicates**: **Device IDs**: Opens the **Duplicate device ID** dialog box, 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" (93)).

- **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 (**Configure** > **Services** > **Inventory** tab > **Unknown items** button) 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 box*

Use this dialog box (**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.
By default, if a duplicate MAC address is detected five or more times, it is automatically added to the ignore list during database maintenance. You can change this threshold by clicking Configure > Services > Inventory tab > Advanced settings > Duplicate MACs threshold.

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 >> 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 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 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 box. You can change other scheduler-related 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 Change login dialog box**

Use the **Change login** dialog box (click Configure > Services > **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 Ivanti 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 user name you want the scheduler to use.
• **Domain:** Enter the domain for the user name you specified.
• **Password:** Enter the password for the credentials you specified.
• **Confirm password:** Retype the password to confirm it.

## 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 Ivanti agent protocol, CBA. When you disable TCP remote execute as the remote execute protocol, custom jobs uses the standard Ivanti agent protocol by default, whether it’s marked disabled or not. Also, if both TCP remote execute and standard Ivanti agent are enabled, the custom jobs service tries to use TCP remote execute first, and if it’s not present, uses standard Ivanti 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 Ivanti 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 Ivanti agent protocol by default.

• **Disable CBA execute / file transfer:** Disables the standard Ivanti agent as the remote execute protocol. If the standard Ivanti 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 are triggered 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 Ivanti 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 are triggered 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 Ivanti agent ping via UDP. Most Ivanti device components depend on the standard Ivanti agent, so your managed devices should have the standard Ivanti 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. When selected, this will result in a subnet directed broadcast being sent via UDP using PDS.

- **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 (pre-9.6 agents only)**

Multicast was improved in Endpoint Manager 9.6 and the options on this tab only apply if you multicast to devices with older agent versions.

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 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 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.

### Configuration Center

The Configuration Center gives you access to applications used to establish web access to BridgeIT and Workspaces. From this interface, you can configure settings for the Framework and login authorization service Identity Server. Once configured, users access the web page to reach Workspaces and manage assets, user types, and other settings.

Although the Configuration Center is also used on Ivanti Service Desk, the version of Configuration Center included in Ivanti® Endpoint Manager powered by Landesk installations and upgrades only extend to setting up Workspaces.

The Configuration Center is automatically installed and ready for use with a clean install or upgrade to Ivanti® Endpoint Manager powered by Landesk 2016.4.

Any errors generated by the Configuration Center are logged in

C:\ProgramData\LANDesk\ConfigurationCenter\Logfiles.

Upgrades to Ivanti® Endpoint Manager powered by Landesk 2016.4 must update the Configuration Center Service Desk Framework.

### Using the Identity Server for centralized Workspace logons

Identity Server is a Secure Token Service that delivers OAuth2 and OpenID Connect tokens. It acts as a login authorization service that replaces the standard logon policy for Framework and BridgeIT. Using this service, you can utilize single sign in and federated authentication.
Identity Serve also allows you to handle both explicit and token logons simultaneously through the framework.

To set up Identity Server, see the process overview.

**Accessing the Configuration Center**

When you have installed the software to run on your Ivanti Web Server, you need to use the Configuration Center to create an instance, an application pool, and then the required web applications.

From a web browser, open https://[server name]/ConfigurationCenter.

Replace [server name] with the name of your Ivanti Web server. The page automatically logs you in with your Ivanti® Endpoint Manager powered by Landesk credentials. Select the one instance option available.

By default, both My.Framework and My.BridgeIT are installed to your instance.

---

**NOTE:** Your login credentials are specific to your Ivanti core server. Just 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).

---

**Changing the Framework to use Identity Server**

The Identity Server logon policy allows you to handle both token and explicit connection types. While this setting is not exclusive to users wanting Identity Server, we recommend making this change as a long-term solution. It can remove the need to specify only one Windows logon method or the other, instead allowing you to handle both simultaneously.

If you want to use the Identity Server, this task must be completed.

**To change the logon policy**

1. Click **Edit** next to the My.Framework application.
2. Change the **Logon policy** to **Identity Server**.
3. Click **OK** to save.

If you're setting up Identity Server, continue to [the task below](#) for changing the BridgeIT logon policy.

**Updating the Framework application**

If you've upgraded to Ivanti® Endpoint Manager powered by Landesk 2016.4 from a previous version, then you must update your framework for users to access Workspaces. Until this is performed, Workspaces is no longer accessible to users.
• For environments using only Ivanti® Endpoint Manager powered by Landesk 2016.4, this upgrade is required to use Workspaces.

• For integrated environments using Ivanti® Endpoint Manager powered by Landesk and Service Desk 2016.4 with an integrated Workspace, this upgrade is required, but must be performed in a specific order.

From the Configuration Center, click **Update** next to the My.Framework application. The update begins.

Plan this task accordingly, as the update may take some time to complete. Once complete, you’ll need to perform the next task below of changing the Framework **Logon policy** to **Identity Server**.

### Creating the Identity Server application

When using the Identity Server with Ivanti® Endpoint Manager powered by Landesk, all configuration settings are automatically populated with the details needed to run it from your LDAP database.

This step must be done prior to changing the logon policy for BridgeIT to Identity Server.

**To use the Identity Server, you must first add it as an application**

1. Under Available Applications, click **Create** for Identity Server. The Identity Server Secret is automatically populated with the values set from the BridgeIT application.

2. Set the **User Consent Expiration (Days)** as desired. By default, this is set to 7. This determines how often users must allow their user identifier to be used when accessing Workspaces before they are prompted to give access once again.

3. Click **OK**.

### Setting the logon policy for BridgeIT

Organizations use different methods of user authentication. Companies using Active Directory or logins explicit to Ivanti® Endpoint Manager powered by Landesk only will use the **Token only** option, whereas the **Explicit only** logon policy is more relevant to Service Desk users.

Selecting a logon policy defines the authentication method you wish to use when determining which users credentials you want to leverage. Specific services will require certain logon policies.

**IMPORTANT:** BridgeIT must connect to a framework with the same **Logon policy**. For example, if BridgeIT is set to **Token only**, then you must also set the Framework to **Token only**.

• **Explicit only.** This option is available for all applications. When selected, users must enter their Ivanti Service Desk credentials to access the applications each time they log in.
• **Integrated only.** This option is available for Framework and Web Access. By picking this option, the Identity Server uses the user's network credentials to identify their corporate account and log in automatically.

• **Token only.** This is the default, and available for Framework, Web Access, and BridgeIT. We recommend using this specifically for Web Access and BridgeIT. This option provides single sign-on (SSO) for Web Access and BridgeIT using Ivanti's Secure Token Server (STS). The STS is installed as part of the Ivanti Service Desk or Asset Central server installation option. SSO allows users to log in once to access a variety of different applications through the use of a single username and password. If you use the STS, this means that users can log in to Workspaces (BridgeIT) or Web Access with their Active Directory username and password.

• **Shibboleth only.** This option is available for Framework, Web Access, and BridgeIT. Shibboleth must be configured to pass the user's identity in the URL request that is sent to Ivanti® Endpoint Manager powered by Landesk. For more information about configuring Shibboleth, see Service Desk's documentation on Configuring Shibboleth authentication. You'll need to include the following in the header of the form:

  ```
  ?http_landesk_user=userid
  ```

  **CAUTION:** If the Logon policy is set to Shibboleth only, secure access to Workspaces becomes the sole responsibility of Shibboleth.

• **Identity Server.** This option allows you to use the Identity Server, a login authorization service that utilizes both Explicit and Token logon policies.

**Changing BridgeIT to use Identity Server**

As part of the process for configuring use of the Identity Server, you must configure the BridgeIT app before creating the Identity Server application.

If you want to handle all user logins to Workspaces with Identity Server, you'll need to change the logon policy for the BridgeIT application.

**To redirect the BridgeIT application to use Identity Server**

1. Click **Edit** for the My.BridgeIT application.
2. Open the drop-down menu for **Logon policy** and select **Identity Server**. The **Identity Server Secret** and **Identity Server Url** automatically populates.
3. Click **OK**.

**Configuring Discovery Services for Workspaces**

Discovery Services allows you to collect discovery data from third-party sources. You can monitor this device data from the Workspaces interface, as well as make changes.
To enable device discovery

1. Click Edit for the My.BridgeIT application.
2. For the Discovery Web Api Url field, enter https://[hostname]/discovery\api, replacing [hostname] with your core server hostname.
3. If needed, enter the User Name and Password for STS and click Test STS Connection to ensure a connection can be made between services.
4. Click OK.

Once completed, you can continue device discovery setup on Workspaces.

For more information on using Configuration Center with Service Desk, see the Service Desk online help here:


For more information on configuring Workspaces, see the Featured Content Ivanti Community documents here:

- [https://community.landesk.com/support/community/systems/workspaces](https://community.landesk.com/support/community/systems/workspaces)

Identity Server

Identity Server is a Secure Token Service that delivers OAuth2 and OpenID Connect tokens. It acts as a centralized login authorization service that replaces the logon policy for BridgeIT, allowing you to handle both token and explicit policies simultaneously. Using this service, you can utilize single sign in and federated authentication.

End users obtain authorization to access resources via authentication redirection. Using this secret exchange, user clients obtain access tokens needed to use Workspaces.

Running Identity Server on a new core installation

By default, the settings, framework, and applications needed to use Identity Server when accessing Workspaces are preconfigured and require no additional setup. When accessing Workspaces using My.BridgeIT, users are redirected to the Identity Server login page.

Running Identity Server on an upgraded 2016.4 core server

Administrators that upgrade to 2016.4 or later must manually add the Identity Server app from the Configuration Center.
To configure Identity Server

1. Change the Framework logon policy to Identity Server. Once updated, edit the Service Desk Framework application to change the logon policy to Identity Server. This allows the framework to handle both explicit and token connections.

2. Update the Service Desk Framework in Configuration Center. This is required of all upgraded servers and is not specific to Identity Server. No other changes should be made in this process until that update is complete.

3. Add the Identity Server application to the Application Pool.

4. Change the BridgeIT application logon policy to Identity Server.

5. Log in to Workspaces using Identity Server by following the task below.

Signing in to Workspaces with Identity Server

After configuring My.Framework and My.BridgeIT’s logon policy, as well as adding Identity Server as an application, you can now use Identity Server as a single-source login portal to access Workspaces from multiple authentication sources.

1. From a web browser, open https://[server name]/My.BridgeIT.

   Replace [server name] with the name of the fully-qualified server name. The page automatically logs you in with your Ivanti® Endpoint Manager powered by Landesk credentials.

2. Log in with your desired credentials, based on your login policy. If the policy is set to Allow Windows Logins, users must enter their LDAP credentials. This includes domain credentials, if applicable.

3. If the login was successful, the browser asks permission to use your user identifier. If you select Yes, allow, then you are redirected to Workspace.
Core synchronization

Core synchronization lets you 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
- Agent settings
- Alerting
- Dashboards
- Delivery methods
- Distribution packages
- Power management settings
- Queries and query column settings
- Reports
- Rollout projects
- Scripts
- Software scan
- Tasks and policies
- User management

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 Endpoint Manager 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 provisioning and software license monitoring tools don't support core synchronization.

### Add servers to the core synchronization list

Before you can use core 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](image)
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 box. 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 Change login dialog box” (96).

Synchronize items on demand

Use core synchronization to 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.
Automatically synchronizing items

Before using auto sync, configure which Endpoint Manager 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 core sync 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 the 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 the group hierarchy specified in the .ldms file. New IDs are assigned to each item.

For more information on how conflict management works, see "Core sync conflict management" (110).

**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**.

**Monitoring core synchronization status**

When you select a **Core server** or **Component** in the Core synchronization tool's 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.

**Core sync conflict management**

Core sync exportable items have a unique ID that helps Endpoint Manager 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.

**Change 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 box 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**.
Agent configuration

Configuring device agents

Devices need the Endpoint Manager agents on them to be fully manageable.

Read this topic to learn about:

- "Working with agent configurations" (112)
- "Create an agent configuration" (114)
- "Using the advance agent" (116)
- "Update agent preferences on devices" (115)
- "Create standalone agent configuration packages" (116)
- "Agent security and trusted certificates" (140)
- "Uninstalling device agents" (122)

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.

NOTE: 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 Ivanti agent and the remote control agents aren't present. For more information, see the deployment documentation on the Ivanti community at https://community.landesk.com.

NOTE: Agent configuration in mixed-language environments
When creating agent configurations in mixed-language environments, make sure the agent configuration name uses only ASCII characters (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.

Working with agent configurations

Endpoint Manager uses agent configurations that you create to deploy agents and agent preferences to managed devices. Once devices have the Endpoint Manager agents on them, you can use agent settings to easily update your agent configuration preferences without reinstalling the agent. For more information, see "Agent Settings overview" (317).
You can use the Agent Configuration tool 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 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. There can only be one default configuration for each configuration type. The default configuration can’t be deleted, but it can be edited. It is a good idea to not have too many different configurations, as this makes support and troubleshooting more complex and time-consuming.

Prior to installing any agent software, you must 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. For example, a laptop system might need a different configuration than a desktop system. In order to avoid deploying an 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 Ivanti 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 Ivanti software updates on devices and core servers even if you don’t have a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content subscription. With an Endpoint Security for Endpoint Manager 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 Ivanti User Community Web site at https://community.landesk.com/support/docs/DOC-23482.

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

However, if the agent configuration name uses 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:

- "Create an agent configuration" (114)
- "Using the advance agent" (116)
- "Update agent preferences on devices" (115)

**Create 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.
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" (116).
- **Schedule the agent configuration:** Push the configuration to devices that have the standard Ivanti agent installed. 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**.

**Update 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.

Create 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 Endpoint Manager to create the package. It may take a few minutes.

Using the advance agent

The advance agent is the preferred method for deploying the agent in most environments. This agent has been created to leverage Ivanti bandwidth-friendly technology during the agent deployment. It can reduce the amount of network bandwidth used for Windows-based agent configuration. The Advance agent uses 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 package.
The advance agent works well for most devices, including laptops with intermittent or slow network connections. However, it 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.

### Create an advance agent configuration

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 them 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.

Self-electing subnet services

Ivanti® Endpoint Manager powered by Landesk 10 introduced a new feature called Self-electing subnet services (SESS). With SESS, managed devices:

- Self-organize on the same subnet to provide services, allowing automatic fail-over and avoiding duplication of services.
- Use a smart election process that ranks available devices by configuration and ability to provide the service.
- Trust each other if they report to the same core server.
- Use signed messages for SESS security purposes (to avoid impersonation).
- Use the same client certificates used for CSA access.

Click the link below if you want to see a brief video that describes where SESS is configured.

With Endpoint Manager 2017.1, SESS is used for the following tools and services. Other services will be supported in the future.

- Unmanaged device discovery tool
- Multicast service
- PXE boot service
- Agentless scanner service

Here's a brief video introducing SESS.

Self-Electing Subnet Services in Ivanti Management and Security (3:09)
Configuring SESS in agent settings

Manage SESS from the client connectivity agent settings (Tools > Configuration > Agent settings, Client connectivity).

The multicast service is always enabled. The Extended device discovery service for ARP is also enabled by default, though you can disable it if necessary.

These services are disabled by default:

- Extended device discovery WAP discovery
- Provisioning PXE server
- Agentless scanner service

Note that for SESS to function, both the deployed SESS agent setting and the desired network state in the Self-electing subnet services tool must both be enabled. If you don’t enable the SESS service you want in the deployed agent settings, enabling SESS for that service in the Self-Electing subnet services tool won’t have an effect because there won’t be electable devices on the subnet.

If for whatever reason you want to make sure a device can’t be elected, you can disable SESS in its deployed agent setting.

Managing self-electing subnet services

As elected devices with SESS on them report to the core, the core creates a list of subnets it detected and the status of ARP and WAP device discovery on those subnets. This information is available in the Self-electing subnet services tool (Tools > Configuration > Self-electing subnet services).

Use this tool to:

- Configure default SESS state for newly discovered networks
- View detected subnets
- Enable/Disable SESS on devices or networks
- View the elected device for each subnet
- Specify the Windows credentials the agentless scanner service should use

To configure the default SESS state for newly discovered networks

1. In the Self-electing subnet services tool, click the Set default state of new networks toolbar button.
2. Enable or disable the state you want for each service.

To change the desired state of an existing network

- In the Self-electing subnet services tool, right-click the network you want to change and Enable or Disable it.
To specify Windows credentials for the agentless scanner

- See this topic: "Agentless inventory scanner" (334).

Configuring Linux and UNIX device agents

You can use Ivanti® Endpoint Manager powered by Landesk to manage supported Linux/UNIX distributions. For information on supported Linux/UNIX versions and installation instructions, see the Ivanti Linux/UNIX landing page on the Ivanti User Community at https://community.landesk.com/support/community/systems/nix.

Deploying agents to non-persistent VDI images

When deploying agents to non-persistent virtual desktop interface (VDI) disk images, there are a few extra steps you must take.

The agent configuration process adds unique ID and logon history tracking registry entries for that device. In a non-persistent environment, this data will be lost when the image resets.

If you want to make sure Endpoint Manager tracks each machine in the VDI pool individually, you must delete these registry keys from the base image. Doing this allows the registry keys to be recreated when each machine in the VDI pool boots the first time and the agents load.

These are the UniqueID and logon tracking registry keys you must delete from the VDI base image.

For 64-bit VDI images:

- `HKLM\SOFTWARE\Wow6432Node\Intel\LANDesk\CommonApi\UniqueID`
- `HKLM\SOFTWARE\Wow6432Node\LANDesk\CommonApi\UniqueID`
- `HKLM\SOFTWARE\Wow6432Node\LANDesk\Inventory\LogonHistory\Logons`

For 32-bit VDI images:

- `HKLM\SOFTWARE\Intel\LANDesk\CommonApi\UniqueID`
- `HKLM\SOFTWARE\LANDesk\CommonApi\UniqueID`
- `HKLM\SOFTWARE\LANDesk\Inventory\LogonHistory\Logons`

If you’re using software usage monitoring, you must also set a UNC path where software monitor data files will be stored. If you don’t set a path, software license monitoring will store monitoring data in the registry. In a non-persistent environment, this data will be lost when the image resets.

To record software usage statistics to a network location

1. Click **Tools > Agent configuration**.
2. Double-click the agent configuration that you will use on your VDI image.
3. Click **Standard Ivanti agent > Software usage monitoring**.
4. Select **Use software monitor**.
5. Select **Record software usage statistics to a network location**.

6. Enter the UNC path information and the credentials the agents on the VDI image should use to access that UNC path.

7. Save your changes.

8. Deploy the agent configuration to your VDI base image.

9. Delete the UniqueID and logon tracking registry keys mentioned earlier in this section.

10. Save the changes to your VDI base image.

### Uninstalling device agents

Prior to Endpoint Manager 8.5, anyone could uninstall Endpoint Manager agents by running wscfg32.exe with the /u parameter. Since wscfg32.exe was in the LDLogon share, which managed devices could access, it was relatively easy for users to uninstall Endpoint Manager agents.

With Endpoint Manager 8.5 and later, the /u parameter has been removed from wscfg32.exe. 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 Endpoint Manager 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.

### Managed device help

The Agent configuration window (**Tools > Configuration > Agent configuration**) is where you customize device agent configurations. Use the Agent configuration dialog box 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 select the configuration platform.

3. Complete the **Agent configuration** dialog box as described in the following sections. Click **Help** on a page for more information.

**NOTE:** If you use the **Agent configuration** dialog box to create a new default agent configuration, be aware that all devices that are configured by WSCFG32 using login scripts will be automatically...
reconfigured with the new default configuration settings the next time a user logs in, even if their current settings match the new default settings.

The following sections describe the Agent configuration dialog box pages.

**About the Start page**

The Agent configuration dialog box's Start page contains the following options:

- **Configuration name:** This option appears above all dialog box 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:** When selected, makes this configuration the default configuration that gets installed when no other configuration is specified.

Agent components to install (Standard):

- **Standard Ivanti agent:** Installs the standard Ivanti 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 that the security scanner is automatically installed with the standard Ivanti 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. This option is required. You can’t disable it, but you can customize the components associated with it.

Security:
• **Ivanti Antivirus**: Installs the Antivirus agent on managed devices. Antivirus uses the security scanner (installed with the standard Ivanti 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 check box 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 three separate and complementary security components: Enpoint security, Ivanti 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, disk space, and overall temperature of the device.

• **Extended components**: Installs an agent that monitors system process, services, and overall performance.

Other options:

• **.NET installation**: When the agent is installed, you can select whether to install Microsoft .NET 4.0 on the managed device. This is a convenience that is useful for two new options that can be installed on devices: Portal Manager (the new version of Desktop Manager) and the Location Detection option (under Inventory settings), both of which require .NET 4.0. If you include either of these options in an agent configuration, select one of the following bundling options.

  • **Include .NET in agent installation package**: The .NET install is contained within the agent package and is always installed.

  • **If .NET is not installed, download and install**: .NET is not automatically installed. After the agent is installed, it checks to see whether the managed device already has .NET 4.0 installed. If it does not, the agent uses Vulscan.exe to download and install .NET 4.0. (Any earlier versions of .NET are not affected by this installation.)

• **Include software in inventory scan during installation**: After this configuration is installed on clients, do a full inventory scan (hardware ad software). Software scans can take a while, but you can enable this if you don’t want to wait for the inventory scanner to do one on it’s own. By default, the inventory scanner does a software scan once a day.

• **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 Ivanti agent**

All Endpoint Manager components require the standard Ivanti agent, which is installed by default on all device installations. Among other things, the standard Ivanti agent provides device discovery and manages core server/device communication.

By default, the standard agent includes the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk security scanner.

Use the Standard Ivanti agent pages to configure the Standard Ivanti agent, which includes these components and settings:

- Client connectivity
- Inventory settings
- Alerting
- Reboot settings

**Standard Ivanti agent global settings**

The Standard Ivanti agent page has two global settings you can set:

- **Never reboot:** Disable all product-related reboots. This overrides any agent install reboot settings you specify.
- **Never autofix:** Disable automatic remediation for security vulnerabilities.

These global settings override any reboot and autofix settings you make elsewhere in the product. Consider using these settings on critical devices where you want to manage reboots and autofixes manually.

**About the Client connectivity page (under Standard Ivanti agent)**

Use the **Client connectivity** page to select and apply a collection of Client connectivity agent settings that have already been specified and saved with a single unique identifier or to create a new collection of Client connectivity agent settings. Client connectivity settings are required by agent configurations.

- **Client connectivity:** Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration.
- **Edit...** Opens the **Client connectivity settings** dialog box, where you can change an existing collection of settings.
- **Configure...**: Opens the **Configure Client connectivity settings** dialog box. This dialog lists the collections of Client connectivity settings you have configured.
  - **New...**: Opens the **Client connectivity settings** dialog box, where you can create a new collection of settings.
  - **Edit...**: Opens the **Client connectivity settings** dialog box, where you can change the specified collection of settings.
  - **Copy...**: Creates a copy of the selected collection of settings and opens the **Client connectivity settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. Modify the copy of the selected settings and then rename the collection of settings with a unique identifier.
  - **Use selected**: Applies the selected settings to the agent configuration.

**About the Inventory settings page (under Standard Ivanti agent)**

Use the **Inventory settings** page to select and apply a collection of Inventory settings that have already been specified and saved with a single unique identifier or to create a new collection of Inventory settings.

- **Inventory settings**: Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration.
- **Edit...**: Opens the **Inventory settings** dialog box, where you can change an existing collection of settings.
- **Configure...**: Opens the **Configure Inventory settings** dialog box. This dialog lists the collections of Inventory settings you have configured.
  - **New...**: Opens the **Inventory settings** dialog box, where you can create a new collection of settings.
  - **Edit...**: Opens the **Inventory settings** dialog box, where you can change the specified collection of settings.
  - **Copy...**: Creates a copy of the selected collection of settings and opens the **Inventory settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  - **Use selected**: Applies the selected settings to the agent configuration.

**About the Alerting page (under Standard Ivanti 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 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 Reboot settings page (under Standard Ivanti agent)**

Use the **Reboot settings** page to select and apply a collection of reboot settings that have already been specified and saved with a single unique identifier or to create a new collection of settings.

• **Reboot settings**: Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration.

• **Edit...**: Opens the **Reboot settings** dialog box, where you can change an existing collection of settings.

• **Configure...**: Opens the **Configure Reboot settings** dialog box. This dialog lists the collections of Device reboot settings you have configured.
  
  • **New...**: Opens the **Reboot settings** dialog box, where you can create a new collection of settings.
  
  • **Edit...**: Opens the **Reboot settings** dialog box, where you can change the specified collection of settings.
  
  • **Copy...**: Creates a copy of the selected collection of settings and opens the **Reboot settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  
  • **Use selected**: Applies the selected settings to the agent configuration.

**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 box.

Customize the forms that are distributed to devices in your management domain using the form designer. For more information, see "Using custom data forms" (362).

**About the Custom data forms 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 Idlogon 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 Ivanti program folder:** The selected forms appear as items in the device's Ivanti Management folder. They aren't automatically run.

### About the Forms sent with agent page (under Custom data forms)

The Forms sent with agent page lists all defined custom data forms. Select 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 section. You can deploy the software distribution agent to devices before you set up a package server. For more information, see "About software distribution" (457).

### About the Distribution and Patch page

Use the Distribution and Patch page to select and apply a collection of Distribution and Patch settings that have already been specified and saved with a single unique identifier or to create a new collection of settings.

- **Distribution and Patch settings:** Lists the collections of settings that are available. Click an identifier in the list and then click Save to apply those settings to the agent configuration.
- **Edit...:** Opens the Distribution and Patch settings dialog box, where you can change the specified collection of settings.
Configure...: Opens the Configure Distribution and Patch settings dialog box. This dialog lists the collections of Distribution and Patch settings you have configured.

- New...: Opens the Distribution and Patch settings dialog box, where you can create a new collection of settings.
- Edit...: Opens the Distribution and Patch settings dialog box, where you can change the specified collection of settings.
- Copy...: Creates a copy of the selected collection of settings and opens the Distribution and Patch settings dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
- Use selected: Applies the selected settings to the agent configuration.

About the Portal Manager page (under Distribution and Patch)

Use the Portal manager page to select and apply a collection of Portal manager settings that have already been specified and saved with a single unique identifier or to create a new collection of settings. The options on this page are enabled if you select the Use Portal Manager option on the Software Distribution page of the agent configuration.

- Portal Manager settings: Lists the collections of settings that are available. Click an identifier in the list and then click Save to apply those settings to the agent configuration.
- Edit...: Opens the Portal manager settings dialog box, where you can change the specified collection of settings.
- Configure...: Opens the Configure portal manager settings dialog box. This dialog lists the collections of Portal Manager settings you have configured.
  - New...: Opens the Portal manager settings dialog box, where you can create a new collection of settings.
  - Edit...: Opens the Portal manager settings dialog box, where you can change the specified collection of settings.
  - Copy...: Creates a copy of the selected collection of settings and opens the Portal manager settings dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  - Use selected: Applies the selected settings to the agent configuration.

- Shortcut configuration: Select the locations where you want to add Portal Manager shortcuts on the managed device.

- Start up/shut down options: Select this option if you want Portal Manager to always open when the end user logs on. This will ensure that required policy-based tasks will run on a regular basis.

About the Ivanti Workspace page (under Distribution and Patch)

Use the Ivanti Workspace page to add a Ivanti Workspace shortcut to the Ivanti program group. For more information on Workspaces, see Workspaces.
Deploying Ivanti Security services

The security scanner (patch and compliance scanner) is installed by default with the standard Ivanti agent. However, you need to use the options on the specific Security and compliance pages 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 Endpoint Security for Endpoint Manager 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” (679).

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 the definitions of certain security types) 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.

This page contains the following options:

- **Apply custom variables settings to this configuration**: Enables custom variables and allows you to select from the Custom variables settings list.

- **Custom variable settings**: Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration. The custom variable override settings will be 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.

- **Edit...**: Opens the **Custom variables settings** dialog box, where you can change an existing collection of settings.
- **Configure...**: Opens the **Configure custom variables settings** dialog box. This dialog lists the collections of Custom variables settings you have configured.
  - **New...**: Opens the **Custom variables settings** dialog box, where you can create a new collection of settings.
  - **Edit...**: Opens the **Custom variables settings** dialog box, where you can change an existing collection of settings.
  - **Copy**: Creates a copy of the selected collection of settings and opens the **Custom variables settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  - **Use selected**: Applies the selected settings to the agent configuration.

**About the Ivanti 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 select the **Ivanti Antivirus** agent's check box 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.

If another antivirus product is installed on target devices, it will be removed automatically during Ivanti Antivirus agent configuration.

This page contains the following options:

- **Ivanti 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 list. Click **Configure** to open the **Ivanti Antivirus settings** dialog box, where you can create a new setting.

- **Reboot settings**: Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration.

**Self-contained agent package or agent push settings**

Use these options to configure how Ivanti antivirus will be installed on managed devices. The option you choose affects how large the antivirus installation package download will be. You can choose from the following options:
- Include both 32-bit and 64-bit Antivirus setup files
- Include only 32-bit Antivirus setup files
- Include only 64-bit Antivirus setup files
- Exclude Antivirus setup files
- Include the latest virus definitions approved for distribution

**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).

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 list to apply it to the configuration you’re creating.

- **Configure...**: Opens the **Configure custom variables settings** dialog box. This dialog lists the collections of Windows Firewall settings you have configured.
  - **New...**: Opens the **Windows Firewall settings** dialog box, where you can create a new collection of settings.
  - **Copy...**: Creates a copy of the selected collection of settings and opens the **Windows Firewall settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  - **Use selected**: Applies the selected settings to the agent configuration.

**About the Endpoint Security page**

Use this page to select an Endpoint Security setting for managed devices with this agent configuration. Endpoint Security includes three components: Endpoint security, Ivanti Firewall, and Device Control.

In order to select an Endpoint Security setting, you must first select the Endpoint Security agent check box on the Start page.

This page contains the following options:

- **Machine configuration**: Specifies the Endpoint Security settings for managed devices with this agent configuration. Endpoint Security settings determine 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 Endpoint security, Ivanti Firewall, and Device Control.
• **Edit...:** Opens the **Endpoint security settings** dialog box, where you can change an existing collection of settings.

• **Configure...:** Opens the **Configure Endpoint security settings** dialog box. This dialog lists the collections of Endpoint security settings you have configured.
  • **New...:** Opens the **Endpoint security settings** dialog box, where you can create a new collection of settings.
  • **Edit...:** Opens the **Endpoint security settings** dialog box, where you can change an existing collection of settings.
  • **Copy...:** Creates a copy of the selected collection of settings and opens the **Endpoint security settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  • **Use selected:** Applies the selected settings to the agent configuration.

**About the Agent Watcher page**

Use this page to enable and configure the Ivanti Agent Watcher utility on devices with this agent configuration.

Agent Watcher allows you to actively monitor devices for selected Ivanti 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 can’t 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, how often, and whether the utility remains resident on the device. Select a setting from the list.
• **Configure...**: Opens the **Settings List** dialog box. This dialog lists the collections of Agent watcher settings you have configured.
  
  • **New...**: Opens the **Agent watcher settings** dialog box, where you can create a new collection of settings.
  
  • **Edit...**: Opens the **Agent watcher settings** dialog box, where you can change an existing collection of settings.
  
  • **Copy...**: Creates a copy of the selected collection of settings and opens the **Agent watcher settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  
  • **Use selected**: Applies the selected settings to the agent configuration.

**About the Other security page**

Use this page to enable and configure other security settings on managed devices with this agent configuration. Other security settings include the real-time application blocker for unauthorized applications and real-time spyware blocking.

• **Apply other security settings to this configuration**: Selecting this allows you to select an **Other security settings** profile.

• **Other security settings**: Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration.

• **Edit...**: Opens the **Other security settings** dialog box, where you can change an existing collection of settings.

• **Configure...**: Opens the **Configure other security settings** dialog box. This dialog lists the collections of other security settings you have configured.

  • **New...**: Opens the **Other security settings** dialog box, where you can create a new collection of settings.

  • **Edit...**: Opens the **Other security settings** dialog box, where you can change an existing collection of settings.

  • **Copy...**: Creates a copy of the selected collection of settings and opens the **Other security settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.

  • **Use selected**: Applies the selected settings to the agent configuration.

**About the Remote control page**

Use the Remote control page to select and configure remote control settings profiles. You can also change the driver settings here.

• **Remote control settings**: Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration.
• **Configure...:** Opens the **Configure remote control settings** dialog box. This dialog lists the collections of Remote control settings you have configured.
  - **New...:** Opens the **Remote control settings** dialog box, where you can create a new collection of settings.
  - **Edit...:** Opens the **Remote control settings** dialog box, where you can change an existing collection of settings.
  - **Copy...:** Creates a copy of the selected collection of settings and opens the **Remote control settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  - **Use selected:** Applies the selected settings to the agent configuration.

• **Agent settings:**
  - **Use mirror driver:** Selected by default, this option uses the remote control mirror driver on devices for faster remote control performance.
  - **Use screen blanking driver:** Selected by default, this option uses a special driver that can tell the target device’s display driver to turn off the monitor. When active, this driver filters commands going to the real display driver to prevent them from turning the monitor back on. Remote control operators can turn screen blanking on or off from the remote control viewer application. If you’re having compatibility problems with this driver, you can clear the check box to use a more compatible but possibly less effective mode of screen blanking. If you don’t use the screen blanking driver, the alternative mode of screen blanking may cause some screen flicker on the target device during remote control. This option requires the mirror driver.

**About the Extended device discovery page**

Extended device discovery is an extension of the Unmanaged device discovery tool. It 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.

Use this page to enable and configure extended device discovery on managed devices with this agent configuration.

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 Ivanti agent installed. If the Ivanti 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 on 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.

- **ARP discovery settings:**
  - **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 list to apply it to the configuration you’re creating.
  
  - **Configure...:** Opens the **ARP Discovery Settings** dialog box. This dialog lists the collections of ARP Discovery settings you have configured.
    
    - **New...:** Opens the **Configure ARP Discovery Settings** dialog box, where you can create a new collection of settings.
    
    - **Edit...:** Opens the **Configure ARP Discovery Settings** dialog box, where you can change an existing collection of settings.
    
    - **Copy...:** Creates a copy of the selected collection of settings and opens the **Configure ARP Discovery Settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
    
    - **Use selected:** Applies the selected settings to the agent configuration.

- **Use Wireless Access Point discovery (WAP):** Enables extended device discovery using the wireless application protocol (WAP) discovery method on devices with this agent configuration.
• **WAP discovery settings:**
  
  • **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.

  • **Configure...:** Opens the **WAP Discovery Settings** dialog box. This dialog lists the collections of WAP Discovery settings you have configured.
    
    - **New....:** Opens the **Configure WAP Discovery Settings** dialog box, where you can create a new collection of settings.
    
    - **Edit....:** Opens the **Configure WAP Discovery Settings** dialog box, where you can change an existing collection of settings.
    
    - **Copy....:** Creates a copy of the selected collection of settings and opens the **Configure WAP Discovery Settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
    
    - **Use selected:** Applies the selected settings to the agent configuration.

  • **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.

**About the Power management page**

Ivanti Power Management functionality allows administrators to centrally control end-node power consumption by facilitating the creation, financial evaluation, and deployment of power management policies.

Use the Power Management page to select the power policy to be distributed out to the client device. 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:
- **Use power policy on client**: Enables power management in this agent configuration.
- **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.
  - **Configure...**: Opens the **Configure power management settings** dialog box. This dialog lists the collections of Power management settings you have configured.
    - **New...**: Opens the **Power management settings** dialog box, where you can create a new collection of settings.
    - **Edit...**: Opens the **Power management settings** dialog box, where you can change an existing collection of settings.
    - **Copy...**: Creates a copy of the selected collection of settings and opens the **Power management settings** dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  - **Use selected**: Applies the selected settings to the agent configuration.

**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.

### About the Tenant page

Use this page to manage tenants associated with an agent configuration. Tenant management is an add-on to Ivanti® Endpoint Manager powered by Landesk that is available for purchase separately. Tenant management allows you to compartmentalize managed devices and configurations by company. For more information, see "Tenant management overview" (982).

This page contains the following options:

- **Assign a Tenant to this configuration**: Select this option if you want to assign a tenant.
- **Choose a Tenant**: Select the tenant you want from the list of tenants that you’ve configured.

### About the Adaptive settings page

Use this page to manage adaptive settings. Adaptive settings allow agent settings to dynamically change on a device based on location (geofencing) or IP address. For more information, see "Adaptive settings" (159).

This page contains the following options:

- **Apply adaptive settings to this configuration**:
- **Adaptive settings**: Lists the collections of settings that are available. Click an identifier in the list, then click **Save** to apply those settings to the agent configuration.
- **Edit...**: Opens the Adaptive settings dialog box, where you can change an existing collection of settings.
- **Configure...**: Opens the Configure adaptive settings dialog box. This dialog lists the collections of adaptive settings you have configured.
  - **New...**: Opens the Adaptive settings dialog box, where you can create a new collection of settings.
  - **Edit...**: Opens the Adaptive settings dialog box, where you can change an existing collection of settings.
  - **Copy...**: Creates a copy of the selected collection of settings and opens the Adaptive settings dialog box. This is helpful when you want to create a new collection of settings that are similar to a collection you have already configured.
  - **Use selected**: Applies the selected settings to the agent configuration.

### Deploying agent configurations 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” (121).

**About the Start page (under Linux/UNIX 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 Ivanti agent** and **Software distribution**: These options install by default and you can’t disable them.
- **Ivanti vulnerability scanner**: Installs the Linux version of the vulnerability scanner.
- **Defaults**: Resets the options to the default (disables the Ivanti vulnerability scanner option).

**About the Standard Ivanti agent page (under Linux/UNIX agent configuration)**

The Linux Agent configuration’s Standard Ivanti 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" (140).
- **Core address**: This needs to be a resolvable name or IP address that managed devices will use to communicate with the core server.
- **NOTE**: The other options on this page are dimmed and don’t apply to Linux agent configurations.

**About the Inventory settings page (Under Linux/UNIX 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 is reflected in the ldiscan_daily.xml job file on installation, which the Ivanti Agent Scheduler processes.

**About the Agent status options dialog box**

Use the Agent status options dialog box (**Configure > Agent status options**) to configure the following agent discovery options.

- **Gather agent status**:
  - **Never**: Never gather the agent status. Use this option if you have a lot of unreliable devices or a slow network link.
  - **For selected visible items only**: Specifies that a device's agent status is updated as the device is selected in the network view. Consider using this option and disabling auto-refresh if the ratio of available devices to unavailable devices is around 50/50. Using this option and disabling auto-refresh is also good when you want to reduce the amount of network traffic generated by the console.
  - **For all visible items**: 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. This option generates the most network traffic.
  - **Refresh every < > minutes**: Indicates whether agent status is automatically updated at the interval you select. To enable this option, select the box beside **Refresh**. This option is disabled by default, and the refresh interval only applies if the option’s box is checked. If you enable this, consider using the default 5 minute interval or longer to reduce the amount of network traffic.

**Agent security and trusted certificates**

Endpoint Manager uses a certificate-based authentication model. Device agents authenticate to authorized core servers, preventing unauthorized cores from accessing clients. Each core server has a unique certificate and private key that Endpoint Manager 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 folder that contains many different certificates. The name is a hash (checksum) of the certificate’s 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 folder. It will display the hash associated with a certificate using the following command line:

```bash
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 folder and needs to be there by default. `<keyname>` is the certificate name you provided during Endpoint Manager 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 folder 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.

### Managed device certificates

With Ivanti® Endpoint Manager powered by Landesk version 2016, agent installation automatically generates a certificate on each managed device. These certificates aren’t valid on the core until they’re approved (Configure > Client access). Unapproved devices won’t be able to communicate through a Cloud Services Appliance.

Ivanti® Endpoint Manager powered by Landesk version 2016 also introduces a new client certificate-based security model for Windows-based devices. When this security model is active, only devices with valid certificates can decrypt secure core server data.

Because this security model isn’t compatible with agents from older Endpoint Manager (9.x) versions, it isn’t enabled by default. However, Ivanti strongly recommends that you enable this security model once your managed devices are all using version 2016 or later agents. For more information, see "Client certificate-based security" (144).

On managed devices, certificates are stored here:

- C:\Program Files (x86)\LANDesk\Shared Files\cbaroot\broker

There are three files:

- **broker.key**: Private key. This should be protected. Only administrators have rights to it.
- **broker.cs**: Certificate signing request sent to the core to be signed.
- **broker.crt**: Public key in X509 certificate format.
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 Idlogon folder. 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 “Copy certificate/private key files among core servers” (143).

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 folder. Once the trusted certificate is in this folder, you can select it within the device setup dialog’s **Common base agent** page. Device setup copies keys to this folder 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 folder 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 folder of the core server to a device. To use this, replace “d960e680” with the hash value for the trusted certificate you want to deploy.

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

### Copy 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.

**NOTE:** *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 one 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 Endpoint Manager device.
Client certificate-based security

Ivanti® Endpoint Manager powered by Landesk 2016 introduces a new client certificate-based security model for Windows-based devices. When this security model is active, only devices with valid certificates can decrypt secure core server data.

Because this security model isn’t compatible with agents from older Endpoint Manager (9.x) versions, it isn’t enabled by default. However, Ivanti strongly recommends that you enable this security model once your managed devices are all using version 2016 or later agents.

If Endpoint Manager version 2016 or later is the first installation of Endpoint Manager in your network environment, you can safely enable client certificate-based security because older agent versions won’t be present.

If you have devices with older agent versions and you enable client certificate-based security, those devices won’t be able to decrypt secure data from the core server and many agent features won’t work correctly.

Once client certificate-based security is enabled, it can’t be disabled.

Follow these steps to enable client certificate-based security

1. Assess readiness and update devices running older (9.x) agent versions
2. Approve client certificates
3. Enable client certificate-based security on the core server
4. Re-encrypt core server component passwords that clients use
5. (If you use core synchronization): Copy new encryption keys to other core servers

Step 1: Make sure managed Windows devices are ready

The Security settings dialog box (Configure > Security) includes a chart showing the certificate-based authentication success rate for managed devices. When managed devices attempt a secure connection to the core server or when the security scanner (vulscan.exe) runs, the connection results are saved to the device inventory. This happens even if the new security model isn’t enabled yet.

Devices not in an Authentication succeeded state won’t be fully manageable after the new security model is enabled. Usually it’s older device agents causing devices to be in other states. Don’t enable the new security model until your devices are ready for it.
The chart in this dialog box summarizes connection attempt results:

- **Authentication succeeded**: The device has version 2016 agents, is securely connected, and is ready for the new security model. Ideally all devices are here.

- **No authentication info**: The device hasn’t attempted a secure connection or the security scanner hasn’t reported connection results back to the core yet. Note that if your core server doesn’t have agents installed on it, the core will appear in this list and that’s OK.

- **Authentication failed**: The device tried to authenticate and couldn’t for some reason. Usually this happens because the device hasn’t received client certificate approval (Configure > Manage client access), as discussed in the next section.

- **Client agents must upgrade**: The device can’t authenticate because it’s running older (9.x) agents.

Double-click items in the chart to view associated devices in the network view. The dynamically generated query for an item you double-clicked appears under Queries > My queries > Chart-generated queries. You can use this view to more easily target or troubleshoot devices.

More connection details may be available in the device inventory under Ivanti Management > Client certificate-based security > Authentication status.
Step 2: Approve client certificates

Endpoint Manager 2016 agent installation also automatically generates client security certificates. Previously this was something administrators had to do manually after agent installation. When a device with a security certificate first communicates with the core, the core adds an "unapproved" entry for that device in the Client access dialog box's Manage client certificates tab. Administrators can then approve or block core access for those certificates.

When client certificate-based security isn’t enabled, unapproved devices function normally but they can’t communicate through a Cloud Services Appliance (CSA) until they are approved.

When client certificate-based security is enabled, unapproved devices won’t be able to decrypt secure data from the core server and many agent features won’t work correctly.

When you approve a device’s certificate, the core won’t get an authentication status update from that device until it runs a security scan, triggering a new authentication check.

You can view the Certificate approval status chart for more information on approval progress and status (Tools > Security and Compliance > Security activity).

To manage client certificate approvals
1. Click Configure > Manage client access.
2. Select the valid unapproved devices and click Approve selected.
3. Click Close.

Step 3: Enable client certificate-based security on the core server

If you’ve made sure your environment is ready for client certificate-based security and you’re ready to enable it, do the following.

To enable client certificate-based security
1. Click Configure > Security.
2. View the chart and read the warnings. Make sure you understand and are ready to upgrade.
3. Click the Client certificate-based security radio button so it’s enabled.
4. If you want to save authentication and decryption results, select the choices you want.
5. Click Save.
6. Carefully read the security settings warning dialog box that comes up.
7. Click **OK** to activate client certificate-based security. Click **Cancel** if you aren’t sure you’re ready. Once activated this can’t be disabled.

**Step 4: Re-encrypt core server component passwords**

When you enable client certificate-based authentication, the core server creates a new and unique encryption key that it will use for encrypting new data. Data that hasn’t changed since you enabled the new security model will still be encrypted the old way. To re-encrypt important core server component passwords that are shared with managed devices, change them after enabling the new security model.

**To update preferred server passwords**

1. Click **Tools > Distribution > Content replication/Preferred servers**.
2. In the properties for each preferred server, change the password.

**To update credentials stored in software packages**

1. Click **Tools > Distribution > Distribution packages**.
2. On the toolbar, click **Bulk package credentials update**.
3. Enter the **Domain\User** and **Password** information.
4. Click **Update**.

**To update distribution and patch agent passwords**

1. Click **Tools > Configuration > Agent settings**.
2. In the tree, click **Distribution and Patch**.
3. Edit each distribution and patch agent setting, and on the MSI information page update the MSI and run-as credentials.
Step 5 (if you use core synchronization): Copy new encryption keys to other core servers

If the core server you’re configuring uses core synchronization, you’ll see an additional warning about needing to copy encryption keys to those other core servers. Once data is encrypted with the new encryption keys, target core servers won’t be able to decrypt that data until you do this.

Securely copy the .xml encryption keys from this folder to the same folder on your target cores:

- C:\Program Files\LANDesk\Shared Files\keys\Compatible

Since these are encryption keys, treat them carefully. Only the core server should be able to access them.
Agent settings

Agent Settings overview

Agent Settings control how Ivanti® Endpoint Manager powered by Landesk services and other components operate on managed devices. These components 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.

If a component is installed on a managed device, changes to that component’s settings don’t require redeployment of the whole agent. Settings are stored as XML files and the managed device only needs an updated XML file to reconfigure how an installed component operates. Changes to a component setting are propagated to all devices with that setting installed automatically.

Use agent configurations to initially deploy or change installed Endpoint Manager components. Use agent settings to modify how installed Endpoint Manager components operate.
Create change settings tasks

Components in an agent configuration require corresponding settings profiles. Ivanti® Endpoint Manager powered by Landesk ships with default settings profiles for all components. You can use the default component settings profile or you can create your own. If you modify a component setting profile that has been deployed to managed devices, those changes are propagated automatically the next time a device using that settings profile runs the vulnerability scanner.

You can use a change settings task to change a component setting to a different settings profile. The Agent settings tool provides a way to do this without having to redeploy an entirely new and complete agent configuration. When you create a change settings task, changed settings are sent to the device in XML format and the changes take effect without requiring a reboot or any other changes to agent files.

Ivanti® Endpoint Manager powered by Landesk 9.6 greatly improved this feature. Almost all of the component preferences that were stored in agent configurations have now been moved to agent settings. Use an agent configuration for your initial agent deployment, and then use agent settings to manage future component preference changes.

Note that agent settings work only for components included in a device’s agent configuration. If you want to add or remove agent components, you will have to deploy a new agent configuration from Tools > Configuration > Agent configuration.

To create a change settings task

1. Click Tools > Configuration > Agent settings.
2. In the toolbar, click the Create a task toolbar button and click Change settings.

Change settings...
- Install/Update security components...
- Remove security components...
- LANDESK Antivirus task...
- Security scan...
- Compliance scan...
3. The **Change settings task** dialog box appears.

![Change settings task dialog box](image)

4. Next to the component you want to change, select the setting you want to apply. Clicking **Edit** edits the selected setting. Clicking **Configure** lets you manage that component's settings.

5. You can configure the task targeting and scheduling options immediately on the rest of the dialog box pages or you can click **Save** and do it later in the Scheduled tasks window.

**Create a task to install or update security components**

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 > Configuration > Agent Settings.
2. Click the Create a task toolbar button, and then click Install/Update security components.
3. The Install/Update security components task dialog box appears.

4. Enter a name for the task.

5. Select the component you want to install. You can create new settings or edit existing settings by clicking Configure.

6. If you want to display the installation progress in the security scanner dialog on targeted devices, select the Show progress dialog on client option.

7. Select a Scan and repair setting from the list to apply its reboot configuration (only) to the agent configuration you’re creating. You can create new settings or edit 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 existing Scan and repair settings that already includes the reboot configuration you want, or you can create brand new Scan and repair settings specifically for your agent deployment.
8. You can configure the task targeting and scheduling options now on the rest of the dialog box pages, or you can click **Save** and do it later in the Scheduled tasks window.

**Create a task to remove security components**

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 > Configuration > Agent Settings**.
2. Click the **Create a task** toolbar button, and then click **Remove security components**.
3. The Remove security components task dialog box appears.

4. Enter a name for the task.

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 setting from the available list to apply its reboot configuration to the task you’re creating. You can create new settings or edit 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. You can configure the task targeting and scheduling options now on the rest of the dialog box pages, or you can click **Save** and do it later in the Scheduled tasks window.
Configure Windows Firewall settings

The Agent Settings tool also lets you create, configure, and deploy Windows Firewall settings to manage the Windows Firewall on target devices.

To create Windows Firewall settings

1. Click **Tools > Configuration > Agent Settings**.
2. Right-click **Security > Windows Firewall**, click **New**, select the desired Windows platform, and then click **OK**.

Once configured, you can deploy settings to target devices with an installation or update task, or a change settings task.
Windows Firewall help

About the Create Windows Firewall settings dialog box

Use this dialog box 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 and later

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 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

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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 and later): General rules page**

Use this page to configure firewall general rules.

**About the Windows Firewall (Vista and later): Inbound rules**

Use this page to configure firewall inbound rules.

**About the Windows Firewall (Vista and later): Outbound rules**

Use this page to configure firewall outbound rules.

**Generate security authorization codes**

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 appears 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. This allows them to perform the action on a temporary basis.

**To generate an authorization code**

1. In the Agent Settings tool, click the Configure 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 wants to perform.
5. Give the new authorization code to the end user. The user enters that authorization code when prompted in order to perform the blocked operation.

**CAUTION: 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 Application Control has been disabled regardless of the actual action taken by the user. This
Adaptive settings

Adaptive settings allow agent settings to dynamically change on a device based on location (geofencing) or IP address. This is mainly oriented towards mobile devices and laptops. For example, you could have one set of agent settings while a device is connected to the corporate network, but when the device connects to an external network, the agent settings could be more restrictive.

IP address adaptive settings work with Windows devices. Geofencing uses the Windows 8 and newer location API and only works with devices running Windows 8 and newer.

Enabling adaptive settings will cause .NET4 to be installed with the agent.

Creating adaptive settings

An adaptive setting has three parts:

1. **Trigger**: The geofence coordinates and range, or the starting and ending IP address range.
2. **Rule**: The combination of a trigger and the agent setting overrides that trigger activates.
3. **Adaptive setting**: The list of rules you want monitored, ordered by priority. This is what you deploy to devices in an agent configuration.

Follow these steps to get started with adaptive settings.

1. Create a trigger
2. Create a rule
3. Create an adaptive setting
4. In an agent configuration, enable adaptive settings and select an adaptive setting
5. Deploy the agent configuration you modified

Change settings tasks can't be used for the initial deployment of adaptive settings. You must first deploy adaptive settings with an agent configuration. If you later want to change the adaptive setting a device's agent configuration references, you can then use a change settings task.

Adaptive settings take advantage of Ivanti agent behavior technology. Once you deploy an adaptive setting to a device, any subsequent changes to the adaptive setting those devices are using will be automatically distributed to affected devices. You don’t need to schedule an additional agent deployment or a change settings task to update a deployed adaptive setting.

Adaptive setting triggers

There are two adaptive setting trigger types:

- Geofence (requires Windows 8 and newer and a device with a GPS)
• IP address range (works with any Windows device)

For geofencing, the target radius circle defaults to 10 meters. Increase the **Radius** if you want it to include a corporate campus, city, and so on.

The geofencing minimum device accuracy determines how accurate the GPS reading must be for the trigger to activate. If the GPS-reported accuracy exceeds the value you specify, the trigger won’t activate.
The IP address range **Verify core existence on the network** option can help prevent network spoofing by making sure the Ivanti® Endpoint Manager powered by Landesk core server is visible to the device. Don’t use this option with IP address ranges that won’t have access the core server.

**To configure a geofence adaptive setting trigger**

1. Click **Tools > Configuration > Agent settings**.
2. In the Agent settings window toolbar, click the **Configure settings** button (ioms) and click **Edit adaptive settings rules**.
3. Click **New**.
4. Click **New** beside the **Select trigger** list.
5. Enter a **Trigger name**.
6. Select the **Geofence** trigger type.
7. Click and drag the map so the red cross-hair is over the location you want to geofence. Use the scroll bars to zoom in and out.
8. Adjust the **Radius** and **Minimum device accuracy**. The circle around the red cross-hair indicates the covered area.
9. Click **Save**.

**Adaptive settings rules**

An adaptive settings rule associates a trigger with one or more agent settings to override when the trigger activates, along with additional one-time actions, such as locking the screen.
To create an adaptive setting rule

1. Click **Tools > Configuration > Agent settings**.
2. In the Agent settings window toolbar, click the **Configure settings** button (𒐙) and click **Edit adaptive settings rules**.
3. Click **New**.
4. Enter a **Rule name**.
5. Select an existing trigger or click **New** and configure a new trigger. For more information, see the next section.
6. In the settings list, select the agent setting you want to use for each type.
7. Select any one-time actions that you want to run for this rule. For more information, see “Adaptive settings one time actions” (164).

8. Click Save.

Creating an adaptive setting

An adaptive setting is a list of one or more adaptive settings rules ordered by priority. In the adaptive settings agent configuration, you can select multiple rules from a list of available rules. The agent on the managed device will check the triggers for each rule in the selected rules list, starting at the top. The first rule the agent encounters with a matching trigger will be applied and rule processing stops. Only one rule can be active at a time. If no rules are triggered, the default settings specified in the agent configuration page will be applied.

In an adaptive setting you can set the **Check GPS location every** interval. The default is two minutes. Frequent checks will reduce device battery life.
To create an adaptive setting

1. Click Tools > Configuration > Agent settings.
2. In the Agent settings tree, right-click Adaptive settings and click New.
3. In the Adaptive settings dialog box, move the rules you want applied from the Available rules list to the Selected rules list. Click Move up and Move down to change the order if necessary.
4. If no rules apply, you can use the default agent configuration settings (in other words, don’t change anything), or you can specify a specific rule to apply.
5. If you want, select Lock windows session if location services are disabled. This locks the device if someone turns on airplane mode, for example.
6. Click Save.

Adaptive settings one time actions

Adaptive settings rules can have one-time actions that execute when the rule activates. For example, you could use the Lock windows session action when the device leaves your office building.

You can choose from the following one time actions:

- **Apply HP's recommended locked-down security BIOS settings**: This only works on HP devices. You’ll need to provide the BIOS password.
- **Lock Windows session**: Locks the session so the user has to log back in. This can help prevent unauthorized access when the device leaves a secure area.
- **Run security scan**: Runs the security scan that you select.

Applying adaptive settings to agent configurations

Once you have configured an adaptive setting you need to create or modify an agent configuration to use adaptive settings.

**To enable adaptive settings:**

1. Click Tools > Configuration > Agent Configuration.
2. Edit or create a new Windows agent configuration.
3. In the list on the left, click Adaptive settings.
4. Select **Apply adaptive settings to this configuration**. Note that this will cause .NET to be installed on the device.
5. Select an adaptive setting to be deployed with this agent configuration.
6. Click Save.
7. Deploy the agent configuration.
Available agent settings

Below is a list of configurable agent settings. Clicking one will take you to the help topic for that agent setting.

- "Agent settings: Adaptive settings" on page 187
- "Agent settings: Agent health" on page 189
- "Agent settings: Agent watcher" on page 192
Skin/Formats/CrossReferencePrintFormat("Agent settings: Ivanti Antivirus

Ivanti Antivirus features are accessed from the Agent Settings tool window (Tools > Security and Compliance > Agent Settings). In the Agent settings window, right-click Ivanti Antivirus in the Security folder, then click New...Antivirus allows you to 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 Ivanti Antivirus introduces this complementary security management tool, which is a component of both Ivanti® Endpoint Manager powered by Landesk and Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk. 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 help topics that describe the Antivirus Settings dialog. From the console interface, access these topics by clicking the Help button on each dialog box. About the Ivanti Antivirus General page Use this page to configure Ivanti Antivirus scanner settings on target devices. This page contains the following options: Name: Identifies the antivirus settings with a unique name. This name will appear in the Agent settings list in the console and in the Antivirus scan task dialog box. Protection: File Antivirus: Enables real-time scanning of files on target devices. Mail Antivirus: Enables real-time email scanning on target devices. Real-time email scanning continuously monitors incoming and outgoing messages, checking for viruses in both the body of the message and any attached files and messages. Any detected viruses are removed. Web Antivirus: Enables real-time scanning of web traffic, website URLs, and links on target devices. IM Antivirus: Enables real-time scanning of instant messages on target devices. Network Attack Blocker: Enables the Network Attack Blocker that detects and adds attacking computers to the list of blocked devices for a specified period of time. System Watcher: Enables the System Watcher utility that monitors application activity on target devices. User interface: Show Ivanti Antivirus icon in system tray: Makes the Ivanti 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. Enable database out-of-date and obsolete warning messages: Allows Ivanti Antivirus to display warning messages when the database is out-of-date or obsolete. Specifies the number of days for each status. Do not send Ivanti Antivirus reboot status: Select this option if you do not want Ivanti Antivirus to send the reboot status to the core. By default, Ivanti Antivirus sends a status update about whether or not it requires a reboot to complete an install or update. The status will appear in Security activity | Ivanti Antivirus | Activity and the core will set 'Reboot Needed' inventory information under Computer | Ivanti Management. Set As Default: Establishes the settings on all of the pages of the Ivanti Antivirus dialog box as the default settings. The name you entered will appear in the console with the default icon next to it. You cannot delete a setting that is marked as default. When you create a new agent configuration, those settings will be selected by default. Unless an antivirus scan task has specific antivirus settings associated with it, Ivanti Antivirus will use the default settings during scan and definition file update tasks. About the
Ivanti Antivirus Permissions page

Use this page to configure Ivanti Antivirus permissions settings on target devices. This page contains the following options:

- Allow user to disable protection components for up to: Specifies the period of time during which the user can turn off the protection components listed on the Protection page.
- Allow user to update definitions: Allows the user to update antivirus definition files.
- Allow user to restore objects: Allows the user to restore objects quarantined backed up objects.
- Allow user to change settings: Allows the user to configure settings and edit tasks.
- Allow user to schedule scans: Allows the user to schedule scans.
- Allow user to exclude objects from scanning: Allows the user to exclude objects from scanning.
- Allow users to add Web URLs: Allows the user to add Web URLs.
- Allow users to configure exclusions in Network Attack Blocker: Allows the user to list IP addresses that Ivanti Antivirus will trust. Ivanti Antivirus will not block network attacks from these IP addresses but will still log information about such attacks.

About the Ivanti Antivirus Protection page

Use this page to configure Ivanti Antivirus protection settings on target devices. This page contains the following options:

- Start Ivanti Antivirus on computer startup: Enables the automatic start of Ivanti Antivirus after the operating system loads, protecting the computer during the entire session. This option is selected by default. If you disable this option, Ivanti Antivirus will not start until the user starts it manually and the user data may be exposed to threats.
- Enable Advanced Disinfection Technology: If you select this option, when Ivanti Antivirus detects malicious activity in the operating system, it displays a pop-up message that suggests performing a special advanced disinfection procedure. After the user approves this procedure, Ivanti Antivirus neutralizes the threat. After completing the advanced disinfection procedure, Ivanti Antivirus restarts the computer. The advanced disinfection technology uses considerable computing resources, which may slow down other applications. If you leave this option unselected, which is the default setting, when Ivanti Antivirus detects malicious activity in the operating system, it carries out the disinfection procedure according to the current application settings. No computer restart is performed after Ivanti Antivirus neutralizes the threat.
- Threats: Specifies the objects for detection.
- Malware: By default, Ivanti Antivirus scans for viruses, worms, and Trojan programs. On this tab, you can specify whether to scan for malicious tools. Adware, auto-dialers, other programs: Specifies whether to control adware and legitimate applications that may be exploited by intruders to harm the computer or user data. Select Other to protect against objects such as Internet chat clients, downloaders, monitoring programs, and remote administration applications.
- Compressed files: Specifies whether to scan for packed files that may cause harm and multi-packed objects.
- Exclusions: Specifies files, folders, or extensions for Ivanti Antivirus to exclude from the scan. Ivanti Antivirus will check the \LDClient and \Shared files folders for .exe files. If those files are signed by Ivanti, Antivirus automatically excludes them from all scans and adds them to the Trusted application list.
- Realtime: Specifies files, folders, or extensions to exclude from the scan in realtime. Click Add... to open the Add excluded path dialog, where you can specify file type and browse to the objects you want to exclude.
- Virus Scan: Specifies files, folders, or extensions to exclude from the virus scan. Click Add... to open the Add excluded path dialog, where you can specify file type and browse to the object(s) you want to exclude.
- Monitored ports: Specifies which ports to monitor.
- Monitor all network ports: The protection components monitor data streams that are transmitted via any open network ports of the computer.
- Monitor only selected ports: The protection components monitor only user-
specified ports. Whatever is listed in network ports gets included and will be checked on the client. This network port monitoring mode is selected by default. Click Settings to open the Network ports dialog box, where you can create a list of monitored network ports and a list of applications. Network ports list: This list contains network ports that are normally used for transmission of email and network traffic. Select a port for Ivanti Antivirus to monitor network traffic that passes through this network port via any network protocol. Click Add... to enter a new port number and description. Monitor all ports for specified applications: Specifies whether all network ports are monitored for applications that are specified in the Applications list. Applications list: This list contains applications that have network ports which Ivanti Antivirus will monitor. For each application, the list of applications specifies the path to its corresponding executable file. Click Add... to select an application from the database or browse for an application from the file location. About the Ivanti Antivirus Protection: File Antivirus page Use this page to configure the way File Antivirus works with Ivanti Antivirus on target devices. This page contains the following options: Enable File antivirus: Starts File Antivirus with Ivanti Antivirus. File Antivirus continuously remains active in computer memory and scans all files that are opened, saved, or started on the computer. By default, File Antivirus is enabled and configured with the recommended settings. Security Level: Specifies one of the three file security levels (High, Recommended, or Low). You can configure a custom file security level by selecting settings on the General, Performance, and Additional tabs. High: File Antivirus takes the strictest control of all files that are opened, saved, and started. File Antivirus scans all file types on all hard drives, network drives, and removable storage media of the computer. It also scans archives, installer packages, and embedded OLE objects. Recommended: File Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer. It also scans embedded OLE objects. With the Recommended setting, File Antivirus doesn’t scan archives or installer packages. Low: Ensures the maximum scanning speed. With this setting, File Antivirus scans only files with specified extensions on all hard drives, network drives, and removable storage media of the computer. File Antivirus won’t scan compound files. If you choose to create a custom security level, be sure to consider the working conditions and current situation. General: Specifies whether Antivirus scans by file format, extension, or both. File types: There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then regardless of the extension, File Antivirus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware. Protection scope: Specifies which drives to scan. Performance: Specifies the scan methods, whether to only scan new files, and how to handle compound files. Heuristic analysis: This technology detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as probably infected. Scan new and changed files only: Enables File Antivirus to scan only new files and files that have been modified since the previous scan. Scan
archives: Enables File Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.

Scan installation: Enables File Antivirus to scan installation packages.

Scan embedded OLE objects: Enables File Antivirus to scan files that are embedded in another file, such as Microsoft ® Office Excel ® spreadsheets, macros that are embedded in Microsoft ® Office Word ® files, or email attachments.

Additional...: Opens the Compound files dialog box, where you can specify whether to unpack compound files in the background and set a size limit for compound files.

Additional: Specifies the mode and technology File Antivirus will use and when it will pause.

Scan mode: The default scan mode is Smart mode, in which File Antivirus scans files by analyzing operations performed with a file by the user, an application, or the operating system. In the On access and modification mode, File Antivirus scans files when the user, an application, or the operating system attempts to open or modify the files. In the On access mode, File Antivirus scans files only when the user, an application, or the operating system attempts to open the files. In the On execution mode, File Antivirus scans files only when the user, an application, or the operating system attempts to run files.

Scan technologies: Specifies the scan technologies that File Antivirus uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. This speeds up scanning of objects that are from various file systems and operating systems.

Pause task: Specifies when to pause File Antivirus. The By schedule option allows pausing File Antivirus for a specified time. This feature can decrease the load on the operating system. Click Schedule... to open the Pausing the task window. In this window, you can specify the time interval for which File Antivirus is paused. The At application startup option pauses File Antivirus while the user works with applications that require significant resources from the operating system. This option is not selected by default.

Click Select... to open the Applications window, where you can create a list of applications that pause File Antivirus when they are running.

Action: Specifies the action that File Antivirus performs if infected files are detected. Before attempting to disinfect or delete an infected file, File Antivirus creates a backup copy for subsequent restoration or disinfection.

Select action automatically: Enables File Antivirus to perform the default action that is specified by Ivanti. This action is 'Disinfect. Delete if disinfection fails.' Perform actions: Enables File Antivirus to automatically attempt to disinfect all infected files that are detected. If disinfection fails, File Antivirus deletes those files.

Disinfect: Enables File Antivirus to automatically attempt to disinfect all infected files that are detected. File Antivirus applies the Delete action to files that are part of the Windows Store application.

Delete if disinfection fails: Enables File Antivirus to automatically delete all infected files that it detects.

About the Ivanti Antivirus Protection: Mail Antivirus page:

Use this page to configure the way Mail Antivirus works with Ivanti Antivirus on target devices. This page contains the following options:

Enable Mail Antivirus: Starts Mail Antivirus with Ivanti Antivirus.

Mail Antivirus continuously remains active in computer memory and scans all email messages that are transmitted via the POP3, SMTP, IMAP, MAPI, and NNTP protocols. By default, Mail Antivirus is enabled and configured with the recommended settings.

Security Level: Specifies one of the three file security levels (High, Recommended, or Low). You can configure a custom mail file security level by selecting settings on the General, Performance, and Additional tabs. High: Mail Antivirus scans email messages most thoroughly. Mail Antivirus scans incoming and outgoing messages and performs deep heuristic analysis. The High mail security level is recommended when working in a dangerous environment, such as a...
connection to a free email service from a home network that is not guarded by centralized email protection. Recommended: Provides the optimal balance between the performance of Ivanti Antivirus and email security. Mail Antivirus scans incoming and outgoing email messages, and performs middle-intensity heuristic analysis. This mail traffic security level is recommended by Ivanti. This is the default setting. Low: Scans only incoming email messages, performs light heuristic analysis, and doesn’t scan archives that are attached to email messages. At this mail security level, Mail Antivirus scans email messages at maximum speed and uses a minimum of operating system resources. The Low mail security level is recommended for use in a well-protected environment, such as a LAN with centralized email security. If you choose to create a custom security level, be sure to consider the working conditions and current situation. General: Protection scope: Specifies whether to scan incoming and outgoing messages or incoming messages only. POP3 / SMTP / NNTP / IMAP traffic: Enables Mail Antivirus to scan emails before they are received on the computer. If you clear this option, Mail Antivirus will not scan email messages that are transferred via the POP3, SMTP, NNTP, and IMAP protocols before they arrive on your computer. Instead, Mail Antivirus plug-ins that are embedded into the Microsoft Office Outlook and The Bat! email clients will scan the messages after they arrive on your computer. Additional: Microsoft Office Outlook plug-in: Enables access to the Mail Antivirus settings from Microsoft Office Outlook so you can configure the component to scan email messages for viruses and other malware. A plug-in embedded into Microsoft Office Outlook is enabled to scan email messages transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they arrive on your computer. Additional: The Bat! plug-in: Enables the plug-in embedded into The Bat! to scan email messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they are received on your computer. Scan attached archives: Enables Mail Antivirus to scan archives that are attached to email messages. You can specify the size of archives to scan and the amount of time allocated for the scanning of archived email attachments. Attachment filter: Disable filtering: Specifies whether Mail Antivirus filters files that are attached to email messages. Rename specified attachment types: Enables Mail Antivirus to replace the last character in attached files of the specified types with the underscore (_) symbol. Delete specified attachment types: Enables Mail Antivirus to delete attached files of the specified types from the email messages. You can specify the types of attached files to delete from emails in the Extension list. Additional: Specifies whether Mail Antivirus will use heuristic analysis during scanning of email. This technology detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as probably infected. Move the slider along the horizontal axis to change the detail level for heuristic analysis. The detail level for heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of heuristic analysis are available: Light scan: Heuristic Analyzer doesn’t perform all instructions in executable files while scanning email for malicious code. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Email scanning is faster and less resource-intensive. Medium scan: When scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti. The medium scan detail level is selected by default. Deep scan: When
scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Email scanning consumes more system resources and takes more time. Action: Select action automatically. Enables Mail Antivirus to perform the default action that is specified by Ivanti. This action is to disinfect all infected email messages that are detected and if disinfection fails, to delete them. Perform actions: Mail Antivirus automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, Mail Antivirus deletes them. If this option is selected, Mail Antivirus automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, Mail Antivirus moves them to Quarantine. Disinfect: Mail Antivirus automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, Mail Antivirus moves them to Quarantine. Delete: Mail Antivirus automatically deletes all infected email messages that are detected. About the Ivanti Antivirus Protection: Web Antivirus page
Use this page to configure the way Web Antivirus works with Ivanti Antivirus on target devices. This page contains the following options: Enable Web Antivirus: Web Antivirus starts with Ivanti Antivirus and protects information that arrives on the computer via the HTTP and FTP protocols. By default, Web Antivirus is enabled and configured with the recommended settings. Security Level: Specifies one of the three file security levels (High, Recommended, or Low). You can configure a custom web security level by selecting settings on the Scan methods and optimization and Trusted URLs tabs. High: Web Antivirus performs maximum scanning of web traffic that the computer receives via the HTTP and FTP protocols. Web Antivirus scans in detail all web traffic objects, with use of the full set of application databases, and performs the deepest possible heuristic analysis. This technology was developed for detecting threats that cannot be detected by using the current version of Ivanti databases. It detects files that may be infected with an unknown virus or a new variety of a known virus. Files in which malicious code is detected during heuristic analysis are marked as probably infected. Recommended: Provides the optimal balance between the performance of Ivanti Antivirus and the security of web traffic. Web Antivirus performs heuristic analysis at the Medium scan level. This default web traffic security level is recommended by Ivanti. Low: Ensures the fastest scanning of web traffic. Web Antivirus performs heuristic analysis at the Light scan level. If you choose to create a custom security level, be sure to consider the working conditions and current situation. Scan methods and optimization: Check if links are listed in the database of suspicious URLs: Specifies whether to scan URLs against the database of malicious web addresses. Checking URLs against the database of malicious web addresses helps to detect websites that are in the black list of web addresses. Check if links are listed in the database of phishing URLs: Specifies whether to scan URLs against the database of phishing web addresses. The database of phishing URLs includes the web addresses of currently known websites that are used to launch phishing attacks. Heuristic analysis for detecting viruses: Specifies whether to use heuristic analysis when scanning web traffic for viruses and other malicious programs. The technology was developed for detecting threats that cannot be detected by using the current version of Ivanti application databases. It detects files that may be infected with an unknown virus or a new variety of a known virus. Files in which malicious code is detected during heuristic analysis are marked as probably infected. Heuristic analysis for phishing links:
Specifies whether to heuristic analysis when scanning web pages for phishing links. Limit web traffic caching time: Scans cached fragments of web traffic objects for one second. If the option is cleared, Web Antivirus performs deeper web traffic scanning. Access to web traffic objects may become slower during scanning. Trusted URLs: Do not scan web traffic from trusted URLs. Specifies whether to scan the content of websites whose addresses are included in the list of trusted URLs. Click Add to open the Address mask (URL) window, where you can enter a URL and enable or disable it. If a URL is disabled, Web Antivirus temporarily excludes it from the list of trusted URLs. Action:Select action automatically: Enables Web Antivirus to perform the default action that is specified by Ivanti when it detects an infected object in web traffic. The default action is 'Block download.' Block download: Enables Web Antivirus to block access to an infected object and display a notification about the object. Allow download: Enables Web Antivirus to allow an infected object to be downloaded to your computer. About the Ivanti Antivirus Protection: IM Antivirus page Use this page to configure the way IM Antivirus works with Ivanti Antivirus on target devices. This page contains the following options: Enable IM Antivirus: IM Antivirus starts with Ivanti Antivirus, remains constantly in the computer's RAM, and scans all messages that arrive through Internet messaging clients. IM Antivirus ensures the safe operation of numerous instant messaging applications, including ICQ, MSN® Messenger, AIM, Mail.Ru Agent, and IRC. Protection scope: Specifies the type of messages that are transmitted by IM clients to be scanned by IM Antivirus. Incoming and outgoing messages: IM Antivirus scans both incoming and outgoing instant messages for malicious objects or URLs that are in databases of malicious and phishing web addresses. This is the default setting. Incoming messages only: IM Antivirus scans only incoming instant messages for malicious objects or URLs that are in databases of malicious and phishing web addresses. IM Antivirus doesn’t scan outgoing messages. Scan methods: Specifies the methods that IM Antivirus uses when scanning messages that arrive through IM clients. Check if links are listed in the database of suspicious URLs: Specifies whether to scan URLs in IM client messages against the database of malicious URLs. Check if the links are listed in the database of phishing URLs: Specifies whether to scan URLs in IM client messages against the database of phishing URLs. Heuristic analysis: Specifies whether IM Antivirus will use heuristic analysis scanning IM client messages. This technology detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as probably infected. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail level for Heuristic Analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic Analysis are available: Light Scan: Heuristic Analyzer scans instant messages for threats by using a minimum set of attributes. Scanning is faster and less resource-intensive, with the least number of false positives. Medium scan: Heuristic Analyzer scans instant messages for threats by using the number of attributes that ensures the optimum balance between the speed and detail of scanning and avoids a large number of false positives. This level of detail for heuristic analysis is set by default. Deep scan: Heuristic Analyzer scans instant messages for threats by using a maximum set of attributes. The scan is performed in detail, requires more operating system resources, and takes more time. False positives are probable. About the Ivanti Antivirus Protection: Network
Attack Blocker page

Use this page to configure the Network Attack Blocker that Ivanti Antivirus uses on target devices to detect and add attacking computers to the list of blocked devices for a specified period of time. This page contains the following options:

- **Enable Network Attack Blocker**: Network Attack Blocker starts with Ivanti Antivirus and scans incoming network traffic for network activity that is characteristic of network attacks. After detecting an attempted network attack, Network Attack Blocker blocks network activity from an attacking computer that targets the user's computer.

  - **Add the following computer to the list of blocked computers for (minutes)**: Specifies the number of minutes that Network Attack Blocker will block network activity from an attacking computer. This block automatically protects the user's computer against possible future network attacks from the same address. The default value is 60 minutes.

- **Configure addresses of exclusions**: Specifies IP addresses from which network attacks will not be blocked, although information about such attacks will be logged. Click the Exclusions... button to open the Exclusions window, where you can add IP addresses.

- **About the Ivanti Antivirus Protection: System Watcher page**

  Use this page to configure System Watcher, which Ivanti Antivirus uses to monitor application activity on target devices. System Watcher settings only take effect after the next reboot.

  - **This page contains the following options**:
    - **Enable System Watcher**: Enables the functionality specified in the System Watcher settings.
    - **Enable Exploit Prevention**: Enables Ivanti Antivirus to keep track of executable files launched by applications. On detecting that an attempt to run an executable file from a vulnerable application was not initiated by the user, Ivanti Antivirus blocks the launch of this file. Ivanti Antivirus stores information about the blocked launch of the executable file in the Exploit Prevention report.
    - **Log application activity for the BSS database**: Enables the logging of application activity. This information is used to update the BSS (Behavior Stream Signatures) database. System Watcher logs application activity by default.
    - **Do not monitor the activity of applications that have a digital signature**: Ivanti Antivirus adds digitally signed applications to the Trusted group and doesn’t monitor the activities of applications from this group.
    - **Rollback of malware actions**: Allows rolling back malware actions in the operating system while disinfection is in progress. This option is selected by default.
    - **Proactive Defense**: Specifies whether Ivanti Antivirus will analyze the activity of an application and what action it will take if it determines the activity is malicious.
    - **Use behavior stream signatures (BSS)**: Specifies whether to use BSS (Behavior Stream Signatures) technology, which involves analyzing the behavior of applications based on information that is collected about their activities. System Watcher looks for similarities between the actions of an application and the actions of malware. If System Watcher analyzes the activity of an application and determines that it is malicious, System Watcher performs the action that you specified in the On detecting malware activity list.
    - **On detecting malware activity**: Specifies the action that Ivanti Antivirus performs upon detection of malicious activity.
    - **Select action automatically**: Ivanti Antivirus performs the default action that is specified by Ivanti.
      - By default, Ivanti Antivirus moves the executable file of a malicious application to Quarantine.
      - **Move file to Quarantine**:
      - Ivanti Antivirus moves the executable file of a malicious application to Quarantine.
      - **Terminate the malicious program**:
      - Ivanti Antivirus terminates the application.
    - **Skip**: Ivanti Antivirus doesn’t take any action on the executable file of a malicious application. About the Ivanti Antivirus: Scheduled Tasks page

Use this page to create a scheduled task that will be performed by the Ivanti Local Scheduler tool. These tasks
are separate from the tasks that can be scheduled via the Ivanti Antivirus client on the managed device. Note that task notifications that appear in the client interface refer to the Ivanti Antivirus client’s native scheduler, not the core server’s Local Scheduler tool. This page contains the following options:

Scheduled tasks: Creates a scheduled task that will be performed by Ivanti Antivirus on the managed device. These tasks are separate from the tasks that can be scheduled via the Ivanti Local Scheduler tool. Update: Specifies when to update virus definitions. Click Change schedule... to open the Schedule periodic virus definition updates window, where you can select the events that will trigger an update, the time of an update, and the filters. Full Scan: Specifies when to do a full scan. Click Change schedule... to open the Schedule periodic antivirus scans window, where you can select the events that will trigger a scan, the time of a scan, and the filters. Critical Areas Scan: Specifies when to scan critical areas only. Click Change schedule... to open the Schedule periodic antivirus scans window, where you can select the events that will trigger a scan, the time of a scan, and the filters. Background scan tasks: Specifies whether to performing the background scan of the system memory, startup objects, and the system partition while the computer is idle to optimize the use of computer resources. Perform idle scan: Starts a scan task for autorun objects, RAM, and the operating system partition when the computer is locked or the screen saver is on for 5 minutes or longer, if one of the following conditions is true: An idle scan of the computer has not occurred since the installation of Ivanti Antivirus. The last idle scan of the computer occurred more than 7 days ago. The last idle scan of the computer was interrupted during an update of the application databases and modules. The last idle scan of the computer was interrupted during an on-demand scan. Scan removable drive on connection: Specifies whether to scan a removable drive when it is connected to the computer. Action on removable drive connection: Allows you to select the action that Ivanti Antivirus will perform when you connect a removable drive to the computer. Do not scan: Ivanti Antivirus doesn’t run a scan and doesn’t prompt you to select an action to perform when a removable drive is connected. Full scan: Ivanti Antivirus starts a full scan of the removable drive according to the Full Scan task settings. Quick scan: Ivanti Antivirus starts a start a scan of the removable drive according to the Critical Areas Scan task settings. Maximum removable drive size (MB): Specifies the size of removable drives on which Ivanti Antivirus performs the action that is selected in the Actions on drive connection list. The default size is 4096 MB.

About the Ivanti Antivirus Scheduled Tasks: Update page

Use this page to configure virus definition (pattern) file updates scheduling, user download options, and access options, for target devices with these antivirus settings. To schedule an update, select Update on the Scheduled Tasks page. This page contains the following options:

Download "pilot" version of virus definition files: Download virus definition files from the pilot folder instead of from the default \LDLogon\Antivirus8\Win\BasesEP 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\Antivirus8\Win\BasesEP) are not downloaded. Download virus definition updates
from: Specifies the source site (core server or Kaspersky content server) from which virus
definition files are downloaded. Preferred server/Peer download options: Allows you to
configure core server settings if you’ve selected one of the download source site options that
includes the core. Attempt peer download: Prevents virus definition file downloads via peer
download (the local cache or a peer in the same multicast domain). Attempt preferred server:
Prevents virus definition file downloads via a preferred server. For more information about
preferred servers, see About software distribution. Bandwidth used from core or preferred
server (WAN): Specifies the bandwidth used. You can move the slider or enter a value in the
percentage box. Bandwidth used peer-to-peer (Local): Specifies the bandwidth used. You can
move the slider or enter a value in the percentage box. Application update settings: Specifies
whether to update application modules. Update application modules: Enables downloads of
application module updates along with antivirus database updates. If selected, Ivanti Mac
Antivirus includes application module updates in the update package when the application
runs the update task. This option is selected by default. Scan removable drive on connection:
Specifies whether to scan a removable drive when it is connected to the computer. Action on
removable drive connection: Allows you to select the action that Ivanti Antivirus will perform
when you connect a removable drive to the computer. Do not scan: Ivanti Antivirus doesn’t run
a scan and doesn’t prompt you to select an action to perform when a removable drive is
connected. Full scan: Ivanti Antivirus starts a full scan of the removable drive according to the
Full Scan task settings. Quick scan: Ivanti Antivirus starts a start a scan of the removable drive
according to the Critical Areas Scan task settings. Maximum removable drive size (MB): Specifies
the size of removable drives on which Ivanti Antivirus performs the action that is selected in the
Actions on drive connection list. The default size is 4096 MB. About the Schedule periodic
antivirus scans dialog box: If you want this antivirus settings to include a recurring antivirus
scan, use this dialog box 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 box 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 box contains the
following options: Run when user logs in: The scan will occur when the user logs into the
machine. Run whenever the machine’s IP address changes: The scan will occur when the
machine’s IP address changes. 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 Ivanti Antivirus Scheduled Tasks: Full Scan page Use this page to configure the way Ivanti Antivirus performs full scans on target devices. To schedule a full scan, select Full Scan on the Scheduled Tasks page. This page contains the following options: Security Level: Specifies one of the three file security levels (High, Recommended, or Low). High: If the probability of computer infection is very high, select this file security level. Ivanti Antivirus scans all types of files. When scanning compound files, Ivanti Antivirus also scans mail-format files. Recommended: Ivanti Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives or installation packages. Low: Ensures maximum scanning speed. Ivanti Antivirus scans only new or modified files with the specified extensions on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives, installation packages, or compound files. Scope: You can expand or restrict the scan scope by adding or removing scan objects or by changing the type of files to be scanned. By default, a full scan includes system memory, startup objects, disk boot sectors, system backup storage, email, hard drives, and removable drives. File types: Specifies whether to scan files by format, extension, or both. There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is
skipped by the scan. If scanning of files by format is selected, then regardless of the extension, Ivanti Antivirus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware. Scan only new and changed files: Enables Ivanti Antivirus to scan only new files and files that have been modified since the previous scan. Skip files that are scanned for longer than: Specifies in seconds the length of time to scan a file before skipping it. Scan archives: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives. On a full scan, this option is enabled by default. Scan installation packages: Enables Ivanti Antivirus to scan installation packages. On a full scan, this option is enabled by default. Scan embedded OLE objects: Enables Ivanti Antivirus to scan files that are embedded in another file (such as Microsoft® Office Excel® spreadsheets, macros that are embedded in Microsoft® Office Word® files, or email attachments). On a full scan, this option is enabled by default. Parse email formats: Enables Ivanti Antivirus to parse email formats during the scan. Scan password-protected archives: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives that are password-protected. Additional: Click this button to open the Compound files window, where you can specify whether to unpack compound files in the background and set a size limit for compound files. Additional: Specifies the method and technology Ivanti Antivirus will use during a full scan. Scan methods: Heuristic analysis detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as probably infected. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail level for Heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic analysis are available: Light scan: Heuristic Analyzer doesn’t perform all instructions in executable files while scanning. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Scanning is faster and less resource-intensive. Medium scan: When scanning, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti. The medium scan detail level is selected by default. Deep scan: When scanning for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Scanning consumes more system resources and takes more time. Scan technologies: Specifies the scan technologies that Ivanti Antivirus uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. These technologies optimize the speed of scanning files by excluding files that have not been modified since the most recent scan. Action: Specifies the action that Ivanti Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Antivirus creates a backup copy for subsequent restoration or disinfection. Select action automatically: Ivanti Antivirus performs the default action that is specified by Ivanti. This action is 'Disinfect. Delete if disinfection fails.' This action is selected by default. Perform actions: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. If disinfection fails, Ivanti Antivirus deletes those files. Disinfect: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Antivirus applies the 'Delete' action to files that are part of the Windows Store application. Delete if disinfection fails: Ivanti
Antivirus automatically deletes all infected files that it detects. About the Ivanti Antivirus Scheduled Tasks: Critical Areas Scan page

Use this page to configure the way Ivanti Antivirus performs critical areas scans on target devices. To schedule a critical areas scan, select Critical Areas Scan on the Scheduled Tasks page. This page contains the following options:

Security Level: Specifies one of the three file security levels (High, Recommended, or Low). High: If the probability of computer infection is very high, select this file security level. Ivanti Antivirus scans all types of files. When scanning compound files, Ivanti Antivirus also scans mail-format files. Recommended: Ivanti Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won't scan archives or installation packages. Low: Ensures maximum scanning speed. Ivanti Antivirus scans only new or modified files with the specified extensions on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won't scan archives, installation packages, or compound files. Scope: You can expand or restrict the scan scope by adding or removing scan objects or by changing the type of files to be scanned. By default, a critical areas scan includes only system memory, startup objects, and disk boot sectors. File types: Specifies whether to scan files by format, extension, or both. There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then regardless of the extension, Ivanti Antivirus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware. Scan only new and changed files: Enables Ivanti Antivirus to scan only new files and files that have been modified since the previous scan. Skip files that are scanned for longer than: Specifies in seconds the length of time to scan a file before skipping it. Scan archives: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives. On a critical areas scan, this option is disabled by default. Scan installation packages: Enables Ivanti Antivirus to scan installation packages. On a critical areas scan, this option is disabled by default. Scan embedded OLE objects: Enables Ivanti Antivirus to scan files that are embedded in another file (such as Microsoft® Office Excel® spreadsheets, macros that are embedded in Microsoft® Office Word® files, or email attachments). On a critical areas scan, this option is enabled by default. Parse email formats: Enables Ivanti Antivirus to parse email formats during the scan. On a critical areas scan, this option is enabled by default. Scan password-protected archives: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives that are password-protected. Additional: Click this button to open the Compound files window, where you can specify whether to unpack compound files in the background and set a size limit for compound files. Additional: Specifies the method and technology Ivanti Antivirus will use during a critical areas scan. Scan methods: Heuristic analysis detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as probably infected. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail
level for Heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic analysis are available:

Light scan: Heuristic Analyzer doesn’t perform all instructions in executable files while scanning. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Scanning is faster and less resource-intensive.

Medium scan: When scanning, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti. Deep scan: When scanning for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Scanning consumes more system resources and takes more time.

For a critical areas scan, this is the default heuristic analysis level.

Scan technologies: Specifies the scan technologies that Ivanti Antivirus uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. These technologies optimize the speed of scanning files by excluding files that have not been modified since the most recent scan.

Action: Specifies the action that Ivanti Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Antivirus creates a backup copy for subsequent restoration or disinfection. Select action automatically: Ivanti Antivirus performs the default action that is specified by Ivanti. This action is 'Disinfect. Delete if disinfection fails.' This action is selected by default. Perform actions: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. If disinfection fails, Ivanti Antivirus deletes those files.

Disinfect: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Antivirus applies the 'Delete' action to files that are part of the Windows Store application. Delete if disinfection fails: Ivanti Antivirus automatically deletes all infected files that it detects.

About the Ivanti Antivirus Scheduled Tasks: Custom Scan page

Use this page to configure custom scans on target devices. This page contains the following options:

Security Level: Specifies one of the three file security levels (High, Recommended, or Low). High: If the probability of computer infection is very high, select this file security level. Ivanti Antivirus scans all types of files. When scanning compound files, Ivanti Antivirus also scans mail-format files.

Recommended: Ivanti Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives or installation packages.

Low: Ensures maximum scanning speed. Ivanti Antivirus scans only new or modified files with the specified extensions on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives, installation packages, or compound files.

Scope: You can expand or restrict the scan scope by adding or removing scan objects or by changing the type of files to be scanned.

File types: Specifies whether to scan files by format, extension, or both. There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is
skipped by the scan. If scanning of files by format is selected, then regardless of the extension, Ivanti Antivirus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware. Scan only new and changed files: Enables Ivanti Antivirus to scan only new files and files that have been modified since the previous scan. Skip files that are scanned for longer than: Specifies in seconds the length of time to scan a file before skipping it. Scan archives: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives. Scan installation packages: Enables Ivanti Antivirus to scan installation packages. Scan embedded OLE objects: Enables Ivanti Antivirus to scan files that are embedded in another file (such as Microsoft® Office Excel® spreadsheets, macros that are embedded in Microsoft® Office Word® files, or email attachments). Parse email formats: Enables Ivanti Antivirus to parse email formats during the scan. Scan password-protected archives: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives that are password-protected. Additional: Click this button to open the Compound files window, where you can specify whether to unpack compound files in the background and set a size limit for compound files. Additional: Specifies the method and technology Ivanti Antivirus will use during a custom scan. Scan methods: Heuristic analysis detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as probably infected. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail level for Heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic analysis are available: Light scan: Heuristic Analyzer doesn’t perform all instructions in executable files while scanning. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Scanning is faster and less resource-intensive. Medium scan: When scanning, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti. The medium scan detail level is selected by default. Deep scan: When scanning for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Scanning consumes more system resources and takes more time. Scan technologies: Specifies the scan technologies that Ivanti Antivirus uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. These technologies optimize the speed of scanning files by excluding files that have not been modified since the most recent scan. Action: Specifies the action that Ivanti Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Antivirus creates a backup copy for subsequent restoration or disinfection. Select action automatically: Ivanti Antivirus performs the default action that is specified by Ivanti. This action is 'Disinfect. Delete if disinfection fails.' This action is selected by default. Perform actions: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. If disinfection fails, Ivanti Antivirus deletes those files. Disinfect: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Antivirus applies the 'Delete' action to files that are part of the Windows Store application. Delete if disinfection fails: Ivanti Antivirus automatically deletes all infected files that it detects. About the Ivanti Antivirus: Advanced settings page Use this page to configure Ivanti
Antivirus Advanced settings on target devices. This page contains the following options:
Enable Self-Defense: Prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry. Disable external management of the system service: Blocks any attempts to remotely manage Ivanti Antivirus. If an attempt is made to manage application services remotely, a notification is displayed in the Microsoft Windows taskbar, above the application icon (unless the notification service is disabled by the user). Send dump and trace files to Ivanti for analysis: Sends dump and trace files to Ivanti, where the cause of the crashes will be examined. If you select this option, the Uploading support information to server window will open when Ivanti Antivirus restarts after a crash. In this window, you can select dump and trace files from the list and send them to Ivanti for examination.
Operating mode: Allows you to configure optimum energy and computer resource consumption in the operation of Ivanti Antivirus. Do not start scheduled tasks while running on battery power: Computer scan tasks and database update tasks tend to consume considerable resources and take a long time to finish. This option enables energy conservation mode when a portable computer is running on battery power, which postpones scan and update tasks. The user can start scan and update tasks manually, if necessary.
Concede resources to other applications: When Ivanti Antivirus runs scheduled tasks, this may result in increased workload on the CPU and disk subsystems, which slows down the performance of other applications. This option suspends scheduled tasks when it detects an increased load on the CPU and frees up operating system resources for user applications.
About the Ivanti Antivirus Advanced settings: Reports and Storages page Use this page to configure Ivanti Antivirus Advanced Reports and Storages settings on target devices. This page contains the following options:
Reports parameters: Specifies the length of time to store a report and the maximum size of a report. Store reports no longer than (days): Specifies the maximum report storage term in number of days. The default maximum storage term for reports is 30 days. After that period of time, Ivanti Antivirus automatically deletes the oldest entries from the report file. Maximum file size (MB): Specifies the maximum report file size in megabytes. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Ivanti Antivirus automatically deletes the oldest entries from the report file when the maximum report file size is reached.
Local quarantine and backup settings: Allows you to configure quarantine and backup settings. The data storage comprises a quarantine catalog and a storage for backup copies of files. Rescan quarantine after update: Enables automatic scanning of quarantined files after each update of the databases and application software modules of Ivanti Antivirus. If you select this option, Ivanti Antivirus starts a scan of quarantined files after every update of databases and application software modules.
Store objects no longer than: Specifies the maximum storage term for files in quarantine and copies of files in backup. The maximum file storage term is measured in days. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Ivanti Antivirus deletes the oldest files from Quarantine and Backup. Maximum storage size: Specifies the maximum data storage size in megabytes. By default, the maximum size is 100 MB. To not exceed the maximum data storage size, Ivanti Antivirus automatically deletes the oldest files when the data storage reaches its maximum size.
About the Ivanti Antivirus Advanced settings: Interface page Use this page to configure the Advanced Interface settings that Ivanti Antivirus will use on target devices. This page contains the following options: Show
"Protected by Kaspersky Lab" on Microsoft Windows logon screen: Enables the "Protected by Kaspersky Lab" message on the Microsoft Windows logon screen. This option is selected by default. If the application is installed on a computer that runs on an operating system in the Microsoft Windows Vista family, this option is unavailable. Use icon animation while running tasks: Enables the animation of the application icon in the taskbar notification area of Microsoft Windows when tasks are running. This option is selected by default. About the Ivanti Antivirus Advanced settings:

Import settings page: Use this page to configure how Ivanti Antivirus will import Kaspersky settings on target devices. This page contains the following options:

- **Import settings file from a Kaspersky antivirus client:** Lets you import settings from a client machine. To import the settings, specify Kaspersky settings on a client and save the settings as a .CFG file. From the console, browse to the .CFG file. The options listed in the .CFG file will be set first and then any Ivanti Antivirus settings will be set. Note that Ivanti Antivirus will not look for a new .CFG update and auto-update it. You must manually update the .CFG file if you want to import different settings.

- **Current configuration imported from:** The Browse button [...] opens the Select a previously saved Kaspersky configuration file window. Browse to the \Idlogon folder, click the .CFG file, then click Open.

- **Clear password after import:** Enables users to change Kaspersky settings without the settings file password. Use imported scan settings: Uses scan settings from the imported settings file. On date: The current date of the import.

Notes: Any notes about the .CFG file. " on page 1)

- "Agent settings: Antivirus legacy" on page 221
- "Agent settings: Application Control" on page 237
- "Agent settings: Branding" on page 243
Skin_Formats_CrossReferencePrintFormat("Agent settings: Client connectivityTools > Configuration > Agent Settings > Client connectivityUse the Client connectivity settings dialog box to specify and save a collection of client connectivity settings. About the General pageUse the General page to name the client connectivity setting that you’re configuring. You can have multiple profiles for client connectivity settings, but one must be set as the default for agent configurations. By selecting the Set as default option, the setting will be the default selection in the Agent Configuration tool. About the Core information pageUse this page to configure certificate-based security and what scope devices using this configuration will have. Core certificates the client will trustSelect 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. 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 is 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. Core address This needs to be a resolvable name or IP address that managed devices will use to communicate with the 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 Endpoint Manager 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 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 NetWare 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 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 and device group scopes. For more information on how scopes are used in Endpoint Manager role-based administration, and how you can define a scope using custom directory paths, see Role-based administration overview. About the Cloud Services Appliance page

The Cloud Services Appliance (CSA) page has the following features:

Enable Cloud Services Appliance communication: Select this if you’ve installed one or more CSAs and you want an agent configuration to use the appliance to connect to the core server. Available items and Selected items: Lists the available and selected CSAs that you’ve configured for this core server. Select the one you want to use. There isn’t a limit to the number of CSAs that you can add. Use the CSA failover policy for CSA load balancing and to set what happens if there’s a connection failure when a client tries to communicate with a CSA. When there’s a connection failure, the client will try connecting to other CSAs in the Selected items list. When a CSA connection failure happens, the client won’t try to use that CSA for 24 hours. Use ordered list as shown in the selected items: Clients will attempt to connect to the first CSA in the Selected items list. If that fails, clients will connect to the next CSA in the list until all CSAs have had a connection attempt. Use this mode when one CSA is preferred over others for clients. For example, you may want devices for employees working in one country to use a CSA in that country as the top priority and some from other countries as backup systems. Use random order: Clients will connect to a random CSA in the Selected items list. If that fails, clients connect to the next randomly selected CSA in the list until all CSAs have had a connection attempt. Use this mode when there are several CSAs of equal preference to a client, but you want to spread the workload across these CSAs. For example, devices for employees in one country may have three CSAs set up for them to use. Using the random order selection would generally distribute the work load across these CSAs and still provide failover if one stops working. When you have enabled Cloud Service Appliance communication, you have three ways to connect to the core:

Dynamically determine connection route: This is the default and the most flexible choice. If the agent can connect directly, it will. If it can’t connect directly, it tries to use the CSA. This mode may take a bit longer to connect since it tries each connection mode. Connect directly to the LDMS core: Always connects directly to the core. Connect using the Cloud Service Appliance: Always connects to the core via the CSA. About the Download page

Use the Download page to block peer downloads over adapters that you specify. You can exclude adapters that are wireless. You can also exclude adapters by using case-sensitive keywords. If any of the keywords entered are found in the description field of the adapter, it will not use that adapter. As you can see by the default keywords, this method is used for disabling peer download over a VPN adapter. You can also change the number of days files stay in the download cache on clients. About the Preferred server page

Use the Preferred server page to control preferred server behavior: Update preferred server list from core every: Preferred server list update interval. This is the maximum amount of time a client will use the list of preferred servers before going to the core for a potentially new list. The default is once a day. The preferred server list is also discarded every time the IP address changes. Number of preferred servers to attempt before falling back to source: The default is three servers. Number of files not found on preferred server before the server is moved to the end of the preferred server priority list: The default is three files not found. About the Self-electing subnet services page

Use the Extended device discovery page to customize ARP and
WAP extended device discovery scan settings. Use address resolution protocol (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 Ivanti 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), or everything (3). The default level is 1 - errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xdclient.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. Use wireless access point discovery (WAP) 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), or everything (3). The default level is 1 - errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xdclient.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 Local scheduler page: Use the Local scheduler page to configure how often the local scheduler checks for tasks and network bandwidth. The local scheduler agent enables Endpoint Manager to launch device tasks based on a time of day or bandwidth availability. The local scheduler agent is most useful for mobile devices that may not always be on the network or may connect to the network via a dial-up connection. For example, you can use the local scheduler to allow mobile device 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 the minimum bandwidth the packages or policies require before they are applied. The local scheduler runs as a service on Windows devices. The Local scheduler page contains the following features: General frequency: How often the local scheduler checks for tasks. The default is 10 seconds. The polling interval you select is stored on the local device. 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. The local scheduler also enables bandwidth detection between devices and the core server. You can limit Endpoint Manager 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. ICMP or PDS: 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 dial-up 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 dial-up 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 Ivanti agent to the package server. Bandwidth detection LAN threshold: The threshold that classifies a connection as WAN rather than LAN. The default is 262144 bps." on page 1)

- "Agent settings: Custom variables to override" on page 248
- "Agent settings: Custom variables to override" on page 248
- "Agent settings: Device control" on page 249
- "Agent settings: Reboot settings" on page 261
- "Agent settings: Distribution and patch" on page 251
- "Agent settings: Endpoint security" on page 264
- "Agent settings: Exchange/Office 365" on page 292
- "Agent settings: Extended device discovery" on page 264
- "Agent settings: HP BIOS" on page 266
- "Agent settings: Remote secure erase" on page 265
- "Agent settings: HP software policies" on page 267
- "Agent settings: Inventory settings" on page 267
- "Agent settings: Ivanti Firewall" on page 270
- "Agent settings: Ivanti Mac Antivirus" on page 274
- "Agent settings: Mac configuration profile" on page 291
- "Agent settings: Mobile Compliance" on page 294
- "Agent settings: Mobile Connectivity" on page 295
- "Agent settings: Mobile Security" on page 297
- "Agent settings: Other security settings" on page 305
- "Agent settings: Portal manager" on page 306
- "Agent settings: Power management" on page 307
- "Agent settings: Mac power management" on page 309
- "Agent settings: Remote control" on page 310
- "Agent settings: Tenant" on page 315
- "Agent settings: Trusted file lists" on page 315
- "Agent settings: Windows Firewall" on page 315
Agent settings: Adaptive settings

Tools > Configuration > Agent settings > Adaptive settings

An adaptive setting is a list of one or more adaptive settings rules ordered by priority. In the adaptive settings agent configuration, you can select multiple rules from a list of available rules. The agent on the managed device will check the triggers for each rule in the selected rules list, starting at the top. The first rule the agent encounters with a matching trigger will be applied and rule processing stops. Only one rule can be active at a time. If no rules are triggered, the default settings specified in the agent configuration page will be applied.

Adaptive settings allow agent settings to dynamically change on a device based on location (geofencing) or IP address. This is mainly oriented towards mobile devices and laptops. For example, you could have one set of agent settings while a device is connected to the corporate network, but when the device connects to an external network, the agent settings could be more restrictive.

For more information, see "Adaptive settings" (159).

NOTE: Enabling adaptive settings will cause .NET4 to be installed with the agent.

The Adaptive settings dialog box contains the following options:

- **Name**: The name for this adaptive setting.
- **Rules**: Move the rules you want applied from the Available rules list to the Selected rules list. Click **Move up** and **Move down** to change the order if necessary. Click **New...** to open the Edit adaptive setting rule dialog box.
- **If no rules apply**: If no rules apply, you can use the default agent configuration settings (in other words, don’t change anything) or you can select a specific rule to apply from the Apply the following rule list.
- **Lock windows session if location services are disabled**: Click to lock the device when location services are disabled, such as when someone leaves your office building or if someone turns on airplane mode.
- **Check GPS location every**: The default is two minutes. Frequent checks will reduce device battery life.
- **Set as default within agent config**: Makes this adaptive setting the default for new agent configurations.

About the Edit adaptive setting rule dialog box

Clicking **New** or **Edit** in the Adaptive settings dialog box shows the Edit adaptive setting rule dialog box. An adaptive settings rule associates a trigger with one or more agent settings to override when the trigger activates, along with additional one-time actions, such as locking the screen.

For more information, see "Adaptive settings" (159).
The **Edit adaptive setting rule** dialog box contains the following options:

- **Rule name**: The name for this rule.
- **Select trigger**: Shows available triggers. Use **New** if there aren’t any or if you want to make a new one. Triggers can be either geo fence or IP address range.
  - **New**... Opens the **Edit trigger** dialog box, where you can configure a new trigger.
  - **Edit**...Edits the selected trigger.
  - **Delete** Deletes the selected trigger.
- **Type/Settings**: In the settings list, select the agent setting you want to use for each type.
On rule activation, perform the following one time actions: Adaptive settings rules can have one-time actions that execute when the rule activates. Select any one-time actions that you want run for this rule.

- **Apply HP’s recommended locked-down security BIOS settings:** This only works on HP devices. You’ll need to provide the BIOS password.
- **Lock Windows session:** Locks the session so the user has to log back in. This can help prevent unauthorized access when the device leaves a secure area.
- **Run security scan:** Runs the security scan that you select. Click **Configure** and select a scan.
- **Run a batch file or powershell script:** Click **Configure** and select a batch file or powershell script.

**About the Edit trigger dialog box**

The **Edit trigger** dialog box contains the following options:

- **Trigger name:** The name for this trigger.
- **Select Type:** One of the following:
  - **Geofence:** Requires Windows 8 and a device with a GPS. Click and drag the map so the red cross-hair is over the location you want to geofence. Use the scroll bars to zoom in and out. The target radius circle defaults to 10 meters. Increase the **Radius** if you want it to include a corporate campus, city, and so on. The minimum device accuracy determines how accurate the GPS reading must be for the trigger to activate. If the GPS-reported accuracy exceeds the value you specify, the trigger won’t activate.
  - **IP address range:** Works with any Windows device. The **Verify core existence on the network** option can help prevent network spoofing by making sure the Ivanti® Endpoint Manager powered by Landesk core server is visible to the device. Don’t use this option with IP address ranges that won’t have access the core server.

**Agent settings: Agent health**

Tools > Configuration > Agent settings > Agent health

Use the **Agent health** agent setting to manage agent health on devices. With agent health, the vulnerability scanner will make sure agents components stay installed, are current, and have the proper agent settings. Even if users disable agent services or delete files, agent health will restore the agent status and files to a working state.

Agent health uses a vulnerability definition for each agent component that comes from the Ivanti Software update server. When the vulnerability scanner runs on managed devices that use agent health, the scanner uses these definitions to verify the agent status, in addition to its other tasks. By default, the vulnerability scanner runs once a day.
Any changes to component settings that are part of an agent health setting are applied automatically during agent health checks. If a setting is part of an active agent health setting, you won’t need to schedule a task separately if that component setting changes.

Agent health also runs LANDeskAgentBootstrap.exe once a day on devices using agent health. This program checks to see if the vulnerability scanner is present and working. If it has been tampered with or isn’t available, this program installs it again and uses the vulnerability scanner to restore agent health.

Agent health has three main parts:

1. Agent components and their install state
2. Enforcement
3. Agent settings to apply for each component

To configure agent health

1. Click Tools > Configuration > Agent settings.
2. In the Agent settings tree, right-click Agent health and click New, or double-click an existing agent health setting.
3. Configure agent health as described in the following sections.

Downloading agent health vulnerability definitions

Before using agent health, you need to download the agent health vulnerability definitions.

To download agent health vulnerability definitions

1. Click Tools > Configuration > Agent settings.
2. In the toolbar, click the Download updates button.
3. In the Updates tab’s Definition types tree, navigate to Windows > Software updates > Ivanti 2017 Agent Health. Click it.
4. Click Download now or schedule it to download later.

About Agent health: General

Use the General page to set the Autofix and Reboot global behavior overrides.

- **Autofix:** If a component uses the security scan autofix option, you can globally keep the existing autofix setting, allow it, or disable it.
- **Reboot:** Globally leave reboot behavior as configured, allow Ivanti reboot, or disable Ivanti reboot. When reboot is disabled, Ivanti agents won’t reboot devices even if an action was taken that requires a reboot. Devices will have to be rebooted manually in this case.
About Agent health: Components

Use the Components page to configure install state actions for each agent component. Most components can have these install states:

- **Do nothing:** Leaves the component as is, whether it is installed or not.
- **Install:** Makes sure the component is installed and stays installed.
- **Remove:** Removes the component if it is installed. This doesn’t remove files associated with the component, but it does deactivate the component on the managed device. This option isn’t available for the Base agent component.

About Agent health: Enforcement

Use the Enforcement page to specify the vulnerability definitions to use when managing agent health.

**Periodically scan for agent health issues using the following group:** Enable this if you want agent health to be actively managed, either with an event-driven schedule or a time-based schedule. When it is enabled, you must select a vulnerability group. To use the Ivanti default agent health vulnerability definitions, click the browse button and select Predefined groups > Agent health. You won’t be able to select this group unless you’ve first downloaded the Ivanti agent health vulnerability definitions.

If you’ve enabled this option, you can configure when agent health scans occur.

About Agent health: Settings

Use the Settings page to assign a specific settings configuration to agent components. You can only assign settings to components that you’ve set to the “Install” state on the Components page.

**Apply settings listed below**

- **Only if associated settings aren’t specified:** When selected, component settings you configure below this option are only assigned if the component is installed but doesn’t have a setting assigned to it. If a component already has a setting, it won’t be overwritten.
- **Always:** The component setting you configure below will always be applied, even if the component already has a different setting.

**Specify settings list**

Components that you set to the “Install” state on the Components page appear in this list, along with the default setting associated with that component.

Click a setting name to keep the current component setting or to select a different existing component setting.

Click Edit to edit the selected setting, or Configure to manage the list of available settings for that component.
**Agent settings: Agent watcher**

*Tools > Configuration > Agent settings > Agent watcher*

Use this dialog box to create and edit 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 box 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 select 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 the Agent Watcher settings.
- **Monitor these files:** Specifies which critical files will be monitored with the Agent Watcher settings.
- **Polling interval:** Specifies how often you want Agent Watcher to monitor the selected services and files. The minimum value 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 have been modified during that time span, the new settings are 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.

---

**IMPORTANT:** 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.

---

**Agent settings: Ivanti Antivirus**

Ivanti Antivirus features are accessed from the Agent Settings tool window (*Tools > Security and Compliance > Agent Settings*). In the Agent settings window, right-click Ivanti Antivirus in the Security folder, then click **New**...
Antivirus allows 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 Ivanti Antivirus introduces this complementary security management tool, which is a component of both Ivanti® Endpoint Manager powered by Landesk and Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk. 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 help topics that describe the Antivirus Settings dialog. From the console interface, access these topics by clicking the Help button on each dialog box.

About the Ivanti Antivirus General page

Use this page to configure Ivanti Antivirus scanner settings on target devices.

This page contains the following options:

- **Name:** Identifies the antivirus settings with a unique name. This name will appear in the Agent settings list in the console and in the Antivirus scan task dialog box.
- **Protection:**
  - **File Antivirus:** Enables real-time scanning of files on target devices.
  - **Mail Antivirus:** Enables real-time email scanning on target devices. Real-time email scanning continuously monitors incoming and outgoing messages, checking for viruses in both the body of the message and any attached files and messages. Any detected viruses are removed.
  - **Web Antivirus:** Enables real-time scanning of web traffic, website URLs, and links on target devices.
  - **IM Antivirus:** Enables real-time scanning of instant messages on target devices.
  - **Network Attack Blocker:** Enables the Network Attack Blocker that detects and adds attacking computers to the list of blocked devices for a specified period of time.
  - **System Watcher:** Enables the System Watcher utility that monitors application activity on target devices.
• **User interface:**
  
  • **Show Ivanti Antivirus icon in system tray:** Makes the Ivanti 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.
  
  • **Enable database out-of-date and obsolete warning messages:** Allows Ivanti Antivirus to display warning messages when the database is out-of-date or obsolete. Specifies the number of days for each status.
  
  • **Do not send Ivanti Antivirus reboot status:** Select this option if you do not want Ivanti Antivirus to send the reboot status to the core. By default, Ivanti Antivirus sends a status update about whether or not it requires a reboot to complete an install or update. The status will appear in **Security activity | Ivanti Antivirus | Activity** and the core will set ‘Reboot Needed’ inventory information under **Computer | Ivanti Management**.
  
  • **Set As Default:** Establishes the settings on all of the pages of the Ivanti Antivirus dialog box as the default settings. The name you entered will appear in the console with the default icon next to it. You cannot delete a setting that is marked as default. When you create a new agent configuration, those settings will be selected by default. Unless an antivirus scan task has specific antivirus settings associated with it, Ivanti Antivirus will use the default settings during scan and definition file update tasks.

---

**About the Ivanti Antivirus Permissions page**

Use this page to configure Ivanti Antivirus permissions settings on target devices.

This page contains the following options:

• **Allow user to disable protection components for up to:** Specifies the period of time during which the user can turn off the protection components listed on the **Protection** page.

• **Allow user to update definitions:** Allows the user to update antivirus definition files.

• **Allow user to restore objects:** Allows the user to restore objects quarantined backed up objects.

• **Allow user to change settings:** Allows the user to configure settings and edit tasks.
  
  • **Allow user to schedule scans:** Allows the user to schedule scans.

• **Allow user to exclude objects from scanning:** Allows the user to exclude objects from scanning.

• **Allow users to add Web URLs:** Allows the user to add Web URLs.

• **Allow users to configure exclusions in Network Attack Blocker:** Allows the user to list IP addresses that Ivanti Antivirus will trust. Ivanti Antivirus will not block network attacks from these IP addresses but will still log information about such attacks.

---

**About the Ivanti Antivirus Protection page**

Use this page to configure Ivanti Antivirus protection settings on target devices.
This page contains the following options:

- **Start Ivanti Antivirus on computer startup:** Enables the automatic start of Ivanti Antivirus after the operating system loads, protecting the computer during the entire session. This option is selected by default. If you disable this option, Ivanti Antivirus will not start until the user starts it manually and the user data may be exposed to threats.

- **Enable Advanced Disinfection Technology:** If you select this option, when Ivanti Antivirus detects malicious activity in the operating system, it displays a pop-up message that suggests performing a special advanced disinfection procedure. After the user approves this procedure, Ivanti Antivirus neutralizes the threat. After completing the advanced disinfection procedure, Ivanti Antivirus restarts the computer. The advanced disinfection technology uses considerable computing resources, which may slow down other applications. If you leave this option unselected, which is the default setting, when Ivanti Antivirus detects malicious activity in the operating system, it carries out the disinfection procedure according to the current application settings. No computer restart is performed after Ivanti Antivirus neutralizes the threat.

- **Threats:** Specifies the objects for detection.
  - **Malware:** By default, Ivanti Antivirus scans for viruses, worms, and Trojan programs. On this tab, you can specify whether to scan for malicious tools.
  - **Adware, auto-dialers, other programs:** Specifies whether to control adware and legitimate applications that may be exploited by intruders to harm the computer or user data. Select Other to protect against objects such as Internet chat clients, downloaders, monitoring programs, and remote administration applications.
  - **Compressed files:** Specifies whether to scan for packed files that may cause harm and multi-packed objects.
• **Exclusions:** Specifies files, folders, or extensions for Ivanti Antivirus to exclude from the scan. Ivanti Antivirus will check the \LDClient and \Shared folders for .exe files. If those files are signed by Ivanti, Antivirus automatically excludes them from all scans and adds them to the Trusted application list.
  
  • **Realtime:** Specifies files, folders, or extensions to exclude from the scan in realtime. Click **Add...** to open the *Add excluded path* dialog, where you can specify file type and browse to the objects you want to exclude.
  
  • **Virus Scan:** Specifies files, folders, or extensions to exclude from the virus scan. Click **Add...** to open the *Add excluded path* dialog, where you can specify file type and browse to the object(s) you want to exclude.
  
  • **Monitored ports:** Specifies which ports to monitor.

  • **Monitor all network ports:** The protection components monitor data streams that are transmitted via any open network ports of the computer.

  • **Monitor only selected ports:** The protection components monitor only user-specified ports. Whatever is listed in network ports gets included and will be checked on the client. This network port monitoring mode is selected by default. Click **Settings** to open the **Network ports** dialog box, where you can create a list of monitored network ports and a list of applications.

  • **Network ports list:** This list contains network ports that are normally used for transmission of email and network traffic. Select a port for Ivanti Antivirus to monitor network traffic that passes through this network port via any network protocol. Click **Add...** to enter a new port number and description.

  • **Monitor all ports for specified applications:** Specifies whether all network ports are monitored for applications that are specified in the Applications list.

  • **Applications list:** This list contains applications that have network ports which Ivanti Antivirus will monitor. For each application, the list of applications specifies the path to its corresponding executable file. Click **Add...** to select an application from the database or browse for an application from the file location.

**About the Ivanti Antivirus Protection: File Antivirus page**

Use this page to configure the way File Antivirus works with Ivanti Antivirus on target devices. This page contains the following options:

• **Enable File antivirus:** Starts File Antivirus with Ivanti Antivirus. File Antivirus continuously remains active in computer memory and scans all files that are opened, saved, or started on the computer. By default, File Antivirus is enabled and configured with the recommended settings.
• **Security Level**: Specifies one of the three file security levels (High, Recommended, or Low). You can configure a custom file security level by selecting settings on the **General**, **Performance**, and **Additional** tabs.

**High**: File Antivirus takes the strictest control of all files that are opened, saved, and started. File Antivirus scans all file types on all hard drives, network drives, and removable storage media of the computer. It also scans archives, installer packages, and embedded OLE objects.

**Recommended**: File Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer. It also scans embedded OLE objects. With the Recommended setting, File Antivirus doesn’t scan archives or installer packages.

**Low**: Ensures the maximum scanning speed. With this setting, File Antivirus scans only files with specified extensions on all hard drives, network drives, and removable storage media of the computer. File Antivirus won’t scan compound files.

If you choose to create a custom security level, be sure to consider the working conditions and current situation.

• **General**: Specifies whether Antivirus scans by file format, extension, or both.
  
  • **File types**: There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then regardless of the extension, File Antivirus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware.
  
  • **Protection scope**: Specifies which drives to scan.
- **Performance**: Specifies the scan methods, whether to only scan new files, and how to handle compound files.
  - **Heuristic analysis**: This technology detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as *probably infected*.
  - **Scan new and changed files only**: Enables File Antivirus to scan only new files and files that have been modified since the previous scan.
  - **Scan archives**: Enables File Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.
  - **Scan installation**: Enables File Antivirus to scan installation packages.
  - **Scan embedded OLE objects**: Enables File Antivirus to scan files that are embedded in another file, such as Microsoft® Office Excel® spreadsheets, macros that are embedded in Microsoft® Office Word® files, or email attachments.
  - **Additional...**: Opens the **Compound files** dialog box, where you can specify whether to unpack compound files in the background and set a size limit for compound files.

- **Additional**: Specifies the mode and technology File Antivirus will use and when it will pause.
  - **Scan mode**: The default scan mode is **Smart mode**, in which File Antivirus scans files by analyzing operations performed with a file by the user, an application, or the operating system. In the **On access and modification** mode, File Antivirus scans files when the user, an application, or the operating system attempts to open or modify the files. In the **On access** mode, File Antivirus scans files only when the user, an application, or the operating system attempts to open the files. In the **On execution** mode, File Antivirus scans files only when the user, an application, or the operating system attempts to run files.
  - **Scan technologies**: Specifies the scan technologies that File Antivirus uses when scanning files. By default, the **iChecker** and **iSwift** technologies are mutually complementary. This speeds up scanning of objects that are from various file systems and operating systems.
  - **Pause task**: Specifies when to pause File Antivirus. The **By schedule** option allows pausing File Antivirus for a specified time. This feature can decrease the load on the operating system. Click **Schedule**... to open the **Pausing the task** window. In this window, you can specify the time interval for which File Antivirus is paused. The **At application startup** option pauses File Antivirus while the user works with applications that require significant resources from the operating system. This option is not selected by default. Click **Select**... to open the **Applications** window, where you can create a list of applications that pause File Antivirus when they are running.
• **Action:** Specifies the action that File Antivirus performs if infected files are detected. Before attempting to disinfect or delete an infected file, File Antivirus creates a backup copy for subsequent restoration or disinfection.
  
  • **Select action automatically:** Enables File Antivirus to perform the default action that is specified by Ivanti. This action is 'Disinfect. Delete if disinfection fails.'
  
  • **Perform actions:** Enables File Antivirus to automatically attempt to disinfect all infected files that are detected. If disinfection fails, File Antivirus deletes those files.
    
    • **Disinfect:** Enables File Antivirus to automatically attempt to disinfect all infected files that are detected. File Antivirus applies the Delete action to files that are part of the Windows Store application.
    
    • **Delete if disinfection fails:** Enables File Antivirus to automatically delete all infected files that it detects.

**About the Ivanti Antivirus Protection: Mail Antivirus page**

Use this page to configure the way Mail Antivirus works with Ivanti Antivirus on target devices.

This page contains the following options:

• **Enable Mail Antivirus:** Starts Mail Antivirus with Ivanti Antivirus. Mail Antivirus continuously remains active in computer memory and scans all email messages that are transmitted via the POP3, SMTP, IMAP, MAPI, and NNTP protocols. By default, Mail Antivirus is enabled and configured with the recommended settings.
• **Security Level:** Specifies one of the three file security levels (High, Recommended, or Low). You can configure a custom mail security level by selecting settings on the General, Performance, and Additional tabs.

  **High:** Mail Antivirus scans email messages most thoroughly. Mail Antivirus scans incoming and outgoing messages and performs deep heuristic analysis. The High mail security level is recommended when working in a dangerous environment, such as a connection to a free email service from a home network that is not guarded by centralized email protection.

  **Recommended:** Provides the optimal balance between the performance of Ivanti Antivirus and email security. Mail Antivirus scans incoming and outgoing email messages, and performs middle-intensity heuristic analysis. This mail traffic security level is recommended by Ivanti. This is the default setting.

  **Low:** Scans only incoming email messages, performs light heuristic analysis, and doesn’t scan archives that are attached to email messages. At this mail security level, Mail Antivirus scans email messages at maximum speed and uses a minimum of operating system resources. The Low mail security level is recommended for use in a well-protected environment, such as a LAN with centralized email security.

If you choose to create a custom security level, be sure to consider the working conditions and current situation.

• **General:**
  
  • **Protection scope:** Specifies whether to scan incoming and outgoing messages or incoming messages only.

  • **POP3 / SMTP / NNTP / IMAP traffic:** Enables Mail Antivirus to scan emails before they are received on the computer. If you clear this option, Mail Antivirus will not scan email messages that are transferred via the POP3, SMTP, NNTP, and IMAP protocols before they arrive on your computer. Instead, Mail Antivirus plug-ins that are embedded into the Microsoft Office Outlook and The Bat! email clients will scan the messages after they arrive on your computer.

  • **Additional: Microsoft Office Outlook plug-in:** Enables access to the Mail Antivirus settings from Microsoft Office Outlook so you can configure the component to scan email messages for viruses and other malware. A plug-in embedded into Microsoft Office Outlook is enabled to scan email messages transmitted via the POP3, SMTP, NNTP, IMAP and MAPI protocols after they arrive on your computer.

  • **Additional: The Bat! plug-in:** Enables the plug-in embedded into The Bat! to scan email messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they are received on your computer.

  • **Scan attached archives:** Enables Mail Antivirus to scan archives that are attached to email messages. You can specify the size of archives to scan and the amount of time allocated for the scanning of archived email attachments.
- **Attachment filter:**
  - **Disable filtering:** Specifies whether Mail Antivirus filters files that are attached to email messages.
  - **Rename specified attachment types:** Enables Mail Antivirus to replace the last character in attached files of the specified types with the underscore (_) symbol.
  - **Delete specified attachment types:** Enables Mail Antivirus to delete attached files of the specified types from the email messages. You can specify the types of attached files to delete from emails in the Extension list.

- **Additional:** Specifies whether Mail Antivirus will use heuristic analysis during scanning of email. This technology detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as *probably infected*. Move the slider along the horizontal axis to change the detail level for heuristic analysis. The detail level for heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of heuristic analysis are available:

  **Light scan:** Heuristic Analyzer doesn’t perform all instructions in executable files while scanning email for malicious code. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Email scanning is faster and less resource-intensive.

  **Medium scan:** When scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti. The medium scan detail level is selected by default.

  **Deep scan:** When scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Email scanning consumes more system resources and takes more time.
Action:

- **Select action automatically**: Enables Mail Antivirus to perform the default action that is specified by Ivanti. This action is to disinfect all infected email messages that are detected and if disinfection fails, to delete them.

- **Perform actions**: Mail Antivirus automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, Mail Antivirus deletes them. If this option is selected, Mail Antivirus automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, Mail Antivirus moves them to Quarantine.
  
  - **Disinfect**: Mail Antivirus automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, Mail Antivirus moves them to Quarantine.
  
  - **Delete**: Mail Antivirus automatically deletes all infected email messages that are detected.

**About the Ivanti Antivirus Protection: Web Antivirus page**

Use this page to configure the way Web Antivirus works with Ivanti Antivirus on target devices.

This page contains the following options:

- **Enable Web Antivirus**: Web Antivirus starts with Ivanti Antivirus and protects information that arrives on the computer via the HTTP and FTP protocols. By default, Web Antivirus is enabled and configured with the recommended settings.
• **Security Level:** Specifies one of the three file security levels (High, Recommended, or Low). You can configure a custom web security level by selecting settings on the Scan methods and optimization and Trusted URLs tabs.

**High:** Web Antivirus performs maximum scanning of web traffic that the computer receives via the HTTP and FTP protocols. Web Antivirus scans in detail all web traffic objects, with use of the full set of application databases, and performs the deepest possible heuristic analysis. This technology was developed for detecting threats that cannot be detected by using the current version of Ivanti databases. It detects files that may be infected with an unknown virus or a new variety of a known virus. Files in which malicious code is detected during heuristic analysis are marked as *probably infected*.

**Recommended:** Provides the optimal balance between the performance of Ivanti Antivirus and the security of web traffic. Web Antivirus performs heuristic analysis at the Medium scan level. This default web traffic security level is recommended by Ivanti.

**Low:** Ensures the fastest scanning of web traffic. Web Antivirus performs heuristic analysis at the Light scan level.

If you choose to create a custom security level, be sure to consider the working conditions and current situation.

• **Scan methods and optimization:**
  
  • **Check if links are listed in the database of suspicious URLs:** Specifies whether to scan URLs against the database of malicious web addresses. Checking URLs against the database of malicious web addresses helps to detect websites that are in the black list of web addresses.
  
  • **Check if links are listed in the database of phishing URLs:** Specifies whether to scan URLs against the database of phishing web addresses. The database of phishing URLs includes the web addresses of currently known websites that are used to launch phishing attacks.
  
  • **Heuristic analysis for detecting viruses:** Specifies whether to use heuristic analysis when scanning web traffic for viruses and other malicious programs. The technology was developed for detecting threats that cannot be detected by using the current version of Ivanti application databases. It detects files that may be infected with an unknown virus or a new variety of a known virus. Files in which malicious code is detected during heuristic analysis are marked as *probably infected*.
  
  • **Heuristic analysis for phishing links:** Specifies whether to heuristic analysis when scanning web pages for phishing links.
- **Limit web traffic caching time:** Scans cached fragments of web traffic objects for one second. If the option is cleared, Web Antivirus performs deeper web traffic scanning. Access to web traffic objects may become slower during scanning.

- **Trusted URLs:**
  - **Do not scan web traffic from trusted URLs:** Specifies whether to scan the content of websites whose addresses are included in the list of trusted URLs. Click **Add** to open the **Address mask (URL)** window, where you can enter a URL and enable or disable it. If a URL is disabled, Web Antivirus temporarily excludes it from the list of trusted URLs.

- **Action:**
  - **Select action automatically:** Enables Web Antivirus to perform the default action that is specified by Ivanti when it detects an infected object in web traffic. The default action is 'Block download.'
  - **Block download:** Enables Web Antivirus to block access to an infected object and display a notification about the object.
  - **Allow download:** Enables Web Antivirus to allow an infected object to be downloaded to your computer.

**About the Ivanti Antivirus Protection: IM Antivirus page**

Use this page to configure the way IM Antivirus works with Ivanti Antivirus on target devices.

This page contains the following options:

- **Enable IM Antivirus:** IM Antivirus starts with Ivanti Antivirus, remains constantly in the computer's RAM, and scans all messages that arrive through Internet messaging clients. IM Antivirus ensures the safe operation of numerous instant messaging applications, including ICQ, MSN® Messenger, AIM, Mail.Ru Agent, and IRC.

- **Protection scope:** Specifies the type of messages that are transmitted by IM clients to be scanned by IM Antivirus.
  - **Incoming and outgoing messages:** IM Antivirus scans both incoming and outgoing instant messages for malicious objects or URLs that are in databases of malicious and phishing web addresses. This is the default setting.
  - **Incoming messages only:** IM Antivirus scans only incoming instant messages for malicious objects or URLs that are in databases of malicious and phishing web addresses. IM Antivirus doesn't scan outgoing messages.
• **Scan methods**: Specifies the methods that IM Antivirus uses when scanning messages that arrive through IM clients.

  • **Check if links are listed in the database of suspicious URLs**: Specifies whether to scan URLs in IM client messages against the database of malicious URLs.

  • **Check if the links are listed in the database of phishing URLs**: Specifies whether to scan URLs in IM client messages against the database of phishing URLs.

  • **Heuristic analysis**: Specifies whether IM Antivirus will use heuristic analysis scanning IM client messages. This technology detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as *probably infected*. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail level for Heuristic Analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic Analysis are available:

    • **Light Scan**: Heuristic Analyzer scans instant messages for threats by using a minimum set of attributes. Scanning is faster and less resource-intensive, with the least number of false positives.

    • **Medium scan**: Heuristic Analyzer scans instant messages for threats by using the number of attributes that ensures the optimum balance between the speed and detail of scanning and avoids a large number of false positives. This level of detail for heuristic analysis is set by default.

    • **Deep scan**: Heuristic Analyzer scans instant messages for threats by using a maximum set of attributes. The scan is performed in detail, requires more operating system resources, and takes more time. False positives are probable.

**About the Ivanti Antivirus Protection: Network Attack Blocker page**

Use this page to configure the Network Attack Blocker that Ivanti Antivirus uses on target devices to detect and add attacking computers to the list of blocked devices for a specified period of time.

This page contains the following options:

• **Enable Network Attack Blocker**: Network Attack Blocker starts with Ivanti Antivirus and scans incoming network traffic for network activity that is characteristic of network attacks. After detecting an attempted network attack, Network Attack Blocker blocks network activity from an attacking computer that targets the user’s computer.

• **Add the following computer to the list of blocked computers for (minutes)**: Specifies the number of minutes that Network Attack Blocker will block network activity from an attacking computer. This block automatically protects the user’s computer against possible future network attacks from the same address. The default value is 60 minutes.
• **Configure addresses of exclusions:** Specifies IP addresses from which network attacks will not be blocked, although information about such attacks will be logged. Click the Exclusions... button to open the Exclusions window, where you can add IP addresses.

**About the Ivanti Antivirus Protection: System Watcher page**

Use this page to configure System Watcher, which Ivanti Antivirus uses to monitor application activity on target devices. System Watcher settings only take effect after the next reboot.

This page contains the following options:

• **Enable System Watcher:** Enables the functionality specified in the System Watcher settings.

• **Enable Exploit Prevention:** Enables Ivanti Antivirus to keep track of executable files launched by vulnerable applications. On detecting that an attempt to run an executable file from a vulnerable application was not initiated by the user, Ivanti Antivirus blocks the launch of this file. Ivanti Antivirus stores information about the blocked launch of the executable file in the Exploit Prevention report.

• **Log application activity for the BSS database:** Enables the logging of application activity. This information is used to update the BSS (Behavior Stream Signatures) database. System Watcher logs application activity by default.

• **Do not monitor the activity of applications that have a digital signature:** Ivanti Antivirus adds digitally signed applications to the Trusted group and doesn’t monitor the activities of applications from this group.

• **Rollback of malware actions:** Allows rolling back malware actions in the operating system while disinfection is in progress. This option is selected by default.
**Proactive Defense:** Specifies whether Ivanti Antivirus will analyze the activity of an application and what action it will take if it determines the activity is malicious.

**Use behavior stream signatures (BSS):** Specifies whether to use BSS (Behavior Stream Signatures) technology, which involves analyzing the behavior of applications based on information that is collected about their activities. System Watcher looks for similarities between the actions of an application and the actions of malware. If System Watcher analyzes the activity of an application and determines that it is malicious, System Watcher performs the action that you specified in the **On detecting malware activity** list.

**On detecting malware activity:** Specifies the action that Ivanti Antivirus performs upon detection of malicious activity.

- **Select action automatically:** Ivanti Antivirus performs the default action that is specified by Ivanti. By default, Ivanti Antivirus moves the executable file of a malicious application to Quarantine.
- **Move file to Quarantine:** Ivanti Antivirus moves the executable file of a malicious application to Quarantine.
- **Terminate the malicious program:** Ivanti Antivirus terminates the application.
- **Skip:** Ivanti Antivirus doesn’t take any action on the executable file of a malicious application.

**About the Ivanti Antivirus: Scheduled Tasks page**

Use this page to create a scheduled task that will be performed by the Ivanti Local Scheduler tool. These tasks are separate from the tasks that can be scheduled via the Ivanti Antivirus client on the managed device. Note that task notifications that appear in the client interface refer to the Ivanti Antivirus client’s native scheduler, not the core server’s Local Scheduler tool.

This page contains the following options:

- **Scheduled tasks:** Creates a scheduled task that will be performed by Ivanti Antivirus on the managed device. These tasks are separate from the tasks that can be scheduled via the Ivanti Local Scheduler tool.
  - **Update:** Specifies when to update virus definitions. Click **Change schedule...** to open the **Schedule periodic virus definition updates** window, where you can select the events that will trigger an update, the time of an update, and the filters.
  - **Full Scan:** Specifies when to do a full scan. Click **Change schedule...** to open the **Schedule periodic antivirus scans** window, where you can select the events that will trigger a scan, the time of a scan, and the filters.
  - **Critical Areas Scan:** Specifies when to scan critical areas only. Click **Change schedule...** to open the **Schedule periodic antivirus scans** window, where you can select the events that will trigger a scan, the time of a scan, and the filters.
• **Background scan tasks:** Specifies whether to performing the background scan of the system memory, startup objects, and the system partition while the computer is idle to optimize the use of computer resources.
  
  • **Perform idle scan:** Starts a scan task for autorun objects, RAM, and the operating system partition when the computer is locked or the screen saver is on for 5 minutes or longer, if one of the following conditions is true:
    
    • An idle scan of the computer has not occurred since the installation of Ivanti Antivirus.
    • The last idle scan of the computer occurred more than 7 days ago.
    • The last idle scan of the computer was interrupted during an update of the application databases and modules.
    • The last idle scan of the computer was interrupted during an on-demand scan.

• **Scan removable drive on connection:** Specifies whether to scan a removable drive when it is connected to the computer.

  • **Action on removable drive connection:** Allows you to select the action that Ivanti Antivirus will perform when you connect a removable drive to the computer.
    
    • **Do not scan:** Ivanti Antivirus doesn’t run a scan and doesn’t prompt you to select an action to perform when a removable drive is connected.
    • **Full scan:** Ivanti Antivirus starts a full scan of the removable drive according to the Full Scan task settings.
    • Quick scan: Ivanti Antivirus starts a start a scan of the removable drive according to the Critical Areas Scan task settings.

• **Maximum removable drive size (MB):** Specifies the size of removable drives on which Ivanti Antivirus performs the action that is selected in the Actions on drive connection list. The default size is 4096 MB.

**About the Ivanti Antivirus Scheduled Tasks: Update page**

Use this page to configure virus definition (pattern) file updates scheduling, user download options, and access options, for target devices with these antivirus settings. To schedule an update, select **Update** on the Scheduled Tasks page.

This page contains the following options:

  • **Download "pilot" version of virus definition files:** Download virus definition files from the pilot folder instead of from the default \LDLogon\Antivirus8\Win\BasesEP 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\Antivirus8\Win\BasesEP) are not downloaded.
• **Download virus definition updates from:** Specifies the source site (core server or Kaspersky content server) from which virus definition files are downloaded.

• **Preferred server/Peer download options:** Allows you to configure core server settings if you’ve selected one of the download source site options that includes the core.
  
  • *Attempt peer download:* Prevents virus definition file downloads via peer download (the local cache or a peer in the same multicast domain).
  
  • *Attempt preferred server:* Prevents virus definition file downloads via a preferred server. For more information about preferred servers, see "About software distribution" (457).

• **Bandwidth used from core or preferred server (WAN):** Specifies the bandwidth used. You can move the slider or enter a value in the percentage box.

• **Bandwidth used peer-to-peer (Local):** Specifies the bandwidth used. You can move the slider or enter a value in the percentage box.

• **Application update settings:** Specifies whether to update application modules.
  
  • *Update application modules:* Enables downloads of application module updates along with antivirus database updates. If selected, Ivanti Mac Antivirus includes application module updates in the update package when the application runs the update task. This option is selected by default.

• **Scan removable drive on connection:** Specifies whether to scan a removable drive when it is connected to the computer.
  
  • **Action on removable drive connection:** Allows you to select the action that Ivanti Antivirus will perform when you connect a removable drive to the computer.
    
    • *Do not scan:* Ivanti Antivirus doesn’t run a scan and doesn’t prompt you to select an action to perform when a removable drive is connected.
    
    • *Full scan:* Ivanti Antivirus starts a full scan of the removable drive according to the [Full Scan](#) task settings.
    
    • *Quick scan:* Ivanti Antivirus starts a start a scan of the removable drive according to the [Critical Areas Scan](#) task settings.
    
    • **Maximum removable drive size (MB):** Specifies the size of removable drives on which Ivanti Antivirus performs the action that is selected in the [Actions on drive connection](#) list. The default size is 4096 MB.

**About the Schedule periodic antivirus scans dialog box**

If you want this antivirus settings to include a recurring antivirus scan, use this dialog box 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 box 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 box contains the following options:

- **Run when user logs in**: The scan will occur when the user logs into the machine.
- **Run whenever the machine’s IP address changes**: The scan will occur when the machine’s IP address changes.
- **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 Ivanti Antivirus Scheduled Tasks: Full Scan page**

Use this page to configure the way Ivanti Antivirus performs full scans on target devices. To schedule a full scan, select **Full Scan** on the **Scheduled Tasks** page.

This page contains the following options:

• **Security Level:** Specifies one of the three file security levels (High, Recommended, or Low).

  **High:** If the probability of computer infection is very high, select this file security level. Ivanti Antivirus scans all types of files. When scanning compound files, Ivanti Antivirus also scans mail-format files.

  **Recommended:** Ivanti Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives or installation packages.

  **Low:** Ensures maximum scanning speed. Ivanti Antivirus scans only new or modified files with the specified extensions on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives, installation packages, or compound files.

• **Scope:** You can expand or restrict the scan scope by adding or removing scan objects or by changing the type of files to be scanned. By default, a full scan includes system memory, startup objects, disk boot sectors, system backup storage, email, hard drives, and removable drives.

  • **File types:** Specifies whether to scan files by format, extension, or both. There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files...
by format is selected, then regardless of the extension, Ivanti Antivirus analyzes
the file header. This analysis may reveal that the file is in .exe format. Such a file is
thoroughly scanned for viruses and other malware.

- **Scan only new and changed files**: Enables Ivanti Antivirus to scan only new files
  and files that have been modified since the previous scan.

- **Skip files that are scanned for longer than**: Specifies in seconds the length of
time to scan a file before skipping it.

- **Scan archives**: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and
  ICE archives. On a full scan, this option is enabled by default.

- **Scan installation packages**: Enables Ivanti Antivirus to scan installation packages.
  On a full scan, this option is enabled by default.

- **Scan embedded OLE objects**: Enables Ivanti Antivirus to scan files that are
  embedded in another file (such as Microsoft® Office Excel® spreadsheets,
  macros that are embedded in Microsoft® Office Word® files, or email
  attachments). On a full scan, this option is enabled by default.

- **Parse email formats**: Enables Ivanti Antivirus to parse email formats during the
  scan.

- **Scan password-protected archives**: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP,
  CAB, LHA, JAR, and ICE archives that are password-protected.

- **Additional**: Click this button to open the **Compound files** window, where you
  can specify whether to unpack compound files in the background and set a size
  limit for compound files.
• **Additional:** Specifies the method and technology Ivanti Antivirus will use during a full scan.

  • **Scan methods:** Heuristic analysis detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as *probably infected*. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail level for Heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic analysis are available:
    
    1. **Light scan:** Heuristic Analyzer doesn't perform all instructions in executable files while scanning. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Scanning is faster and less resource-intensive.
    2. **Medium scan:** When scanning, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti. The medium scan detail level is selected by default.
    3. **Deep scan:** When scanning for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Scanning consumes more system resources and takes more time.

  • **Scan technologies:** Specifies the scan technologies that Ivanti Antivirus uses when scanning files. By default, the *iChecker* and *iSwift* technologies are mutually complementary. These technologies optimize the speed of scanning files by excluding files that have not been modified since the most recent scan.

• **Action:** Specifies the action that Ivanti Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Antivirus creates a backup copy for subsequent restoration or disinfection.

  • **Select action automatically:** Ivanti Antivirus performs the default action that is specified by Ivanti. This action is ‘Disinfect. Delete if disinfection fails.’ This action is selected by default.

  • **Perform actions:** Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. If disinfection fails, Ivanti Antivirus deletes those files.
    
    1. **Disinfect:** Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Antivirus applies the ‘Delete’ action to files that are part of the Windows Store application.
    2. **Delete if disinfection fails:** Ivanti Antivirus automatically deletes all infected files that it detects.
About the Ivanti Antivirus Scheduled Tasks: Critical Areas Scan page

Use this page to configure the way Ivanti Antivirus performs critical areas scans on target devices. To schedule a critical areas scan, select Critical Areas Scan on the Scheduled Tasks page.

This page contains the following options:

- **Security Level**: Specifies one of the three file security levels (High, Recommended, or Low).
  
  **High**: If the probability of computer infection is very high, select this file security level. Ivanti Antivirus scans all types of files. When scanning compound files, Ivanti Antivirus also scans mail-format files.
  
  **Recommended**: Ivanti Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives or installation packages.
  
  **Low**: Ensures maximum scanning speed. Ivanti Antivirus scans only new or modified files with the specified extensions on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives, installation packages, or compound files.
  
- **Scope**: You can expand or restrict the scan scope by adding or removing scan objects or by changing the type of files to be scanned. By default, a critical areas scan includes only system memory, startup objects, and disk boot sectors.
  
  **File types**: Specifies whether to scan files by format, extension, or both. There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then regardless of the extension, Ivanti Antivirus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware.
  
  **Scan only new and changed files**: Enables Ivanti Antivirus to scan only new files and files that have been modified since the previous scan.
  
  **Skip files that are scanned for longer than**: Specifies in seconds the length of time to scan a file before skipping it.
  
  **Scan archives**: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives. On a critical areas scan, this option is disabled by default.
  
  **Scan installation packages**: Enables Ivanti Antivirus to scan installation packages. On a critical areas scan, this option is disabled by default.
- **Scan embedded OLE objects**: Enables Ivanti Antivirus to scan files that are embedded in another file (such as Microsoft® Office Excel® spreadsheets, macros that are embedded in Microsoft® Office Word® files, or email attachments). On a critical areas scan, this option is enabled by default.

- **Parse email formats**: Enables Ivanti Antivirus to parse email formats during the scan. On a critical areas scan, this option is enabled by default.

- **Scan password-protected archives**: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives that are password-protected.

- **Additional**: Click this button to open the **Compound files** window, where you can specify whether to unpack compound files in the background and set a size limit for compound files.

- **Additional**: Specifies the method and technology Ivanti Antivirus will use during a critical areas scan.

- **Scan methods**: Heuristic analysis detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as **probably infected**. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail level for Heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic analysis are available:
  
  - **Light scan**: Heuristic Analyzer doesn’t perform all instructions in executable files while scanning. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Scanning is faster and less resource-intensive.
  
  - **Medium scan**: When scanning, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti.
  
  - **Deep scan**: When scanning for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Scanning consumes more system resources and takes more time. For a critical areas scan, this is the default heuristic analysis level.

- **Scan technologies**: Specifies the scan technologies that Ivanti Antivirus uses when scanning files. By default, the **iChecker** and **iSwift** technologies are mutually complementary. These technologies optimize the speed of scanning files by excluding files that have not been modified since the most recent scan.
• **Action:** Specifies the action that Ivanti Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Antivirus creates a backup copy for subsequent restoration or disinfection.

  • **Select action automatically:** Ivanti Antivirus performs the default action that is specified by Ivanti. This action is 'Disinfect. Delete if disinfection fails.' This action is selected by default.

  • **Perform actions:** Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. If disinfection fails, Ivanti Antivirus deletes those files.

    • **Disinfect:** Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Antivirus applies the 'Delete' action to files that are part of the Windows Store application.

    • **Delete if disinfection fails:** Ivanti Antivirus automatically deletes all infected files that it detects.

**About the Ivanti Antivirus Scheduled Tasks: Custom Scan page**

Use this page to configure custom scans on target devices.

This page contains the following options:

  • **Security Level:** Specifies one of the three file security levels (High, Recommended, or Low).

    • **High:** If the probability of computer infection is very high, select this file security level. Ivanti Antivirus scans all types of files. When scanning compound files, Ivanti Antivirus also scans mail-format files.

    • **Recommended:** Ivanti Antivirus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won't scan archives or installation packages.

    • **Low:** Ensures maximum scanning speed. Ivanti Antivirus scans only new or modified files with the specified extensions on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Ivanti Antivirus won’t scan archives, installation packages, or compound files.

  • **Scope:** You can expand or restrict the scan scope by adding or removing scan objects or by changing the type of files to be scanned.

  • **File types:** Specifies whether to scan files by format, extension, or both. There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high. An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files
by format is selected, then regardless of the extension, Ivanti Antivirus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware.

- **Scan only new and changed files**: Enables Ivanti Antivirus to scan only new files and files that have been modified since the previous scan.

- **Skip files that are scanned for longer than**: Specifies in seconds the length of time to scan a file before skipping it.

- **Scan archives**: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.

- **Scan installation packages**: Enables Ivanti Antivirus to scan installation packages.

- **Scan embedded OLE objects**: Enables Ivanti Antivirus to scan files that are embedded in another file (such as Microsoft® Office Excel® spreadsheets, macros that are embedded in Microsoft® Office Word® files, or email attachments).

- **Parse email formats**: Enables Ivanti Antivirus to parse email formats during the scan.

- **Scan password-protected archives**: Enables Ivanti Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives that are password-protected.

- **Additional**: Click this button to open the Compound files window, where you can specify whether to unpack compound files in the background and set a size limit for compound files.
• **Additional**: Specifies the method and technology Ivanti Antivirus will use during a custom scan.
  
  • **Scan methods**: Heuristic analysis detects files that may be infected with an unknown virus. If Antivirus detects malicious code in a file during heuristic analysis, it will mark the file as *probably infected*. Move the slider along the horizontal axis to change the detail level for Heuristic Analysis. The detail level for Heuristic analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis. The following levels of detail of Heuristic analysis are available:
    
  • **Light scan**: Heuristic Analyzer doesn't perform all instructions in executable files while scanning. At this level of detail, the probability of detecting threats is lower than at the Medium scan and Deep scan levels. Scanning is faster and less resource-intensive.
  
  • **Medium scan**: When scanning, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Ivanti. The medium scan detail level is selected by default.
  
  • **Deep scan**: When scanning for malicious code, Heuristic Analyzer performs more instructions in executable files than at the Light scan and Medium scan levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the Light scan and Medium scan levels. Scanning consumes more system resources and takes more time.
  
  • **Scan technologies**: Specifies the scan technologies that Ivanti Antivirus uses when scanning files. By default, the **iChecker** and **iSwift** technologies are mutually complementary. These technologies optimize the speed of scanning files by excluding files that have not been modified since the most recent scan.
  
  • **Action**: Specifies the action that Ivanti Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Antivirus creates a backup copy for subsequent restoration or disinfection.
    
    • **Select action automatically**: Ivanti Antivirus performs the default action that is specified by Ivanti. This action is ‘Disinfect. Delete if disinfection fails.’ This action is selected by default.
    
    • **Perform actions**: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. If disinfection fails, Ivanti Antivirus deletes those files.
      
      • **Disinfect**: Ivanti Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Antivirus applies the ’Delete' action to files that are part of the Windows Store application.
      
      • **Delete if disinfection fails**: Ivanti Antivirus automatically deletes all infected files that it detects.
About the Ivanti Antivirus: Advanced settings page

Use this page to configure Ivanti Antivirus Advanced settings on target devices.

This page contains the following options:

- **Enable Self-Defense**: Prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.

- **Disable external management of the system service**: Blocks any attempts to remotely manage Ivanti Antivirus. If an attempt is made to manage application services remotely, a notification is displayed in the Microsoft Windows taskbar, above the application icon (unless the notification service is disabled by the user).

- **Send dump and trace files to Ivanti for analysis**: Sends dump and trace files to Ivanti, where the cause of the crashes will be examined. If you select this option, the **Uploading support information to server** window will open when Ivanti Antivirus restarts after a crash. In this window, you can select dump and trace files from the list and send them to Ivanti for examination.

- **Operating mode**: Allows you to configure optimum energy and computer resource consumption in the operation of Ivanti Antivirus.
  - **Do not start scheduled tasks while running on battery power**: Computer scan tasks and database update tasks tend to consume considerable resources and take a long time to finish. This option enables energy conservation mode when a portable computer is running on battery power, which postpones scan and update tasks. The user can start scan and update tasks manually, if necessary.
  - **Concede resources to other applications**: When Ivanti Antivirus runs scheduled tasks, this may result in increased workload on the CPU and disk subsystems, which slows down the performance of other applications. This option suspends scheduled tasks when it detects an increased load on the CPU and frees up operating system resources for user applications.

About the Ivanti Antivirus Advanced settings: Reports and Storages page

Use this page to configure Ivanti Antivirus Advanced Reports and Storages settings on target devices.

This page contains the following options:

- **Reports parameters**: Specifies the length of time to store a report and the maximum size of a report.
  - **Store reports no longer than (days)**: Specifies the maximum report storage term in number of days. The default maximum storage term for reports is 30 days. After that period of time, Ivanti Antivirus automatically deletes the oldest entries from the report file.
- **Maximum file size (MB):** Specifies the maximum report file size in megabytes. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Ivanti Antivirus automatically deletes the oldest entries from the report file when the maximum report file size is reached.

- **Local quarantine and backup settings:** Allows you to configure quarantine and backup settings. The data storage comprises a quarantine catalog and a storage for backup copies of files.
  
  - **Rescan quarantine after update:** Enables automatic scanning of quarantined files after each update of the databases and application software modules of Ivanti Antivirus. If you select this option, Ivanti Antivirus starts a scan of quarantined files after every update of databases and application software modules.
  
  - **Store objects no longer than:** Specifies the maximum storage term for files in quarantine and copies of files in backup. The maximum file storage term is measured in days. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Ivanti Antivirus deletes the oldest files from Quarantine and Backup.
  
  - **Maximum storage size:** Specifies the maximum data storage size in megabytes. By default, the maximum size is 100 MB. To not exceed the maximum data storage size, Ivanti Antivirus automatically deletes the oldest files when the data storage reaches its maximum size.

**About the Ivanti Antivirus Advanced settings: Interface page**

Use this page to configure the Advanced Interface settings that Ivanti Antivirus will use on target devices.

This page contains the following options:

- **Show "Protected by Kaspersky Lab" on Microsoft Windows logon screen:** Enables the "Protected by Kaspersky Lab" message on the Microsoft Windows logon screen. This option is selected by default. If the application is installed on a computer that runs on an operating system in the Microsoft Windows Vista family, this option is unavailable.

- **Use icon animation while running tasks:** Enables the animation of the application icon in the taskbar notification area of Microsoft Windows when tasks are running. This option is selected by default.

**About the Ivanti Antivirus Advanced settings: Import Kaspersky settings page**

Use this page to configure how Ivanti Antivirus will import Kaspersky settings on target devices.

This page contains the following options:

- **Import settings file from a Kaspersky antivirus client:** Lets you import settings from a client machine. To import the settings, specify Kaspersky settings on a client and save the settings as a .CFG file. From the console, browse to the .CFG file. The options listed in the .CFG file will be
set first and then any Ivanti Antivirus settings will be set. Note that Ivanti Antivirus will not look for a new .CFG update and auto-update it. You must manually update the .CFG file if you want to import different settings.

- **Current configuration imported from:** The Browse button [...] opens the **Select a previously saved Kaspersky configuration file** window. Browse to the \dlogon folder, click the .CFG file, then click **Open**.
- **Clear password after import:** Enables users to change Kaspersky settings without the settings file password.
- **Use imported scan settings:** Uses scan settings from the imported settings file.
- **On date:** The current date of the import.
- **Notes:** Any notes about the .CFG file.

**Agent settings: Antivirus legacy**

IvantiAntivirus features are accessed from the Agent Settings tool window (**Tools > Security and Compliance > Agent Settings**).

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 Ivanti Antivirus introduces this complementary security management tool, which is a component of both Ivanti® Endpoint Manager powered by Landesk and Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk. 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 help topics that describes the Antivirus dialogs. From the console interface, these help topics are accessed by clicking the **Help** button on their respective dialog box.

- "Antivirus Download Updates help" (221)
- "Antivirus tasks help" (225)
- "Antivirus settings help" (226)

**Antivirus Download Updates help**

**About the Ivanti Antivirus page on the Download Updates dialog box**

Use the **Ivanti Antivirus** page of the **Download Updates** dialog box to configure settings for downloading virus definition file updates. 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 box includes several Antivirus updates in the definition type list. Under Ivanti Antivirus Updates, there is a pattern file set for each version. When you select Ivanti AV [operating system version], 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 Ivanti 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)

**NOTE:** **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 Ivanti Antivirus updates, both the scanner detection content AND the Ivanti Antivirus-specific virus definition files are downloaded. Ivanti 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content subscription in order to download each type of security content.

A basic Ivanti® Endpoint Manager powered by Landesk installation allows you to download and scan for Ivanti 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content subscription in order to download the corresponding definitions.

For information about Endpoint Security for Endpoint Manager content subscriptions, contact your reseller, or visit the Ivanti website:

**Ivanti Home Page**

After you specify the types of content you want to download and the other options on the Download updates dialog box:

- 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 box. 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 box, enter a name for the task, verify the information for the task, and then click **OK** to add the task to Scheduled tasks.
IMPORTANT: **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 box 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 box at any time, click **Apply**.

The **Ivanti Antivirus** page contains the following options:

- **Virus definition updates**: The default folders are:
  - Ivanti AV 10.0: \LANDESK\ManagementSuite\ldlogon\antivirus8\Win\basesEP10
  - Ivanti AV 9.5 and 9.6: \LANDESK\ManagementSuite\ldlogon\antivirus8\Win\basesEP
  - Mac: \LANDESK\ManagementSuite\ldlogon\antivirus8\Mac\basesEP

  - **Immediately approve (available to all computers)**: Downloads virus definitions directly to the default folder. Virus definitions downloaded to the default folder are approved and can be deployed to target devices for antivirus scanning.

  - **Restrict them to a pilot**: 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.

    - **Get latest definitions**: Opens the Select Ivanti Antivirus version dialog box, where you can select which virus definitions to download. Click **OK** to start an immediate download of the selection, regardless of the Download Updates list. The **Updating Definitions** dialog box 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.

    - **Schedule approval**: Opens the Scheduled tasks tool with a new task where you can specify the scheduling options (start now, or start at a particular day and time, and set recurrence). This scheduled task automatically moves downloaded virus definition files from the pilot folder to the default virus definition files folder.

    **NOTE**: 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.)

  - **Make backups of previous definition files**: 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. Backups are stored under the following folders:
Ivanti AV 10.0: \LANDESK\ManagementSuite\Idlogin\antivirus8\Win\backupsEP10
Ivanti AV 9.5 and 9.6: \LANDESK\ManagementSuite\Idlogin\antivirus8\Win\backups
Mac: \LANDESK\ManagementSuite\Idlogin\antivirus8\Mac\backups

- **Number of backups to keep:** Specifies the number of virus definition file downloads to save.
- **Update backup lists:** Deletes any saved backups to match the number specified in the Number of backups to keep field. For example, if you previously kept 10 backups and then changed the value to 3, you could click the **Update backup lists** button to immediately remove the 7 oldest backup lists. If you do not click this button, the extra backups will be deleted the next time you download 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 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk web service, which has the very latest known pattern files) is noted below this field.
- **Pilot:** Note that this list appears only if you’ve selected the **Restrict them to a pilot.** This list 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.
- **Notify using Ivanti Antivirus action center:** Opens the Ivanti Antivirus action center dialog box, where you can configure which pattern file set you want to receive notifications about.
- **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 update information** dialog box, 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 box, 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 box and appear the next time you open the dialog box.

• **Close**:: Closes the dialog box without saving your latest settings changes.

For a description of the options on the other pages of the Download updates dialog box, see “About the Download updates dialog box” (693).

**Antivirus tasks help**

**About the Create Ivanti Antivirus task dialog box**

Use this dialog box 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.

NOTE: **On-demand antivirus scans**

You can also run an on-demand antivirus scan on a device via the device’s shortcut menu.

This dialog box 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 box.

  • **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 Ivanti Antivirus machines**:: Adds managed devices that have been configured with the Ivanti Antivirus agent to the task’s target devices list.

  • **Start now**:: Runs the antivirus scan on devices with the Ivanti 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.
• **Ivanti Antivirus settings**: Specifies antivirus settings used for the scan task. Antivirus settings determine whether the Ivanti 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 Ivanti Antivirus page of the Download updates dialog box to configure and schedule a virus definition file download.

**About the Ivanti Antivirus scan now task dialog box**

Use this dialog box 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 **Ivanti 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 Ivanti Antivirus settings dialog box**

Use this dialog box to create and edit an antivirus settings. Antivirus settings determine whether the Ivanti 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 virus definition pages of the Antivirus settings dialog box, 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 box contains the following pages:

- "About the Antivirus: General settings page" (227)
- "About the Antivirus: Real-time protection page" (228)
- "About the Antivirus: Virus scan page" (230)
- "About the Antivirus: Scheduled scan page" (232)
- "About the Antivirus: Virus definition updates page" (234)
About the Antivirus: Legacy virus definition updates page” (235)  
“About the Antivirus: Quarantine/Backup page” (236)

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 box.

- **Show Ivanti Antivirus icon in system tray**: Makes the Ivanti 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 Ivanti 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 Ivanti 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 Ivanti 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 Ivanti 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 Ivanti 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 box'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 box'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 Ivanti 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 Ivanti Antivirus activities. End users are notified when an infected file is detected, quarantined, deleted, skipped, or cleaned. Message dialog boxes 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 Ivanti 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. **(NOTE:** Using heuristic scanning may negatively affect performance on managed devices.)

• **Exclude the following files and folders:**
  - **Add:** Opens the Add excluded path dialog box 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 box**

Use this dialog box (accessed from the Real-time protection dialog box) 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 box 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 box 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.

---

**IMPORTANT: System restore point scanning**

Ivanti 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
About the Antivirus: Scheduled scan page

Use this page to enable and configure a recurring scheduled antivirus scan on target devices.

NOTE: Ivanti 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 Ivanti 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 box where you can set the scheduling options.
- **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 box

If you want this antivirus settings to include a recurring antivirus scan, use this dialog box 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 box 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 box 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 network 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 network 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 Ivanti Antivirus client and can be accessed from that dialog box as well as by right-clicking the Ivanti 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) Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content server (Internet).

- **Download virus definition updates 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. (NOTE: Internet download options are configured on the **Legacy virus definition updates** page.)
• **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.
  
  • **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 "About software distribution" (457).
  
  • **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 schedule**: Opens the Schedule dialog box where you can specify the scheduling options.

### About the Schedule periodic antivirus updates dialog box

If you want this antivirus settings to include a recurring virus definition update, use this dialog box 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.

### About the Antivirus: Legacy virus definition updates page

Use this page to configure legacy virus definition updates settings, as well as the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content server settings if you've selected one of the download source site options above that includes the Internet.

This page contains the following options:

• **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 compressed and downloaded as a single file.

• **Internet download options**: Lets you configure the 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.

---

**IMPORTANT: Legacy settings apply to older Ivanti Antivirus clients only**

The legacy virus definition updates settings specified on this page will be in effect only for older versions of the Ivanti Antivirus client that have been deployed to your managed devices. Typically, older versions of the client are installed by a Ivanti core server version 8.8 SP3 or older.
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 Ivanti 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 Ivanti 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 selected, 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.

**Agent settings: Application Control**

**Tools > Security and Compliance > Agent settings > Security > Endpoint security > Application control**

Use this dialog box to create and edit an endpoint security (EPS) application control setting (configuration file). When creating EPS settings, you first define the general requirements and actions, and then add specific file certifications. You can create as many EPS settings as you like and edit them at any time.
If you want to modify the device default EPS settings without reinstalling the EPS agent or redeploying a full agent configuration, make your changes to any of the options on the EPS settings dialog box, assign the new settings to a Change settings task, and then deploy that task to targeted devices.

This dialog box contains the following pages:

- "About the General settings page" (238)
- "About the Mode configuration page" (240)
- "About the File protection rules page" (241)

### About the General settings page

Use this page to configure the general protection settings and actions for EPS.

- **Name**: Identifies the EPS settings with a unique name. This name appears in the EPS settings list on an Install or Update security components task dialog box.
• **Protection settings**: Provides two types of protection: EPS and whitelist. You can select one or both. Both protection types use the same operating mode, which you select on the Mode configuration page. **(NOTE: This general protection enforcement has one exception. If you specify the Learn protection mode and have the Whitelist-only learning option selected, only whitelist applications are learned and EPS protection is set to the automatic blocking mode.)**

  • **Enable application behavior protection**: Turns on EPS protection, allowing all programs to run (except when the program operation threatens system security) as defined by predefined protection rules. You can grant special rights to program files via trusted file lists by configuring custom file certifications. EPS protection observes application behavior (whether the application is allowed to modify another executable, modify the registry, and so on) 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**: We 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.

  • **Restrict access to physical drives**: Block access to the master boot record (MBR), helping protect clients from ransomware that encrypts the MBR.

  • **Auto-detect and blacklist crypto-ransomware**: The EPS agent will watch for encryption process and if detected, EPS will kill the process, try to remove it from startup, and add it to the blacklist. EPS will detect encryption processes as soon as possible, but it is likely that some files will be encrypted before the process can be killed. We recommend you use file protection rules to protect files from being encrypted by ransomware.

  • **Enable whitelist protection**: Turns on whitelist protection. This means only those applications that are in a trusted file list, and whose file certification has the Allow execution option enabled, are allowed to run.

  • **Prevent Windows Explorer from modifying or deleting executable files**: Enable this option if you don’t want Windows to be able to modify or delete any executable files.

  • **Treat “good reputation” files as if they are in the associated trusted file list**: Whitelists files that are in the Ivanti-hosted database of known good files. For more information, see "Using file reputation to restrict applications" (757).
- **Treat "bad reputation" files as if they are in the blacklist**: Blacklists files that are in the Ivanti-hosted database of known bad files.

- **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. EPS monitors the contents of startup and if it finds a new process, it performs the action you select (Alert and prompt for action; Always allow the program to run; or Remove the program from the Startup without alerting).

- **Set as default**: Assigns this setting as the default setting for tasks that use EPS settings.

- **ID**: Identifies this particular setting. This information is stored in the core database and can be used to keep track of each setting.

- **Save**: Saves your changes and closes the dialog box.

- **Cancel**: Closes the dialog box without saving your changes.

**About the Mode configuration page**

Use this page to configure the operating mode of EPS protection.

- **Host intrusion prevention mode**: Specifies protection behavior when EPS protection is enabled. Choose from one of the following operating methods:
  
  - **Blocking**: Security violations are blocked AND recorded in an action history file on the core server.

  - **Learning**: All application security violations are allowed, but application behavior is observed (or learned) and that information is sent back to the core database in a Trusted File List. Use this mode to discover application behavior on a specific device or set of devices, and then use that information to customize your EPS policies before deploying them and enforcing EPS protection throughout the network.

  - **Log only**: Security violations are allowed AND recorded in an action history file on the core server.

  - **Silent**: Security violations are blocked and are NOT recorded in an action history file on the core server.
- **Whitelist mode:** Specifies protection behavior when whitelist protection is enabled—only applications in a Trusted File List and with the whitelist designation (applications whose file certification has the Allow execution option enabled) are allowed to run and are learned. Choose from one of the following operating methods:
  - **Blocking:** Security violations are blocked AND recorded in an action history file on the core server.
  - **Learning:** All application security violations are allowed, but application behavior is observed (or learned) and that information is sent back to the core database in a Trusted File List. Use this mode to discover application behavior on a specific device or set of devices, and then use that information to customize your EPS policies before deploying them and enforcing EPS protection throughout the network.
  - **Log only:** Security violations are allowed AND recorded in an action history file on the core server.
  - **Silent:** Security violations are blocked and are NOT recorded in an action history file on the core server.

**About the 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 or any file.

- **Protection rules:** Lists all of the predefined (default) file protection rules provided by Ivanti, 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.
  - **Programs:** Displays the executable programs that are protected by the protection rule.
- **Move Up \ Down:** Determines the priority of the file protection rule—a 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 predefined (default) file protection rules that are provided by Ivanti.
- **Add:** Opens the Configure file protection rule dialog box where you can add and remove programs and files and specify the restrictions.
- **Edit:** Opens the Configure file protection rule dialog box where you can edit an existing file protection rule.
- **Delete:** Removes the file protection rule from the core database.
NOTE: File protection rules are stored in the FILEWALL.XML file, located in:
ProgramFiles\Landesk\ManagementSuite\ldlogon\AgentBehaviors\EPS_Behavior.ZIP

About the Configure file protection rule dialog box

Use this page to configure file protection rules.

- **Rule name**: Identifies the file protection rule with a descriptive name.

- **Monitored programs**
  - **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**: Enables you to choose which programs are restricted by the file protection rule. You can use filenames and wildcards.
  - **Edit**: Enables you to modify the program name.
  - **Delete**: Removes the program from the list.

- **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.

- **Protect files**
  - **Any file**: 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**: Enables you to choose which file or files are protected by the rule. You can use filenames or wildcards.
  - **Edit**: Enables you to modify the filename.
  - **Delete**: Removes the file from the list.
  - **Apply to sub-directories too**: Enforces the file protection rules to any subdirectories of a named directory.

- **Restricted actions on protected files**
  - **Read access**: Prevents the programs specified above from accessing the protected files.
  - **Modification**: Prevents the programs specified above from making any changes to the protected files.
  - **Creation**: Prevents the programs specified above from creating the files.
  - **Execution**: Prevents the programs specified above from running the protected files.
**Agent settings: Branding**

The Branding dialog box allows you to customize the client dialog boxes for scanning, repairing, and rebooting devices.

The Branding dialog box contains the following options:

- **Preview**: Click to access a list of client dialog boxes to preview. Select Repair dialog, Status dialog, or Reboot dialog to see the dialog box with the custom icon and banner that the user will see.
- **Upload**: Click to browse to a custom LdCustomIcon.ico or LdCustomBanner.png or LdCustomBanner.jpg file. The files must have those exact file names to replace the default icon and banner.
- **Delete**: Click to remove a custom file and use the default icon or banner instead.

**Agent settings: Client connectivity**

**Tools > Configuration > Agent Settings > Client connectivity**

Use the Client connectivity settings dialog box to specify and save a collection of client connectivity settings.

**About the General page**

Use the General page to name the client connectivity setting that you’re configuring. You can have multiple profiles for client connectivity settings, but one must be set as the default for agent configurations. By selecting the Set as default option, the setting will be the default selection in the Agent Configuration tool.

**About the Core information page**

Use this page to configure certificate-based security and what scope devices using this configuration will have.

**Core certificates the client will trust**

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" (140).
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 is 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.

**Core address**

This needs to be a resolvable name or IP address that managed devices will use to communicate with the 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 Endpoint Manager 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 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 NetWare 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 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 and device group scopes.
For more information on how scopes are used in Endpoint Manager role-based administration, and how you can define a scope using custom directory paths, see "Role-based administration overview" (52).

**About the Cloud Services Appliance page**

The [Cloud Services Appliance](#) (CSA) page has the following features:

- **Enable Cloud Services Appliance communication**: Select this if you’ve installed one or more CSAs and you want an agent configuration to use the appliance to connect to the core server.

- **Available items** and **Selected items**: Lists the available and selected CSAs that you’ve configured for this core server. Select the one you want to use. There isn’t a limit to the number of CSAs that you can add.

Use the **CSA failover policy** for CSA load balancing and to set what happens if there’s a connection failure when a client tries to communicate with a CSA. When there’s a connection failure, the client will try connecting to other CSAs in the **Selected items** list. When a CSA connection failure happens, the client won’t try to use that CSA for 24 hours.

- **Use ordered list as shown in the selected items**: Clients will attempt to connect to the first CSA in the **Selected items** list. If that fails, clients will connect to the next CSA in the list until all CSAs have had a connection attempt.

Use this mode when one CSA is preferred over others for clients. For example, you may want devices for employees working in one country to use a CSA in that country as the top priority and some from other countries as backup systems.

- **Use random order**: Clients will connect to a random CSA in the **Selected items** list. If that fails, clients connect to the next randomly selected CSA in the list until all CSAs have had a connection attempt.

Use this mode when there are several CSAs of equal preference to a client, but you want to spread the workload across these CSAs. For example, devices for employees in one country may have three CSAs set up for them to use. Using the random order selection would generally distribute the workload across these CSAs and still provide failover if one stops working.

When you have enabled Cloud Service Appliance communication, you have three ways to connect to the core:

- **Dynamically determine connection route**: This is the default and the most flexible choice. If the agent can connect directly, it will. If it can’t connect directly, it tries to use the CSA. This mode may take a bit longer to connect since it tries each connection mode.

- **Connect directly to the LDMS core**: Always connects directly to the core.

- **Connect using the Cloud Service Appliance**: Always connects to the core via the CSA.
**About the Download page**

Use the **Download** page to block peer downloads over adapters that you specify. You can exclude adapters that are wireless. You can also exclude adapters by using case-sensitive keywords. If any of the keywords entered are found in the description field of the adapter, it will not use that adapter. As you can see by the default keywords, this method is used for disabling peer download over a VPN adapter.

You can also change the number of days files stay in the download cache on clients.

**About the Preferred server page**

Use the **Preferred server** page to control preferred server behavior:

- **Update preferred server list from core every**: Preferred server list update interval. This is the maximum amount of time a client will use the list of preferred servers before going to the core for a potentially new list. The default is once a day. The preferred server list is also discarded every time the IP address changes.

- **Number of preferred servers to attempt before falling back to source**: The default is three servers.

- **Number of files not found on preferred server before the server is moved to the end of the preferred server priority list**: The default is three files not found.

**About the Self-electing subnet services page**

**About the Extended device discovery page**

Use the Extended device discovery page to customize ARP and WAP extended device discovery scan settings.

**Use address resolution protocol**

- **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 Ivanti 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), or everything (3). The default level is 1- errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xdclient.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.

**Use wireless access point discovery (WAP)**

• **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), or everything (3). The default level is 1- errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xdclient.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 Local scheduler page**

Use the **Local scheduler** page to configure how often the local scheduler checks for tasks and network bandwidth.

The local scheduler agent enables Endpoint Manager to launch device tasks based on a time of day or bandwidth availability. The local scheduler agent is most useful for mobile devices that may not always be on the network or may connect to the network via a dial-up connection. For example, you can use the local scheduler to allow mobile device 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 the minimum bandwidth the packages or policies require before they are applied.

The local scheduler runs as a service on Windows devices.

The **Local scheduler** page contains the following features:

• **General frequency:** How often the local scheduler checks for tasks. The default is 10 seconds. The polling interval you select is stored on the local device.

• **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.
The local scheduler also enables bandwidth detection between devices and the core server. You can limit Endpoint Manager 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.

- **ICMP** or **PDS**: 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 dial-up 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 dial-up 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 Ivanti agent to the package server.

- **Bandwidth detection LAN threshold**: The threshold that classifies a connection as WAN rather than LAN. The default is 262144 bps.

### Agent settings: Compliance

**Tools > Configuration > Agent Settings > Compliance**

Compliance settings are a subset of the Distribution and Patch settings. These settings are only used when a device does a compliance scan. A compliance scan only scans for the definitions found in the **Compliance** group.

### Agent settings: Custom variables to override

**Tools > Configuration > Agent Settings > Custom variables to override**

Use the Custom variables override settings dialog box 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.

---

**IMPORTANT: Edit Custom Variables right required**

In order to edit custom variable settings, and configure custom variable override settings, a Ivanti user must have the Edit Custom Variables role-based administration right. Rights are configured with the **Users**
Agent settings: Device control

Tools > Security and Compliance > Agent settings > Security > Endpoint security > Device control

Use this dialog box to create and edit Device Control settings.

This dialog box 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 the 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 the settings.

About the Storage volumes page

Use this page to specify options for storage volumes that connect to a client configured with this setting.

- **Storage volumes:** Specifies the access level for any storage volume that wasn’t present on the client when the setting was installed. (Note that if a device containing a volume was attached when the setting was installed, the Ivanti Endpoint Security 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 setting. 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 Ivanti Management > Ivanti Encryption Utility. 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 setting. 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.
  - **Allow password hints:** Lets the end user enter a hint that can help them remember the encrypted folder password. The password hint can’t be an exact match to the password itself. The password hint can’t 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 user:** Displays a message box when a user connects an unauthorized storage device.

**About the Configure exception (for storage volumes) dialog box**

Use this dialog box 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 the tabs on this page to configure devices, interfaces, and manage exceptions.

**Devices tab**

Select a device, and in the **Access** column, select whether you want to **Allow**, **Block**, or **Always allow** the device.

**Notify end user:** Displays a message box when a user connects an unauthorized device.

**Interfaces tab**

Select an interface, and in the **Access** column, select whether you want to **Allow** or **Block** the device.

**Block wireless LAN 802.11X:** Blocks a wireless LAN802.11X connection.

**Notify end user:** Displays a message box when a user connects an unauthorized device.
Exceptions tab

Use the exceptions tab to configure exceptions for detected devices. An exception allows a specific device to connect even if that device's class is blocked. Use the filters at the top of the Configure exception window to filter the list. Select the devices you want an exception for, and decide whether you want the exception based on the instance path or hardware ID. Add the selected exceptions by clicking Add to exception list.

About the Shadow copy page

Use this page to enable and configure shadow copy on managed devices configured with this setting. 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 setting.
- **Log events only**: Indicates that only the file copy activity is recorded in a log file, not the actual files that are being copied.
- **Local cache settings**: Specifies the location on the local drive where the shadow copy files and log file are stored.
- **Exceptions**: Click to create exceptions. You can add exceptions based on hardware ID, media serial, or bus type.

About the CD/DVD/Blu-ray page

Use this page to control CD/DVD/Blu-ray connections.

- **CD/DVD/Blu-ray drives**: Select the access level you want for these drives. Click Exceptions if you want exceptions for specific drives or drive types.
- **Devices / Interfaces**: Use the check boxes to block devices and interfaces from accessing the client.
- **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 device.

Agent settings: Distribution and patch

**Tools > Configuration > Agent Settings > Distribution and patch**

The Distribution and Patch agent settings dialog allows you to control how Ivanti® Endpoint Manager powered by Landesk installs packages, runs scans, and repairs files.
General settings

On the General settings page, enter a name that will be associated with the settings you specify on all of the pages in this dialog. This name will appear in the Agent settings list in the console.

Network settings

Use this page to customize how distribution packages will impact your network traffic. For more information, see About file downloading.

- **Attempt peer download**: Allow packages to download if they are already on a peer in the same subnet. This will reduce network traffic. For example, if you have several satellite offices, you could select one device at each office to receive the package over the network. Then, the other devices at each office would get the package directly from the first device instead of downloading it from the network.

- **Attempt preferred server**: Allow automatic redirection to the closest package shares. This will reduce the load on the core server.

- **Allow source**: Download from the core server if the files aren’t found on a peer or preferred server. If the files are not in one of those locations and this option is not selected, the download will fail.

- **Use multicast**: Uses targeted multicast to send files to multiple devices simultaneously. Enter a value for the amount of time to wait on each subnet before the download begins.

- **Bandwidth used from core or preferred server**: Specify the percentage of bandwidth to use so you don’t overload the network. You can limit bandwidth by adjusting the maximum percentage of network bandwidth to use for the distribution. The slider 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**: Specify the percentage of bandwidth to use locally. This value is typically higher than the bandwidth used from core or preferred server because of physical proximity.

- **Send detailed task status**: Click to send information about the task to the core server. This increases network traffic, so if you select this option to help troubleshoot a particular issue, you may want to clear it once you resolve the issue.

Policy sync schedule

Use the Policy sync schedule page to specify when the client will check the core to see if there are any packages available for download.
- **Policy sync schedule**
  - **Event-driven**
    - **When user logs in:** Click to run policy sync once a user has logged in.
    - **When IP address changes:** Click to run policy sync when the IP address changes.
      - **Max random delay:** Specify an amount of time to delay the scan in order to avoid downloading the package on all of the devices at the same time, which could flood the network.
  - **Schedule-driven**
    - **Use recurring schedule:** Click to only download distribution packages during a specified time frame. The default is to check once a day.
    - **Change settings...:** Click to open the Local scheduler command dialog, where you can create a different schedule.

**Notification**

Use the Notification page to specify what information to display to the user and what actions the user can take.

- **Notification options before installing/removing**
  - **Automatically begin downloading:** Begins the download of the distribution package without notifying the user.
  - **Notify user before downloading:** 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.
  - **Automatically begin installing/removing:** Begins the installation of the distribution package without notifying the user.
  - **Notify user before installing/removing:** Displays the installation or removal dialog before a managed device initiates installation or removal of the package.
  - **Only notify user if processes must be stopped:** Only displays a dialog if a process must be stopped before the managed device initiates the installation or removal of the package.
  - **Kill processes that need to be stopped before starting the update:** Click to shut down any processes that must be stopped before installing the package.
  - **Prevent those same processes from running during the update:** Click to ensure the processes are not allowed to restart until after the package has finished installing.
  - **If deferring until lock/logoff:** Specify how long to wait before the package will install.
• **Progress options**
  
  • **Show progress**: Select whether to never show the installation progress, to only show it when installing or removing files, or to show it when installing or removing and when scanning files.
  
  • **Allow user to cancel scan**: If you choose to always show the progress to the user, this option will be enabled. Click to give the user the ability to cancel the scan.

• **No response timeout options**: These options are enabled if you allow the user to defer or cancel.
  
  • **Wait for user response before repair, install or uninstall**: If you allow the user to defer or cancel, this option will be enabled. Click to force the agent to wait for a user response before continuing. This may cause the task to timeout.
  
  • **After timeout, automatically**: Click to automatically start, defer, or cancel the task after the amount of time you specify.

**User message**

Use this page to create a custom message that the user will see if you select **Notify user before downloading** or **Notify user before installing/removing** on the **Notification** page.

When you schedule a task, there is an option to override this message.

**Distribution-only settings**

Use this page to specify what to show the user and how long to defer an installation. These options are dependent on the settings you select on the **Notification** page. You can also use the Distribution-only settings page to select the location for virtualized applications.

• **Feedback**
  
  • **Display full package interface**: Click to show the user everything that the installation displays. This option is for power users only.
  
  • **Show successful or failed status to end user**: Click to only show the user the outcome of the installation.
  
  • **Defer until next logon**: Click to allow users to postpone the installation until the next time they log on to the device.
  
  • **Defer for a specific amount of time**: Specify the maximum amount of time the user can defer the installation.
    
    • **Limit number of user deferrals**: Click to enter a maximum number of times the user can defer the installation.
  
  • **Select the location to store Ivanti virtualized applications**
    
    • **Client Destination**: Click to install the package in a new environment instead of installing the package on the device.
  
  • **Enable LDAP group targeting**: Click to target your distribution to the groups that you have set up on your Microsoft domain instead of targeting devices and user names from Ivanti.
- **Allow LDAP resolution via CSA**: Click to target your distribution to objects in your Microsoft Domain while going through the Cloud Service Appliance.

**Offline**

Use this page to specify what to do if a managed device can’t contact the core server during a package installation.

- **Wait until the device can contact the managed core server**: Click to stop the installation until the device is able to contact the core server.
- **Install the package(s) offline**: Click to create a scheduled task that downloads the files onto the device but doesn’t install them.

**Logged off user options**

Use this page to specify whether to install if the user is logged off a device.

- **Logged off user behavior**
  - **Continue installation**: Click to install the distribution package if the user is logged off.
  - **Fail installation**: Click to not attempt the installation of the distribution package when the user is logged off.
  - **Run at next logon**: Click to not attempt the installation of the distribution package when the user is logged off and to begin the package installation when the user logs on again.

**Download options**

Use the Download options page to specify whether a client should download the patch and then install it or run the installation from the server.

- **Run from source**: Click to install the patch from the preferred server or the core. This option is useful if the client machine does not have enough memory to download the patch.
- **Download and execute**: Click to download the patch to the client and then install it. This option reduces the load on the server.

**Patch-only settings**

Use the Patch-only settings page to select reboot and alternate core options when scanning, repairing, and downloading files.

- **When no reboot is required**
  - **Require end user input before closing**: Select this option for the notification dialog to remain visible until the user responds to it.
  - **Close after timeout**: Select this option to close the notification dialog after a specified countdown.
- **Alternate core**
  - **Communicate with alternate core server**: Click to select a server to use if the default core server is unavailable.
  - **When installing via CSA**: Click an option in the drop-down list to specify how the scanner will install via the portal Cloud Service Appliance (formerly known as Gateway). This is helpful if you have people who are outside the network, such as employees who are on the road, who need to communicate with the core.
  - **Download patches from core as usual**: This will require an extra step and may cause delays or network issues.
  - **Do not download patches. Fail the request**: This will reschedule the download. Select this option if bandwidth is an issue.
  - **Download patches from manufacturer. Fall back to core on failure**: This will attempt to download the patch directly from the manufacturer, such as Microsoft, before going through the core server. This will use less bandwidth on your own network.
  - **Download patches from manufacturer. Do not fall back on failure**: This will attempt to download the patch directly from the manufacturer, such as Microsoft. If it is unable to download the patch, it will reschedule the download.
  - **CPU utilization when scanning**: Set the slider to specify whether to allow low or high CPU utilization during a scan.
  - **Scheduled task log**: Specify which information the scanner sends to the core. For example, if you are experiencing an issue, you may wish to send debug information to try to troubleshoot the problem.

**Do not disturb**

Use this page to specify mission-critical processes so that a scan will not occur if those processes are running. For example, to ensure that the scanner will not run during a presentation, you could apply the filter so that a reboot could occur with PowerPoint open but not if PowerPoint was running full screen.

- **Add defaults**: Populates the list with the default processes.
- **Add...**: Opens the **Specify process filter** dialog box, where you can enter the name of the process and specify whether to apply the filter any time the process is running or only when the process is running full screen.
- **Edit...**: Opens the **Specify process filter** dialog box, where you can change the filter for a process that is already in the list.
- **Delete...**: Removes a process from the list.
• **Legacy Mac agent user interruption settings** If you have upgraded your Mac client, all of the settings on the Do not disturb page are supported. However, if you have not upgraded your Mac client, you can use the following options:
  
  • **Hide scan progress dialog when a presentation is running:** Click to keep the scan progress dialog in the background so that it does not interrupt a presentation.
  
  • **Defer repairing when a presentation is running:** Click to postpone any repairs until the presentation is over.

**Scan options**

Use this page to specify whether the security scanner will scan by group or by type of vulnerability.

• **Scan for**
  
  • **Group:** Select a custom, preconfigured group from the drop-down list.
    
    • **Immediately repair all detected items:** Indicates that any security risk identified by this particular group scan will be automatically remediated.
  
  • **Type:** Specifies which content types you want to scan for with this scan task. You can select only those content types for which you have an Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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 box, only those vulnerabilities and security threats currently residing in their respective Scan groups will be scanned for.
  
  • **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 definition must also have autofix enabled.

**Schedule**

Use this page to specify the time frame during which the security scanner will run as a scheduled task. After you select the settings, this page displays a summary of the schedule.

• **Event-driven**
  
  • **When user logs in:** Click to scan and repair definitions once a user has logged in.
    
    • **Max random delay:** Specify an amount of time to delay the scan in order to avoid simultaneously scanning all of the devices, which could flood the network.
  
  • **Schedule-driven**
    
    • **Use recurring schedule:** Click to only scan and repair definitions during a specified time frame.
    
    • **Change settings...:** Opens the Local scheduler command dialog box where you can define the parameters for the security scan. This dialog box is shared by several Ivanti management tasks. Click the Help button for details.
Frequent scan

Use this page to enable the agent to check definitions in a specific group more frequently than usual. This is helpful when you have a virus outbreak or other time-sensitive patch that needs to be distributed as soon as possible. For example, you may want a client to scan every 30 minutes and at every login for a specific group that may contain critical vulnerabilities. The frequent scan is optional.

- **Enable high frequency scan and repair definitions for the following group**: Enables the frequent security scan features. Once you’ve checked this option, you need to select a custom group from the drop-down list.
  - **Immediately install (repair) all applicable items**: Click to enable the agent to install a patch if it locates one in the folder that you specify.

- **Schedule**
  - **Event-driven**
    - **When user logs in**: Click to scan and repair definitions once a user has logged in.
      - **Max random delay**: Specify an amount of time to delay the scan in order to avoid simultaneously scanning all of the devices, which could flood the network.
  - **Schedule-driven**
    - **Use recurring schedule**: Click to only scan and repair definitions during a specified time frame.
    - **Change settings...**: Opens the Local scheduler command dialog box where you can define the parameters for the security scan. This dialog box is shared by several Ivanti management tasks. Click the Help button for details.

- **Override settings**: From the drop-down box, select the settings that you wish to override with the settings that you specify in the Distribution and Patch dialog.
  - **Edit...**: Click to open the Distribution and Patch settings dialog for that particular setting.
  - **Configure**: Click to open the Configure distribution and patch settings dialog. For more information, click Help.

Pilot configuration

Use the Pilot configuration page to test security definitions on a small group before performing a wider deployment on your entire network. For example, you may wish to install a new Microsoft patch on the devices in only the IT group to make sure that it doesn’t cause any issues before it goes out to everyone in the organization. Using a pilot group is optional.

- **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.
Schedule

- Event-driven
  - When user logs in: Click to scan and repair definitions once a user has logged in.
  - Max random delay: Specify an amount of time to delay the scan in order to avoid simultaneously scanning all of the devices, which could flood the network.

- Schedule-driven
  - Use recurring schedule: Click to only scan and repair definitions during a specified time frame.
  - Change settings...: Opens the Local scheduler command dialog box where you can define the parameters for the security scan. This dialog box is shared by several Ivanti management tasks. Click the Help button for details.

Spyware scanning

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.

- 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.

Install/remove options

Use the Install/remove options to specify what the agent should do once it determines the need for a patch.
- **Reboot is already pending**: Click this option if you want to start a patch installation regardless of whether the device has requested a reboot.

**Continuation**

Use the continuation page to enable the agent to immediately install or remove patches as soon as it meets the specified criteria. For example, if you need to install ten patches to remove a single vulnerability, continuation provides a way to install them one after another.

- **Automatically continue install/remove actions after prerequisites are met**: Click to allow the agent to automatically install or remove patches once it meets any prerequisites.
  - **Additional automatic repair count**: The default is to allow 5 automatic repairs, which balances the urgency of getting the patch installed with allowing users complete their work.

**Maintenance window**

Use this page to specify the parameters for when the agent can perform any install, repair, or remove actions.

- **Machine must be in this state**: Click to specify whether the user must be logged off or the device must be locked for the specified amount of time.
  - **Delay**: Use this option if you want to delay the action for several minutes to ensure that the user is not returning to the device.
- **Machine must be in this time window**: Click to configure the maintenance window by setting a detailed schedule. Specify the time of day, days of the week, and days of the month. The agent will only run when it meets all criteria.

**Pre-repair script**

Use the Pre-repair script page to execute a custom command before installing a patch. For example, if you want to get the environment ready for the patch by turning off a particular service, you can use a script.

- **Abort patch install or uninstall if this script fails**: Specify whether to cancel the patch installation if the script does not run.
- **Insert sample script...**: Click to select a VBScript, PowerShell script, or batch file to include in the pre-repair script.
- **Insert method call...**: Click to open a list of method calls that you can add to the pre-repair script. Click a method call in the list to move it to the Script Content box.
- **Use editor...**: Click to open Notepad, where you can write your custom script.

**Post-repair script**

Use the Post-repair script page to execute a custom command after installing a patch. For example, if you used a script to shut off the AV service before installing a patch, you can use the post-repair script to turn it back on.
- **Run this script even if pre-repair fails**: Specify whether to uninstall the patch if the post-repair script does not run.
- **Insert sample script**: Click to select a VBScript, PowerShell script, or batch file to include in the post-repair script.
- **Insert method call**: Click to open a list of method calls that you can add to the post-repair script. Click a method call in the list to move it to the Script Content box.
- **Use editor**: Click to open Notepad, where you can write your custom script.

**MSI information**

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.

**Branding**

The Branding page allows you to customize the status dialog that will notify the user of a scan or other scheduled task. For information on how to hide or display the dialog, see Notification.

The Branding dialog box contains the following options:

- **Customize window caption**: Enter a title for the dialog.
- **Preview**: Click to see the dialog box with the custom icon and banner that the user will see.

**Agent settings: Reboot settings**

**Tools > Configuration > Agent Settings > Reboot settings**

Administrators now have better control over the reboot experience. With the Reboot settings, administrators can create reboot policies that are consistent across scheduled tasks. These settings will override the default agent settings on the client.
NOTE: The global settings in the Agent configuration dialog box override any reboot settings that you specify in the Reboot settings dialog box. The global setting Never reboot is selected by default on new Windows agent configurations. To change this setting, click Tools > Configuration > Agent configuration > Standard Ivanti agent then clear the Never reboot box.

NOTE: Reboot settings do not apply to the reboot task that you start from the device list. If you right-click a machine in the device list and click Reboot, that task immediately attempts to reboot the device, overriding all reboot settings and global settings in the Agent configuration dialog box.

About the General page

Use the General page to specify when to initiate the reboot process. Once you select options on the other pages of the dialog box, the General page displays a summary of the settings.

The General page contains the following options:

- **Name:** Enter a unique identifier for the reboot settings that you specify on all of the pages of the dialog.

- **When deciding whether a reboot is needed**
  - **Act as if reboot is ALWAYS needed:** Forces a reboot even if neither the Windows OS nor the Ivanti agent indicate the need for one. For example, if there is a virus or malware, you may want to install a patch and force a reboot for security reasons.
  - **Detect whether reboot is needed:** Checks with both the Windows OS and the Ivanti agent and initiates a reboot if either one recommends it. For example, once you install agents on devices, they may need a reboot to complete the agent configuration.
  - **Act as if reboot is NEVER needed:** Disables all other reboot settings so that Ivanti tasks will not reboot the machine, even if the Windows OS or Ivanti agent recommends a reboot.
  - **Suppress Windows Update reboot notifications:** Prevents the Windows Update service from displaying reboot notifications in the task tray. The end user will not see any reboot messages from Windows Update.

About the Prompt page

Use the Prompt page to customize the reboot dialog that will display on the end user's machine.

NOTE: The prompt will only appear if the user is logged in and the machine is not locked. Otherwise, the machine may reboot without displaying the prompt.

The Prompt page contains the following options:

- **Prompt user before rebooting:** Click to enter a custom message the user will see in a reboot prompt before the reboot occurs.


• **Use default message**: Click to discard a custom message you entered and restore the default message.

• **Allow users to defer (snooze) for**: Specify the time period during which the user will be able to postpone the reboot. The user will be able to choose how many times to defer and how long to wait within this time period. When the prompt appears, the user must reboot or defer.

• **Show system tray icon when a reboot is required**: Displays the icon in the system tray, which allows the user to access the reboot prompt. For example, if a user chooses to defer the reboot for four hours but then has time to do it an hour later, the icon in the system tray allows them to reboot sooner than they previously specified.

• **Customize window caption**: Click to enter the text that will appear in the title bar of the reboot prompt.

• **Preview...**: Click to see the prompt that the user will see. Use this option to check the branding options you have selected.

• **Go to "Branding"**: Click to open the Branding dialog box, where you can select custom icon and banner images.

**About the Automatic reboot page**

Use the Automatic reboot page to specify the circumstances for a forced reboot.

The **Automatic reboot** page contains the following options:

• **Automatically reboot if any of these options are selected**: The reboot will occur if the machine meets any of the selected options, whichever happens first.

  • **Logged out for**: The machine will reboot if the user has been logged out for the specified amount of time.

  • **Locked or logged out for**: The machine will reboot if the machine has been locked or logged out for the specified amount of time. Use this option if you want to reboot while the machine is locked, such as during a lunch break or while the user is away in a meeting.

  • **No response to reboot prompt for**: The machine will reboot if the user does not defer or reboot for the specified amount of time.

  • **Reboot deadline exceeds**: The machine will reboot if the user does not reboot before that time. For example, if you have an important security update that must occur in the next three days, set the deadline to 3 days. The reboot deadline must be equal to or greater than the **Allow users to defer** for time on the Prompt page.

  • **Limit automatic reboot in the specified time window**: The machine will only reboot if it is in that window, even if the reboot deadline has occurred. Specify the maintenance window by setting a weekly schedule. For example you could set it to reboot on the weekend if you had a point-of-sale machine that cannot reboot during business hours.
About the Do not disturb page

Use the Do not disturb page to override the settings on the other pages of the Reboot dialog.

The Do not disturb page contains the following options:

- **Do not reboot or prompt to reboot if specified processes are running**: Specify mission-critical processes so that a reboot will not occur if those processes are running.
  - **Add...**: Opens the Specify process filter dialog box, where you can enter the name of the process and specify whether to apply the filter any time the process is running or only when the process is running full screen. For example, to ensure that a machine does not reboot during a presentation, you could apply the filter so that a reboot could occur with PowerPoint open but not if PowerPoint was running full screen.
  - **Edit...**: Opens the Specify process filter dialog box, where you can change the filter for a process that is already in the list.
  - **Delete...**: Removes a process from the list.
  - **Import...**: Opens the Import dialog box, where you can select processes from the Do not disturb lists in other settings, such as Distribution and patch.

Agent settings: Endpoint security

- **Update configuration from core**: Lets you update Endpoint Security settings on target devices configured with this agent configuration.

Agent settings: Extended device discovery

The Configure ARP Discovery Settings dialog contains the following options:

- **Configuration Name**:
- **Duration ARP entry stats cached**:
- **Maximum delay**:
- **Frequency the cached ARP tables is refreshed**:
- **Logging Level**:
  - **Force logging level**:

The Configure WAP Discovery Settings dialog contains the following options:

- **Configuration Name**:
- **Frequency of WAP Scan**:
• Logging Level:
  • Force logging level:

**Agent settings: Remote secure erase**

**Tools > Configuration > Agent settings > HP Remote secure erase**

Use this dialog box to create HP remote secure erase settings profiles.

• **Name:** The name you want to give this setting.

• **Reprovision the device with the selected package:** Click the drop-down list box to see a list of HP RSE keys that have been generated on the core.

• **Remove the package and reset the device to factory defaults:** When selected and this setting is applied to a device, it removes HP RSE data from the BIOS.

• **Launch:** Displays the **HP Remote Secure Erase Package Manager** dialog box. This option is only available on consoles running on the core server.

**About the HP Remote Secure Erase package manager dialog box**

Use this dialog box (**Configure > HP Remote Secure Erase Package Manager**) to create, import, and export remote secure erase packages. You can only launch this dialog box on the core server.

• **Company name:** Can be any string. This gets flashed into the BIOS. Must be 20 or fewer single byte or double byte characters.

• **Package name:** This name appears in dropdown lists and menus. Make this more descriptive. Must be 20 or fewer single byte or double byte characters.

• **Create:** After you’ve entered a company and package name, click **Create** to generate the keys and HP RSE BIOS image. This makes the new key available for export. Back up exported keys as soon as possible.

• **Import an HP remote secure erase provisioning package created on another core server:** Shows any keys that you’ve manually copied to the RSE keys folder (**C:\Program Files\LANDesk\Shared Files\Keys\Rse**) that haven’t been imported yet. Select each key that you want to import and click **Import**. This adds the selected key to the database and removes it from the list.

• **Import:** If there are secure erase packages from another core server that you’ve manually copied to this core server, they appear in this list. Importing them removes them from the list and adds them to the RSE database. The folder containing generated packages and keys must be copied to this folder on the core server: **C:\Program Files\LANDesk\Shared Files\Keys\Rse**.

• **Select the package to export:** Shows the list of HPRSE keys that this core server knows about. Select the key you want to export from this list.
• **Export**: Exports a first-time HP remote secure erase provisioning package that you select. The list shows RSE keys in the RSE database. A dialog box appears that lets you select a location for the exported files. The exported files constitute the provisioning package (hprse.desc, rse.bin, and LDProvisionSecureErase.exe). Copy the exported files to the root of a FAT or FAT32 USB drive that you can use for provisioning/reprovisioning.

**Agent settings: HP BIOS**

**Tools > Configuration > Agent Settings > HP > HP BIOS settings**

Use this dialog to configure BIOS settings that can then be deployed to your managed HP devices.

**IMPORTANT:** New Inventory scan required for settings changes to appear in the Inventory

Any changes you make on this dialog and deploy to a target HP device will not be reflected in the device’s inventory until after the next Inventory scan.

This dialog box contains the following options:

- **Settings selection:**
  - **Apply only modified settings to targeted clients**: Ensures that only the BIOS settings you’ve changed with this configuration are applied to the target HP devices.
  - **Apply all settings to targeted clients**: Ensures that all of the BIOS settings contained in this configuration are applied to the target HP devices.

- **Feature list:**
  - **Feature**: The name of the HP BIOS component.
  - **Current Setting**: The value of the specified HP BIOS component based on the last Inventory scan.
  - **New Setting**: The changed value you want applied to the specified HP BIOS component.

- **BIOS access:**
  - **Current BIOS password**: Allows access to the HP BIOS data.
  - **Confirm passwords**: Required for access to the HP BIOS data.
  - **Load default BIOS settings**: Clears the existing HP BIOS components’ values and resets them to the system default values.

- **Name of package to be created:**
  - **Software Distribution package name**: Identifies the software package with a unique name.
  - **OK**: Closes the dialog and saves the software package in the Ivanti Software Distribution tool.
  - **Cancel**: Closes the dialog without saving any of your changes.
Related topics

For step-by-step instructions on configuring HP BIOS settings that can be deployed to target devices, see Create and deploy HP BIOS settings to HP devices.

Agent settings: HP software policies

Tools > Configuration > Agent Settings > HP > HP software policies

Use this dialog box to configure HP Power Assistant settings that can then be deployed to your managed HP devices.

IMPORTANT: New Inventory scan required for settings changes to appear in the Inventory

Any changes you make on this dialog and deploy to a target HP device will not be reflected in the device’s inventory until after the next Inventory scan.

This dialog box contains the following options:

- **Name**: Identifies the policy settings with a unique name.
- **Schedule event**:
  - **Event name**: Identifies a particular event in the HP Power Assistant policy. You can add one or more events in order to build a customized power policy.
  - **Action**: Specifies the action this event will perform (Hibernate, Sleep, On).
  - **Profile name**: Specifies the default HP power profile (Power Saver, Balanced, HP Optimized, High Performance) for the event you’re defining.
  - **Day**: Indicates which day(s) this event will be activated on target devices.
  - **Time**: Indicates the time of day when this event will be initiated on target devices.
  - **Add**: Saves the event in the list box. You can add as many events as you like when configuring a power policy.
  - **Update**: Saves your changes after you click the pencil icon and make changes to an event.
- **Save**: Saves the policy and closes the dialog.
- **Cancel**: Closes the dialog without saving.

For step-by-step instructions on configuring HP Software Policy settings that can be deployed to target devices, see Create and deploy HP Software Policy settings to HP devices.

Agent settings: Inventory settings

Tools > Configuration > Agent settings > Inventory settings

Use the Inventory settings dialog box to customize inventory agent behavior on managed devices.
About the Inventory settings General settings page

The **General settings** page controls a few inventory-related client settings.

- **Enable scheduled task history maintenance**: Sets the number of days to keep scheduled task history in the client database.
- **Run inventory scanner automatically after software package installation**: Use this if you want to update inventory data after packages are installed without having to wait for your normal inventory scan interval to pass. You can configure a scan delay after installation.

About the Inventory settings Location reporting page

Use the location reporting page to enable location reporting and configure the collection intervals.

If you enable location reporting and deploy the updated agent to a device, location reporting won’t happen unless a user on that device opts in to the Windows 8 **Let apps use my location** privacy setting.

The standard data collection interval is four hours.

For Hewlett Packard devices, if the device is marked lost (on the device’s inspector dialog, **Hewlett-Packard** page), the **When lost** collection interval activates, providing you more frequent location updates. For more information, see **Working with ElitePad tablets in the console**.

---

**NOTE:** Devices that have location reporting enabled must have Microsoft .NET 4.0 installed. You can install .NET 4.0 as part of the agent. To do this, select the .NET install option on the **Start** page of the agent configuration.

---

About the Scanner settings page

Use the scanner settings page to customize scanner behavior.

- **Send all executed files**: Enable this if you want to see all executed file data, and not just data for files in the monitored software list.
- **Send file usage data**: Inventory scans return software usage data gathered by the software monitor.
- **Force exhaustive file scan**: Scans all file extensions, possibly resulting in slow scans and very large inventory scan files. We generally don’t recommend enabling this.
- **Auto-update LDAPl file**: Managed devices store information about what the inventory scanner should look for, such as any changes you’ve made in the Manage software list tool. This option synchronizes that list with the core server so the local list is always current.
- **Do not send logon/lock event dates**: The scanner can return OS logon/lock event data. If you have privacy concerns about this or if you don’t want this data, disable this option.
- **Post to web service**: Rather than copying scan files to a folder on the core server, this option sends scan files directly to a web service. This is more efficient and it is the new default.
**Change history storage:** The inventory scanner uses delta scans to track changes in an XML file. By default this file holds 90 days worth of data. For more information the the change history, see "Viewing a device's inventory change log" (333).

**Software scan frequency:** How often you want to scan for software changes. The default is one day. Software scans are slower than the basic inventory scan and can affect device performance.

**Data file extensions:** If you have data files that are specific to an organization in your company, you can include them here. Include the leading period and separate each data file extension with a space. The Inherited extensions field shows global data file extensions set in the Manage software list tool.

**About the Software Usage Monitoring page**

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.

When deploying agents to non-persistent virtual desktop interface (VDI) disk images, you must set a UNC path where software monitor data files will be stored. If you don’t set a path, software license monitoring will store monitoring data in the registry. In a non-persistent environment, this data will be lost when the image resets. For more information, see "Deploying agents to non-persistent VDI images" (121).

The Software usage monitoring page contains the following options:

- **Use software monitor:** Enables tracking of software through software licensing monitoring, inventory scans, and application blocking through the application blocker feature.
- **Record software usage statistics to a network location:** Select this and configure the related options if you’re deploying this agent configuration to a non-persistent VDI image.
- **UNC path where software monitor data files will be stored:** The UNC path that you want used, in this format: \servername\sharename.
- **Domain and user name:** The user credentials that will allow access to the UNC path.
- **Password** and **Confirm password:** The password for the user account you provided.

**About the Schedule page**

Use the Schedule page to configure when the inventory scanner runs.

- **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 when there's an IP address and to also run every day with a random delay of up to one hour.

**About the Configure inventory settings dialog box**

Use the **Configure inventory settings** dialog box to manage your settings profiles. You can create multiple settings profiles and select the one that you want to be the default for new agent configurations.

• **New**: Creates a new settings profile.
• **Edit**: Edits an existing profile.
• **Copy**: Opens the selected profile and inserts "Copy of" at the beginning of the selected profile's **Name**. When you click **Save**, it will be saved as a new profile.
• **Delete**: Deletes the selected profile. You will be asked to confirm the deletion.
• **Use selected**: Closes the **Configure remote control settings** dialog box and makes the profile you selected the selection in the **Choose which remote control settings to apply** drop-down list box

**Agent settings: Ivanti Firewall**

**Tools > Security and Compliance > Agent settings > Security > Endpoint security > Ivanti Firewall**

The Ivanti Firewall tool is an important component of Endpoint Security that lets you protect managed devices from unauthorized application operations and connections.

With Ivanti Firewall settings, you can create and configure trusted programs (applications), trusted network scopes, and connection rules to protect managed devices from unauthorized intrusions.

**IMPORTANT: Ivanti Firewall and Windows Firewall compatibility**

The Ivanti Firewall complements the Windows Firewall, and both can be enabled and running at the same time on managed devices.

**Component of Endpoint Security**

Ivanti Firewall is one of the components of the comprehensive Endpoint Security solution, along with the Host Intrusion Prevention (HIPS) and Device Control tools. To enable Ivanti Firewall, open the **Endpoint Security settings** dialog and on the **Default policy** page, check **Ivanti Firewall**.

Read this chapter to learn about:

• "Using Ivanti Firewall settings" (271)
• "Ivanti Firewall settings help" (272)
Using Ivanti Firewall settings

Firewall settings give you complete control over how the Ivanti Firewall operates on target devices. This section describes how to create and manage Firewall settings.

Creating Ivanti Firewall settings

To create Ivanti Firewall settings

1. In the Agent Settings tool window, right-click Ivanti Firewall, and then click New.

2. At the General settings page, enter a name for the settings, enable the Ivanti Firewall service, and then specify the protection mode. For information about an option, click Help.

3. At the Trusted scope page, add and edit application executable files 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.

**Ivanti Firewall settings help**

Use this dialog to create and edit Ivanti Firewall settings. When creating Firewall settings, you first define the general protection mode, and then add and configure specific trusted file lists, 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 Ivanti Firewall and configure the protection mode.

This page contains the following options:

- **Name**: Identifies the Firewall settings with a unique name.
- **Enable Ivanti 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 mode**: All security 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.
  - **Use learn mode for**: 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.
    
    **NOTE**: These two time period options are executed successively. In other words, if both are selected, the learn mode period runs first and when it expires the monitor mode period runs.
    
    - **Use monitor mode for**: Specifies a period of time during which the applications that run are recorded in an action history file on the core server.
  - **Learn mode**: All applications are allowed to run. Additionally, all of the applications that are run on the device are learned and added to the trusted file list.
  - **Monitor mode**: Security violations are allowed, but are recorded in an action history file on the core server.
- **Block mode**: Security violations are blocked, and are not recorded in an action history file on the core server.
- **File sharing**: Specifies file sharing privileges allowed by the Ivanti Firewall settings.
  - **Allow file sharing from the trusted scope (network)**: Allows files to be shared within the trusted scope you've defined.
  - **Allow file sharing from outside the trusted scope (Internet)**: Allows files to be shared outside of the trusted scope you've defined.

**About the Trusted scope page**

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 condition to the list. Add a condition by IP address, IP range, or subnet.
- **Edit**: Lets you modify the selected condition location.
- **Delete**: Removes the selected condition.

**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 box**

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 (accepts) or prevents (drops) 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.

**Agent settings: Ivanti Mac Antivirus**

Ivanti Mac Antivirus features are accessed from the Agent settings tool window (Tools > Security and Compliance > Agent settings). In the Agent settings window, right-click **Ivanti Mac Antivirus - Mac**, and then click **New**....

Ivanti Mac Antivirus allows you download and manage antivirus content (virus definition files), configure antivirus scans, and customize antivirus scanner 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 Ivanti Mac Antivirus introduces this complementary security management tool, which is a component of both Ivanti® Endpoint Manager powered by Landesk and Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk. 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 help topics that describe the Ivanti Mac Antivirus settings dialog box. From the console interface, access these topics by clicking **Help** on each dialog box.
About the Ivanti Mac Antivirus General page

Use this page to configure Ivanti Mac 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 list on the Antivirus scan task dialog box, on other dialogs, and in the console.

- **Protection:**
  - **File Antivirus:** Enables real-time scanning of files on target devices. If you do not enable File Antivirus, the collected statistics appear in the Completed tasks section of the report window. When the component runs, it generates a new report. By default, File Antivirus is enabled and configured with the recommended settings.

- **Permissions:**
  - **Allow user to disable protection components for up to:** Specifies the period of time during which the user can pause and stop the protection components listed on the Protection page.
  - **Allow user to update definitions:** Allows the user to update antivirus definition files.
  - **Allow user to restore objects:** Allows the user to restore quarantined objects and objects from backup.
  - **Allow user to change settings:** Allows the user to schedule scans and modify the exclusions and trusted applications lists.

- **Set As Default:** Establishes the settings on all of the pages of the Ivanti Mac Antivirus dialog box as the default settings. The name you entered will appear in the console with the default icon next to it. You cannot delete a setting that is marked as default. When you create a new agent configuration, those settings will be selected by default. Unless an antivirus scan task has specific antivirus settings associated with it, Ivanti Mac Antivirus will use the default settings during scan and definition file update tasks.

About the Ivanti Mac Antivirus Protection page

Use this page to configure the way File Antivirus works with Ivanti Mac Antivirus on target devices.

This page contains the following options:

- **Enable File antivirus:** Enables real-time scanning of files on target devices. If you do not enable File Antivirus, the collected statistics appear in the Completed tasks section of the report window. When the component runs, it generates a new report. By default, File Antivirus is enabled and configured with the recommended settings.
- **Security Level**: Specifies one of the three file security levels: Maximum protection, Recommended, or Maximum speed. To select a security level, move the slider up or down the scale. If none of the preset security levels meets your needs, you can customize the scan settings by selecting settings on the **General, Protection scope**, and **Additional** tabs. This will change the name of the security level to Custom. Select the level closest to your requirements as a basis and then modify its settings.

  **Maximum protection**: Provides the most complete scan of the files you open, save, or start.

  **Recommended**: Contains the settings recommended by Ivanti, which provides for scan of: programs and objects by content, only new objects and objects modified since the last scan, and embedded OLE objects. This level is set by default.

  **Maximum speed**: Allows you to comfortably work with applications requiring significant system resources, since the range of files scanned is smaller.
• **General:**
  - **File types**: Specifies whether to scan all files, scan by content, or scan by extension.
    - **Scan all files**: Specifies which formats of objects should be scanned for viruses when they are opened, run, or saved.
    - **Scan programs and documents (by content)**: Enables only the scan of potentially infected objects, or files that a virus could penetrate. The internal header of the file is scanned to identify its format (TXT, DOC, EXE, etc.). If the scan reveals that a file of such format cannot be infected, it does not scan it for viruses and immediately makes it accessible to the user. If such format is susceptible to viruses, a scan is performed.
    - **Scan programs and document (by extension)**: Enables only the scan of potentially infected objects, but the file format is determined by its extension. Files without extension are always scanned irrespective of the file type selected.

    NOTE: Do not forget that someone could send a virus to your computer with the .txt extension, although in reality it could be an executable file renamed as a .txt file. If you select the Scan programs and documents (by extension) option, such files will be skipped by the scan. If you select the Scan programs and documents (by content) option, Ivanti Mac Antivirus analyzes the file header, determines that the file has the .exe format and scans it for viruses.

- **Scan new and changed files only**: Enables File Antivirus to scan only new files and files that have been modified since the previous scan. This mode applies both to simple and compound files.
- **Scan archives**: Enables File Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.
- **Scan installation packages**: Enables File Antivirus to scan self-extracting archives.
- **Scan embedded objects**: Enables File Antivirus to scan documents that are embedded in another file, such as Excel spreadsheets, macros, and email attachments.
- **Postpone extracting if archive larger than**: Sets a restriction on the scan of large objects. Any compound file with a size exceeding the specified limit value will be scanned as a single object (its header will be scanned). Objects contained in it will be scanned later. If you do not select this option, access to files larger than the size indicated will be blocked until they have been scanned. This option is enabled by default with the value of 0 MB.
Do not process archives larger than: Sets a restriction on large archives. Any compound file with a size exceeding the specified limit value will be skipped without being scanned for viruses. This option is enabled by default with the value of 8 MB.

Protection scope: Specifies whether to scan all removable drives, all hard drives, or all network drives.

Additional: Specifies the mode and technology File Antivirus will use and when it will pause.

Scan mode: In the default scan mode, Smart mode, File Antivirus scans files by analyzing operations performed with a file by the user, an application, or the operating system. In the On access and modification mode, File Antivirus scans files when the user, an application, or the operating system attempts to open or modify the files. In the On access mode, File Antivirus scans files only when the user, an application, or the operating system attempts to open the files. In the On execution mode, File Antivirus scans files only when the user, an application, or the operating system attempts to run files.

iSwift technology: Specifies the scan technology that File Antivirus uses when scanning files. The iSwift technology allows File Antivirus to exclude certain objects from scan using a special algorithm in order to increase the scan speed. The algorithm takes into account the release date of the antivirus databases, the date of the most recent scan of an object, and any changes to the scan settings. This technique works with objects of any format, size, and type.

Use heuristic analyzer: This setting defines the depth of heuristic analysis. Scan level ensures the balance between the thoroughness of searches for new threats, the load on the operating system's resources, and the scan time length. To set a scan level, move the slider along the scale.

Optimal protection level: Heuristic analyzer, emulating the operation of the application being scanned, makes as many operations as required to detect a threat with an acceptable probability value. While this process is in progress, the CPU is not overloaded so that it does not impact the performance of other applications. This scan level is set by default.

High protection level: Heuristic analyzer, emulating the operation of the application being scanned, makes as many operations as required to detect a threat with a higher probability value. While this process is in progress, load on the CPU increases, and the scan takes more time.

Maximum protection level: Heuristic analyzer, emulating the operation of the application being scanned, makes as many operations as required to detect a threat with a maximum probability value. While this process is in progress, the scan takes a lot of time and requires significant CPU resources. The performance of other applications is significantly reduced.
• **Action:** Specifies the action that File Antivirus performs if infected files are detected. Before attempting to disinfect or delete an infected file, File Antivirus creates a backup copy for subsequent restoration or disinfection.

  • **Prompt for action:** File Antivirus displays a warning message with the information about which malicious code has infected or potentially infected the file, and offers you the selection of further actions. These actions may vary depending on the object's status.

  • **Block access:** File Antivirus blocks access to an infected or potentially infected object, without moving it to another folder. Information about this is logged in the report under the Detected tab. To gain access, process the objects in the report.

  • **Disinfect:** Enables automatic disinfection of all infected objects that have been detected. File Antivirus blocks access to the infected object and attempts to disinfect it. A backup copy of the object is moved to Backup Storage. If it is successfully disinfected, it is restored for regular use. File Antivirus does not move the object if the attempt to cure it is unsuccessful. Information about this is logged in the report under the Detected tab. To gain access, process the objects in the report.

  • **Delete if disinfection fails:** Enables the option to automatically delete infected objects if the recovery attempt for them failed. The box is checked by default if the Block access action is selected and the Disinfect box is checked.

**About the Ivanti Mac Antivirus Virus Scan page**

In addition to the protection of the file system provided by File Antivirus in real-time mode, it is extremely important to scan your computer for viruses regularly. This is required to stop the spread of malicious programs that have gone undetected by File Antivirus. For example, this would be necessary if the selected level of protection was too low.

Ivanti Mac Antivirus comprises the following integrated virus scan tasks:

  • **Virus Scan:** Scan individual items for viruses, such as files, folders, disks, plug-and-play devices.
  
  • **Full Scan:** Search for viruses on your computer with a thorough scan of all hard drives.

  • **Quick Scan:** Scans only critical areas of the computer for viruses, including folders with operating system files and system libraries.

If you want to schedule a full or quick client scan, change the Run mode on the [Full Scan](#) page or the [Quick Scan](#) page.

This page contains the following options:

  • **Security Level:** Specifies one of the three file security levels: Maximum protection, Recommended, or Maximum speed.

  • **Maximum protection:** Security level that provides the most complete scan of the files you open, save, or start.
**Recommended**: Default security level that provides for scan of the following categories of objects: programs and objects by content, only new objects and objects modified since the last scan, and • embedded OLE objects.

**Maximum speed**: Security level that allows you to comfortably work with applications requiring significant resources. Range of files being scanned at this level is reduced.

- **File types**: Specifies whether to scan all files, scan by content, or scan by extension.
  - **All files**: If you click this option, Ivanti Mac Antivirus scans absolutely all files on your computer.
  - **Scan programs and documents (by content)**: Ivanti Mac Antivirus only scans potentially infected objects, such as files that may turn out to have been infected with a virus. First of all, the internal header of the file is scanned to identify its format (txt, doc, exe, and so on.). If the scan reveals that a file of such format cannot be infected, it does not scan it for viruses and immediately makes it accessible to the user. If the file format allows a risk of infection, the file will be scanned for viruses.
  - **Scan programs and document (by extension)**: Ivanti Mac Antivirus will only scan potentially infected files, but the file format will be determined by extension. Files without extension are always scanned irrespective of the file type you select.

**NOTE**: Do not forget that someone could send a virus to your computer with the .txt extension, although in reality it could be an executable file renamed as a .txt file. If you select the Scan programs and documents (by extension) option, such files will be skipped by the scan. If you select the Scan programs and documents (by content) option, Ivanti Mac Antivirus analyzes the file header, determines that the file has the .exe format and scans it for viruses.

- **Optimization**:
  - **Skip if scan takes longer than**: Specifies in seconds the length of time to scan a file before skipping it.
  - **Do not scan archives larger than**: Excludes large archives from scan. By default, the value is set to 100 MB.
  - **Scan only new and changed files**: Enables Ivanti Mac Antivirus to scan only new files and files that have been modified since the previous scan. This mode applies both to simple and compound files.
  - **iSwift technology**: Enables the use of the iSwift technology, which allows Ivanti Mac Antivirus to exclude certain objects from scan using a special algorithm in order to increase the scan speed. The algorithm takes into account the release date of the antivirus databases, the date of the most recent scan of an object, and any changes to the scan settings. This technique works with objects of any format, size and type. There are limitations to iSwift: it is bound to a specific file location in the file system and only applies to objects in HFS.
- **Compound files:**
  - **Scan archives:** Enables Ivanti Mac Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives. On a full scan, this option is enabled by default. Certain archive files (such as .har, .uue, .tar archives) cannot be deleted automatically since Ivanti Mac Antivirus does not support their disinfection, even if you select the Disinfect and Delete if disinfection fails options. To delete such archives, click the Delete archive button in the dangerous object detection notification window. This notification is displayed on the screen after the application starts processing the objects detected during the scan. You can also delete infected archives manually.
  - **Scan embedded objects:** Enables Ivanti Mac Antivirus to scan objects embedded in a file, such as Excel spreadsheets, macros, email attachments, and so on.
  - **Scan email format files:** Enables the scan of email-format files and email databases. Ivanti Mac Antivirus examines the email-format file and scans each of its components (body, attachments) for viruses. If you clear this option, Ivanti Mac Antivirus scans the email file as a single object.
  - **Scan password-protected archives:** Enables the scanning of archives that are protected with a password. Click this option to display the password request window on the screen before scanning objects contained in the archive. Otherwise, Ivanti Mac Antivirus will skip password-protected archives when scanning.
  - **Heuristic analyzer:** Defines the depth of heuristic analysis. Scan level ensures the balance between the thoroughness of searches for new threats, the load on the operating system's resources, and the scan time length. To set a scan level, move the slider along the scale.
• **Action**: Specifies the action that Ivanti Mac Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Mac Antivirus creates a backup copy for subsequent restoration or disinfection.

  • **Prompt for action when the scan is complete**: After the scan is complete, Ivanti Mac Antivirus displays a warning message with the information about which malicious code has infected or potentially infected the file, and offers you the selection of further actions. These actions may vary depending on the object’s status.

  • **Prompt for action during scan**: During the scan, File Antivirus displays a warning message with the information about which malicious code has infected (potentially infected) the file, and offers you the selection of further actions. These actions may vary depending on the object’s status.

  • **Do not prompt for action**:
    - **Disinfect**: Ivanti Mac Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Mac Antivirus blocks access to the infected object and attempts to disinfect it. A backup copy of the object is moved to Backup Storage. If it is successfully disinfected, it is restored for regular use. It does not move the object if the attempt to cure it is unsuccessful. Information about this is logged in the report under the Detected tab. To gain access, process the objects in the report.

  - **Delete if disinfection fails**: Ivanti Mac Antivirus automatically delete infected objects if the recovery attempt for them failed.

**About the Ivanti Mac Antivirus Virus Scan: Full Scan page**

In addition to the protection of the file system provided by File Antivirus in real-time mode, it is extremely important to scan your computer for viruses regularly. This is required to stop the spread of malicious programs that have gone undetected by File Antivirus. For example, this would be necessary if the selected level of protection was too low.

Ivanti Mac Antivirus comprises the following integrated virus scan tasks:

  • **Virus Scan**: Scan individual items for viruses, such as files, folders, disks, plug-and-play devices.

  • **Full Scan**: Search for viruses on your computer with a thorough scan of all hard drives.

  • **Quick Scan**: Scans only critical areas of the computer for viruses, including folders with operating system files and system libraries.

Use this page to configure the way Ivanti Mac Antivirus performs full scans on target devices. If you want to schedule a quick client scan, change the Run mode on the **Quick Scan** page.

This page contains the following options:

  • **Security Level**: Specifies one of the three file security levels: Maximum protection, Recommended, or Maximum speed.
**Maximum protection:** Security level that provides the most complete scan of the files you open, save, or start.

**Recommended:** Default security level that provides for scan of the following categories of objects: programs and objects by content, only new objects and objects modified since the last scan, and embedded OLE objects.

**Maximum speed:** Security level that allows you to comfortably work with applications requiring significant resources. Range of files being scanned at this level is reduced.

- **File types:** Specifies whether to scan all files, scan by content, or scan by extension.
  - **All files:** If you click this option, Ivanti Mac Antivirus scans absolutely all files on your computer.
  - **Scan programs and documents (by content):** Ivanti Mac Antivirus only scans potentially infected objects, such as files that may turn out to have been infected with a virus. First of all, the internal header of the file is scanned to identify its format (txt, doc, exe, and so on.). If the scan reveals that a file of such format cannot be infected, it does not scan it for viruses and immediately makes it accessible to the user. If the file format allows a risk of infection, the file will be scanned for viruses.
  - **Scan programs and document (by extension):** Ivanti Mac Antivirus will only scan potentially infected files, but the file format will be determined by extension. Files without extension are always scanned irrespective of the file type you select.

**NOTE:** Do not forget that someone could send a virus to your computer with the .txt extension, although in reality it could be an executable file renamed as a .txt file. If you select the Scan programs and documents (by extension) option, such files will be skipped by the scan. If you select the Scan programs and documents (by content) option, Ivanti Mac Antivirus analyzes the file header, determines that the file has the .exe format and scans it for viruses.
- **Optimization:**
  - **Skip if scan takes longer than:** Specifies in seconds the length of time to scan a file before skipping it.
  - **Do not scan archives larger than:** Excludes large archives from scan. By default, the value is set to 100 MB.
  - **Scan only new and changed files:** Enables Ivanti Mac Antivirus to scan only new files and files that have been modified since the previous scan. This mode applies both to simple and compound files.
  - **iSwift technology:** Enables the use of the iSwift technology, which allows File Antivirus to exclude certain objects from scan using a special algorithm in order to increase the scan speed. The algorithm takes into account the release date of the antivirus databases, the date of the most recent scan of an object, and any changes to the scan settings. This technique works with objects of any format, size and type. There are limitations to iSwift: it is bound to a specific file location in the file system and only applies to objects in HFS.

- **Compound files:**
  - **Scan archives:** Enables Ivanti Mac Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives. On a full scan, this option is enabled by default. Certain archive files (such as .ha, .uue, .tar archives) cannot be deleted automatically since Ivanti Mac Antivirus does not support their disinfection, even if you select the Disinfect and Delete if disinfection fails options. To delete such archives, click the Delete archive button in the dangerous object detection notification window. This notification is displayed on the screen after the application starts processing the objects detected during the scan. You can also delete infected archives manually.
  - **Scan embedded objects:** Enables Ivanti Mac Antivirus to scan objects embedded in a file, such as Excel spreadsheets, macros, email attachments, and so on.
  - **Scan email format files:** Enables the scan of email-format files and email databases. Ivanti Mac Antivirus examines the email-format file and scans each of its components (body, attachments) for viruses. If you clear this option, Ivanti Mac Antivirus scans the email file as a single object.
  - **Scan password-protected archives:** Enables the scanning of archives that are protected with a password. Click this option to display the password request window on the screen before scanning objects contained in the archive. Otherwise, Ivanti Mac Antivirus will skip password-protected archives when scanning.
  - **Heuristic analyzer:** Defines the depth of heuristic analysis. Scan level ensures the balance between the thoroughness of searches for new threats, the load on the operating system's resources, and the scan time length. To set a scan level, move the slider along the scale.
• **Action:** Specifies the action that Ivanti Mac Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Mac Antivirus creates a backup copy for subsequent restoration or disinfection.
  
  • **Prompt for action when the scan is complete:** After the scan is complete, Ivanti Mac Antivirus displays a warning message with the information about which malicious code has infected (potentially infected) the file, and offers you the selection of further actions. These actions may vary depending on the object’s status.
  
  • **Prompt for action during scan:** During the scan, Ivanti Mac Antivirus displays a warning message with the information about which malicious code has infected (potentially infected) the file, and offers you the selection of further actions. These actions may vary depending on the object’s status.
  
  • **Do not prompt for action:**
    
    • **Disinfect:** Ivanti Mac Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Mac Antivirus blocks access to the infected object and attempts to disinfect it. A backup copy of the object is moved to Backup Storage. If it is successfully disinfected, it is restored for regular use. It does not move the object if the attempt to cure it is unsuccessful. Information about this is logged in the report under the Detected tab. To gain access, process the objects in the report.
    
    • **Delete if disinfection fails:** Ivanti Mac Antivirus automatically delete infected objects if the recovery attempt for them failed.
    
  • **Run mode:** By default, Ivanti Mac Antivirus scans once a day. To change the schedule, click Edit... to open the Run mode dialog box. In the Frequency list, select how often Ivanti Mac Antivirus will scan, then specify the additional details that apply to the selected frequency.

### About the Ivanti Mac Antivirus Virus Scan: Quick Scan page

In addition to the protection of the file system provided by File Antivirus in real-time mode, it is extremely important to scan your computer for viruses regularly. This is required to stop the spread of malicious programs that have gone undetected by File Antivirus. For example, this would be necessary if the selected level of protection was too low.

Ivanti Mac Antivirus comprises the following integrated virus scan tasks:

• **Virus Scan:** Scan individual items for viruses, such as files, folders, disks, plug-and-play devices.

• **Full Scan:** Search for viruses on your computer with a thorough scan of all hard drives.

• **Quick Scan:** Scans only critical areas of the computer for viruses, including folders with operating system files and system libraries.

Use this page to configure the way Ivanti Mac Antivirus performs critical areas scans on target devices. If you want to schedule a full client scan, change the Run mode on the Full Scan page.

This page contains the following options:
- **Security Level**: Specifies one of the three file security levels: Maximum protection, Recommended, or Maximum speed.
  
  **Maximum protection**: Security level that provides the most complete scan of the files you open, save, or start.
  
  **Recommended**: Default security level that provides the following categories of objects: programs and objects by content, only new objects and objects modified since the last scan, and embedded OLE objects.
  
  **Maximum speed**: Security level that allows you to comfortably work with applications requiring significant resources. Range of files being scanned at this level is reduced.

- **File types**: Specifies whether to scan all files, scan by content, or scan by extension.
  
  - **All files**: If you click this option, Ivanti Mac Antivirus scans absolutely all files on your computer.
  
  - **Scan programs and documents (by content)**: Ivanti Mac Antivirus only scans potentially infected objects, such as files that may turn out to have been infected with a virus. First of all, the internal header of the file is scanned to identify its format (txt, doc, exe, and so on.). If the scan reveals that a file of such format cannot be infected, it does not scan it for viruses and immediately makes it accessible to the user. If the file format allows a risk of infection, the file will be scanned for viruses.
  
  - **Scan programs and document (by extension)**: Ivanti Mac Antivirus will only scan potentially infected files, but the file format will be determined by extension. Files without extension are always scanned irrespective of the file type you select.

---

NOTE: Do not forget that someone could send a virus to your computer with the .txt extension, although in reality it could be an executable file renamed as a .txt file. If you select the Scan programs and documents (by extension) option, such files will be skipped by the scan. If you select the Scan programs and documents (by content) option, Ivanti Mac Antivirus analyzes the file header, determines that the file has the .exe format and scans it for viruses.
• **Optimization:**
  - **Skip if scan takes longer than:** Specifies in seconds the length of time to scan a file before skipping it.
  - **Do not scan archives larger than:** Excludes large archives from scan. By default, the value is set to 100 MB.
  - **Scan only new and changed files:** Enables Ivanti Mac Antivirus to scan only new files and files that have been modified since the previous scan. This mode applies both to simple and compound files.
  - **iSwift technology:** Enables the use of the iSwift technology, which allows File Antivirus to exclude certain objects from scan using a special algorithm in order to increase the scan speed. The algorithm takes into account the release date of the antivirus databases, the date of the most recent scan of an object, and any changes to the scan settings. This technique works with objects of any format, size and type. There are limitations to iSwift: it is bound to a specific file location in the file system and only applies to objects in HFS.

• **Compound files:**
  - **Scan archives:** Enables Ivanti Mac Antivirus to scan RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives. On a full scan, this option is enabled by default. Certain archive files (such as .ha, .uue, .tar archives) cannot be deleted automatically since Ivanti Mac Antivirus does not support their disinfection, even if you select the Disinfect and Delete if disinfection fails options. To delete such archives, click the Delete archive button in the dangerous object detection notification window. This notification is displayed on the screen after the application starts processing the objects detected during the scan. You can also delete infected archives manually.
  - **Scan embedded objects:** Enables Ivanti Mac Antivirus to scan objects embedded in a file, such as Excel spreadsheets, macros, email attachments, and so on.
  - **Scan email format files:** Enables the scan of email-format files and email databases. Ivanti Mac Antivirus examines the email-format file and scans each of its components (body, attachments) for viruses. If you clear this option, Ivanti Mac Antivirus scans the email file as a single object.
  - **Scan password-protected archives:** Enables the scanning of archives that are protected with a password. Click this option to display the password request window on the screen before scanning objects contained in the archive. Otherwise, Ivanti Mac Antivirus will skip password-protected archives when scanning.

• **Heuristic analyzer:** Defines the depth of heuristic analysis. Scan level ensures the balance between the thoroughness of searches for new threats, the load on the operating system's resources, and the scan time length. To set a scan level, move the slider along the scale.
• **Action:** Specifies the action that Ivanti Mac Antivirus performs if infected files are detected when scanning. Before attempting to disinfect or delete an infected file, Ivanti Mac Antivirus creates a backup copy for subsequent restoration or disinfection.
  
  • **Prompt for action when the scan is complete:** After the scan is complete, Ivanti Mac Antivirus displays a warning message with the information about which malicious code has infected (potentially infected) the file, and offers you the selection of further actions. These actions may vary depending on the object’s status.

  • **Prompt for action during scan:** During the scan, Ivanti Mac Antivirus displays a warning message with the information about which malicious code has infected (potentially infected) the file, and offers you the selection of further actions. These actions may vary depending on the object’s status.

  • **Do not prompt for action:**
    
    • **Disinfect:** Ivanti Mac Antivirus automatically attempts to disinfect all infected files that are detected. Ivanti Mac Antivirus blocks access to the infected object and attempts to disinfect it. A backup copy of the object is moved to Backup Storage. If it is successfully disinfected, it is restored for regular use. It does not move the object if the attempt to cure it is unsuccessful. Information about this is logged in the report under the Detected tab. To gain access, process the objects in the report.

    • **Delete if disinfection fails:** Ivanti Mac Antivirus automatically delete infected objects if the recovery attempt for them failed.

    • **Run mode:** By default, Ivanti Mac Antivirus scans once a day. To change the schedule, click **Edit...** to open the Run mode dialog box. In the Frequency list, select how often Ivanti Mac Antivirus will scan. In the Schedule section, specify the additional details that apply to the selected frequency.

  
  **About the Ivanti Mac Antivirus Threats page**

  Use this page to configure the way Ivanti Mac Antivirus handles various types of malware.

  This page contains the following options:

  • **Malware categories:** Allows you to create a list of threats to detect by enabling control of the most dangerous types of malware.

    • **Virus, worms, Trojans, hack tools:** This group includes the most common and dangerous categories of malware. Ivanti Mac Antivirus always controls malware from this group. This option is selected by default and cannot be cleared.

    • **Spyware and adware:** Enables control of riskware. This option is selected by default.

    • **Auto-dialers:** Enables control of programs that establish phone connections over a modem in hidden mode. This option is selected by default.

    • **Other programs:** Enables control of programs that are not malicious or dangerous but under certain circumstances may be used to do harm to your computer.
- **Trusted zone**: Specifies the objects that Ivanti Mac Antivirus will exclude from the scan. Click Add... to specify the object, threat type, and component for each trusted item.
  - **Object**: Specify all objects or enter the path to a trusted object. The name of a file, folder, or a file mask can be specified as an object.
  - **Threat type**: Specify all threats or enter a threat name. The box next to each element of the list enables or clears the use of this exclusion rule. All boxes are checked by default. The list of trusted zone objects is blank by default.
  - **Component**: Specify whether to exclude the trusted item from File Antivirus, Virus scan, or both.

**About the Ivanti Mac Antivirus: Scheduled Tasks page**

Use this page to schedule client pattern file updates for Mac computers. Macs use the OS X 'launchd' service to download and install these updates, from either the core or Kaspersky's site. If you want to schedule a full or quick client scan, change the Run mode on the Full Scan page or the Quick Scan page.

This page contains the following options:

- **Scheduled tasks**:
  - **Update**: Specifies when to update virus definitions. Click Change schedule... to open the Schedule periodic virus definition updates window, where you can select the frequency and time of an update.

**About the Ivanti Mac Antivirus Scheduled Tasks: Update page**

Use this page to configure virus definition (pattern) file updates scheduling, user download options, and access options for target devices with these antivirus settings. To schedule an update, click Update on the Scheduled Tasks page.

This page contains the following options:

- **Download "pilot" version of virus definition files**: Click this option to download virus definition files from the pilot folder instead of from the default location 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 choose 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 devices receive the latest known virus definition files. If this option is selected, virus definition files in the default folder are not downloaded.
- **Download virus definition updates from**: Specifies the source site (core server or Kaspersky content server) from which virus definition files are downloaded.
**Preferred server/Peer download options:** Allows you to configure core server settings if you’ve selected one of the download source site options that includes the core.

  - **Attempt preferred server:** Prevents virus definition file downloads via a preferred server. For more information about preferred servers, see "About software distribution" (457).

**Bandwidth used from core or preferred server (WAN):** Specifies the bandwidth used. You can move the slider or enter a value in the percentage box.

**Update application modules:** Enables downloads of application module updates along with antivirus database updates. If selected, Ivanti Mac Antivirus includes application module updates in the update package when the application runs the update task. This option is selected by default.

**Rescan Quarantine after update:** Enables the scan of the content of Quarantine after each update. Quarantine stores objects whose contents include malware that was not properly identified by File Antivirus or during a virus scan task. After the databases are updated, Ivanti Mac Antivirus will most likely be able to clearly identify and eliminate the threat.

### About the Ivanti Mac Antivirus Reports page

Use this page to configure Ivanti Mac Antivirus Reports settings on target devices.

This page contains the following options:

- **Reports:**
  - **Log non-critical events:** Enables the logging of information-type events. As a rule, these events are not important for security.
  - **Keep only recent events:** Enables the logging of important events only, which have occurred at the last run of the task. If the box is checked, the information will be updated every time the task is restarted. At that, important information (such as entries of detected malicious objects) will be saved, while non-critical information will be deleted.
  - **Delete reports after:** Specifies the maximum report storage term in number of days. The default maximum storage term for reports is 30 days. After that period of time, Ivanti Mac Antivirus automatically deletes the oldest entries from the report file.

- **Quarantine and Backup storage:** Allows you to configure quarantine and backup settings. The data storage comprises a quarantine catalog and storage for backup copies of files.
  - **Delete objects after:** Specifies the maximum storage term for files in quarantine and copies of files in backup. The maximum file storage term is measured in days. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Ivanti Mac Antivirus deletes the oldest files from Quarantine and Backup.

### About the Ivanti Mac Antivirus Service page

Use this page to configure the Service settings that Ivanti Mac Antivirus will use on target devices.

This page contains the following options:
- **Autorun**: Specifies whether Ivanti Mac Antivirus will run during computer startup. This option is checked by default.
- **Battery**: Specifies whether to disable scheduled scans while running on battery power. This option is checked by default.

**About the Ivanti Mac Antivirus Appearance page**

Use this page to configure the Appearance settings that Ivanti Mac Antivirus will use on target devices.

This page contains the following options:

- **In Menu Bar**: Displays the Ivanti Mac Antivirus icon in the menu bar. This option is selected by default.
- **In Dock**: Displays the Ivanti Mac Antivirus icon in the Dock. Any changes you make to the location of the icon will appear after you restart the application.
- **Nowhere**: Click this option if you do not want the Ivanti Mac Antivirus icon to appear.

**About the Ivanti Mac Antivirus Import Kaspersky settings page**

Use this page to configure how Ivanti Mac Antivirus will import Kaspersky settings on target devices.

This page contains the following options:

- **Import settings file from a Kaspersky antivirus client**: Lets you import settings from a client device. To import the settings, specify Kaspersky settings on a client and save the settings as a configuration file. From the console, browse to the configuration file. The options listed in the file will be set first and then any Ivanti Antivirus settings will be set.

  **NOTE:** Ivanti Antivirus won’t look for a new configuration file and automatically update it. You must manually update the configuration file if you want to import different settings.

- **Current configuration imported from**: The Browse button [...] opens the Select a previously saved Kaspersky configuration file window. Browse to the \dlogon folder, click the configuration file, then click Open.
- **Clear password after import**: Enables users to change Kaspersky settings without the settings file password.
- **On date**: The date of the import.
- **Notes**: Any notes about the configuration file.

**Agent settings: Mac configuration profile**

Tools > Configuration > Agent Settings > Mac configuration profile
Use the Mac configuration profile dialog box to select Mac configuration profiles that you want to apply to Macintosh OS X devices. For more information, see "Applying Mac configuration profiles" (653).

This dialog box contains the following options:

- **Name**: Type a unique identifier for the settings.
- **Rules**:
  - **Available configurations**: Move one or more Available configurations to the Selected configurations list to select them for this named setting.
  - **Import...**: Opens the Import new mac configuration profile dialog box, where you can browse for an existing .mobileconfig file. Give it a descriptive Display name and click Import. At this point the .mobileconfig file contents are imported into the LDMS database.

**NOTE:** The Ivanti console doesn't currently have an XML viewer for this content, so you may want to keep a copy of the file for future reference, even though the core server and console no longer need it.

- **Mode**: Select whether you want to Append or Replace the configuration profile. Append preserves existing profile settings. Replace removes all existing profile settings, including settings you aren’t modifying, and replaces them with the profile settings you specified.
- **Set as default**: Establishes all of the settings on the Mac configuration profile dialog box as the default settings. The name you entered will appear in the console with the default icon next to it. You cannot delete a setting that is marked as default. When you create a new agent configuration, those settings will be selected by default.

**Agent settings: Exchange/Office 365**

**Tools > Configuration > Agent settings > Mobility > Mobile Exchange/Office 365**

The Mobile Exchange/Office 365 dialog box allows you to configure the mail server settings for iOS and Android for Work devices. After a device connects for the first time, it applies these settings and the user can access his mail account.

> **For users with Android for Work, they’ll need to install Gmail or Divide Productivity to receive these settings.**

The Mobile Exchange/Office 365 dialog box contains the following options:

- **Use email address from company Active Directory to log in**: Uses the email address listed for the user in Active Directory to log in to the email account from the user’s device. This email address replaces both the username and email address for that device’s Exchange profile. This option is only available if you have configured a connection to the Active Directory server. (To configure the Active Directory server information, go to the Network View, right-click the Directory node, and click Manage Directory.)
For companies using Microsoft Office 365 that want Active Directory to use your existing email addresses, set up your Office 365 account for Active Directory synchronization.

If you already have Active Directory set up with email addresses, this is the recommended option for synchronizing email accounts to devices.

- **Hosted company domain**: Generates an email address from the username and the value of this field if you are using an external mail server, such as Microsoft Office 365 or Gmail. This email address replaces both the username and email address for that device’s Exchange profile. All usernames must be imported into the external mail server, such as Office 365, for this to work. For example, if a user is listed in Active Directory as jdoe, and receives a payload where this value is mycompany.onmicrosoft.com, the mail app attempts to log in to the mailbox using the email address:

  jdoe@mycompany.onmicrosoft.com

  This option is only available if you have Ivanti Mobility Manager and it is configured with the Active Directory information.

- **Account name**: The name of the account on the phone. This should only be configured if you are creating agent settings for an individual user.

- **Server address**: The domain name or address of the server.

- **Past days of mail to sync**: The number of days’ worth of mail to sync to the device.

- **Use SSL**: Uses an encrypted SSL connection to send mail to the Exchange server.

- **Allow user to move messages from this account**: Allows user to move messages to a different account on the device, or reply to or forward messages using a different mail account. This is only available for iOS devices.

- **Allow recent addresses to be synced using iCloud**: Allows recently used addresses to be synced with other devices using iCloud. This is only available for iOS devices.

- **Only allow this account to send mail from the Mail app**: Only allows messages to be sent from the Mail application, not from other phone applications such as Photos or Safari. This is only available for iOS devices.

### Android for Work Considerations

If you perform a selective wipe or a selective wipe and delete on an Android for Work device, the settings will still remain on the device. You must perform a factory reset to fully remove it.

When removing this setting from affected Android for Work devices, this email account cannot be removed in the Gmail app. Device owners must delete the app.
Agent settings: Mobile Compliance

Tools > Configuration > Agent settings > Mobility > Mobile Compliance

The Mobile Compliance dialog box allows you to configure compliance settings that regulate jailbreaking and rooting of devices, version control, and geofencing.

Compliance page

- **Enable compliance settings**: Enables all compliance settings.
- **Rules List**: Lists all compliance rules applied. To create a new rule, click **Add**. To access the Rule Settings page, select a rule and click **Edit**.

Rule Settings page

- **Jailbreak/Rooted**: Restricts devices with jailbroken or rooted operating systems.
- **Version Control**: Restrict device OS versions. This can be set for both Android and iOS devices.
- **Platform**: Sets the required operating system.
- **Version**: Sets the required operating system version.
- **Out of Geofence (Android only)**: Allows you to specify geofencing coordinates to ensure corporate devices are kept within a confined space, such as a corporate building. This is only available for Android devices.
- **Latitude**: The latitude of the location you wish to restrict devices to.
- **Longitude**: The latitude of the location you wish to restrict devices to.
- **Radius (meters)**: Sets the radius a device may travel within the specified latitude and longitude. By default, this is set to 10.
- **Minimum device accuracy (meters)**: Sets the accuracy of detecting a device's location. By default, this is set to 10.
- **Mobile Action**: Sets the desired behavior when a restricted device violates a compliance setting. You can force a device to lock, perform a selective wipe, or perform a full factory reset.
- **Email**: Specifies an administrator email address that violation alertss will be sent to.
- **Quarantine of email**: If the device is out of compliance, users cannot send or receive emails.

Email Config page

These are the settings to use for sending emails to users when a device is out of compliance with a rule setting.
• **SMTP Server:** The SMTP server address.
• **Account:** The administrator’s user account name.
• **Port:** The port of the SMTP server.
• **Password:** The password for the administrator’s user account.
• **Use SSL:** Forces the email connection to use SSL settings when connecting.

**Agent settings: Mobile Connectivity**

*Tools > Configuration > Agent settings > Mobility > Mobile Connectivity*

The Mobile Connectivity dialog box allows you to configure certificates and Wi-Fi settings for Android, iOS, and Windows devices. After a device connects for the first time, it applies these settings.

The General page allows you to provide a name for the settings and set it as the default setting.

Not all options are supported on all device types. If you disable options after the settings have been distributed to devices, the settings are removed from devices.

**Certificate page**

Certificates are currently supported on iOS devices. To remove a certificate from a device after it has been distributed, you can either remove the certificate from this page and sync the device, disable certificate settings and sync the device, or perform a device wipe.

This page contains the following options:

• **Enable certificate settings:** Allows you to distribute certificates to mobile devices.
• **Remove:** Remove a certificate from the agent settings.
• **Add Certificate:** Add or validate a PKCS12 certificate. Browse to the certificate file in the file system and provide the password for the file.

**Wi-Fi page**

This page contains the following options:

• **Enable Wi-Fi settings:** Allows you to distribute Wi-Fi settings to mobile devices.
• **Add:** Add a Wi-Fi network and its authentication information.
  • **Setting name:** A name to identify the settings.

**Authentication tab**

• **SSID:** The service set identifier for the Wi-Fi network.
• **Auto join:** The device automatically joins the network when it is available.
• **Hidden network:** Allows the device to find the network when it is not open or broadcasting.

• **Authentication type:** The authentication type that the network supports.

• **Password:** The password used to join the network.

• **Protocols:** The authentication protocol or protocols that the network supports. If you enable TTLS, be sure to choose the Inner Identity type from the drop-down menu. If you enable EAP-FAST and Use PAC, you must either enable Provision PAC or else distribute the PAC through another method. To use SCEP, you must use the **TLS** protocol.

• **Authentication:** Credentials to access the network. If the device must provide an identity certificate, you must configure the certificate on the Certificate page before you can select it from the **Identity Certificate** drop-down menu.

• **Trust:** When the network establishes a connection with a secure tunnel, the device may need to know the identity of the authentication server. Provide the certificates presented by the RADIUS servers. Certificates appear in the **Trusted Certificates** box after they have been added on the Certificate page. If you're using SCEP, enable the **Use SCEP** option. You can only enable this security setting when **TLS** is selected as a protocol.

**Proxy tab**

• **Proxy type:** Determines whether the proxy information is set manually or automatically. When you use automatic, provide the proxy server URL.

• **Proxy server URL:** The URL for the proxy server.

• **Proxy server and port:** The URL and port number for the proxy server.

• **Authentication user:** Username to authenticate to the proxy server. This field is only used for iOS devices using manual proxy.

• **Password:** Password to authenticate to the proxy server. This field is only used for iOS devices using manual proxy. If you do not provide a password, the end user must supply the password to access the proxy.

• **Proxy Bypass (Android only):** Addresses or domains for traffic that should bypass the proxy server. For example, you may want to bypass the proxy server when communicating with the Active Directory server.

---

**IMPORTANT:** Not all devices support all proxy settings. If you are using manual proxy, you may need to create separate settings for Android and iOS devices, since the systems do not handle proxies in the same way.
Agent settings: Mobile macOS configuration

Delete this text and replace it with your own content.

General

- Name
- Identifier
- Organization
- Description
- Consent Message
- Security
- Automatically Remove Profile
- Allow save to disk

Certificates

(This is the Drop-down text)

Agent settings: Mobile macOS device configuration

Delete this text and replace it with your own content.

Agent settings: Mobile Security

Tools > Configuration > Agent settings > Mobility > Security

The Mobile Security dialog box allows you to configure security settings on mobile devices.

The General page allows you to provide a name for the settings and set it as the default setting.

If you disable options after the settings have been distributed to devices, the settings are removed from devices. If you disable a passcode requirement, the requirement is removed from the device, but the passcode is not.
Passcode page

The passcode settings here are applied to selected Android, iOS, OS X, and Windows 10 devices. This page contains the following options:

- **Enable passcode settings.** Allows you to configure settings for increased security in accessing devices.
- **Minimum password quality:** A Simple password would be something easily guessed, such as 1111 or ABCD. If you set the minimum password quality to Alphanumeric, the password must contain at least one letter and at least one number.
- **Minimum password length:** Set a minimum length for the password.
- **Lock screen after:** The length of time in minutes of inactivity before the screen locks.
- **Maximum number of failed password attempts before device wipe:** The number of failed attempts to unlock the device before all data on the device is erased.

iOS Restrictions page

The iOS restriction options allow you control over how the device is used. Some options are only available if the device is in Supervised mode. For information about putting a device into Supervised mode, see your Apple documentation.

This page contains the following options:

- **Enable iOS restrictions settings:** Applies the settings on the Device Functionality, Application, Single-app mode, iCloud, and Security and Privacy pages.

Device Functionality page

- **Allow installing apps:** Allows the user to install apps. Removing the check for this option does not prevent users from deleting apps on the device. Mobility Manager cannot prevent the removal of apps at the device level.
- **Allow use of camera:** Allow the user to launch the camera application.
- **Allow FaceTime:** Allows the user to place or receive FaceTime calls.
- **Allow screen capture:** Allows the user to save a screenshot of the display.
- **Allow automatic sync while roaming:** Allows the device to sync accounts automatically even when the device is roaming.
- **Allow Siri:** Allows the user to use Siri, voice commands, or dictation.
- **Allow Siri while locked:** Allows the user to use Siri without entering a passcode when the device is locked.
• **Allow Siri querying user-generated content (Supervised only):** Allows access to content in Siri added by other users.

• **Allow voice dialing:** Allows the user to dial using a voice command.

• **Allow Passbook while device is locked:** Allows the device to display Passbook notifications while the device is locked.

• **Allow in-app purchases:** Allows the user to make purchases through installed apps.

• **Force user to enter password for all purchases:** Forces the user to type in his iTunes Store account password each time he makes a purchase.

• **Allow multiplayer gaming:** Allows the user to play multiplayer games in the Game Center.

• **Allow adding Game Center friends:** Allows the user to add friends in the Game Center.

• **Allow Control Center while locked:** Allows the user to swipe up to view the Control Center even when the device is locked.

• **Allow Notification view while locked:** Allows the user to view notifications even when the device is locked.

• **Allow Today view while locked:** Allows the user to swipe down to see the Today View even when the device is locked.

• **Allow iBooks Store:** Allows the user to access the iBooks Store. This option is only applied if the device is in Supervised mode.

• **Allow use of AirDrop:** Allows the user to access AirDrop. This option is only applied if the device is in Supervised mode.

• **Allow account change:** Allows the user to change account settings. This option is only applied if the device is in Supervised mode.

• **Allow cellular data usage for apps:** Allows apps on the device to use a cellular data connection. This option is only applied if the device is in Supervised mode.

**Applications page**

• **Allow use of iTunes Store:** Allows the user to access the iTunes Store.

• **Allow Web browser:** Allows the user to launch Safari. When this option is disabled, the user cannot launch Safari, but is still able to launch other Web browsers, such as Chrome.

• **Enable autofill:** Allows the user to turn on Safari's autofill feature.

• **Limit AD tracking:** Prevents the device's ID from being used for advertisement tracking.
• **Force fraud warning:** When the user visits a fraudulent or compromised web site, Safari displays a warning.

• **Allow JavaScript:** Allows web pages that the user accesses using Safari to run JavaScript.

• **Block pop-ups:** Sets Safari to block pop-up messages.

• **Accept cookies:** Allows Safari to accept all cookies, reject all cookies, or accept cookies only from sites that are directly accessed.

• **Allow change to FindMyFriends (Supervised only):** Allows apps to access Find My Friends.

### Content and Ratings page

• **Allow explicit content:** Limits the device to only run content meeting the rating standard specified for that content type.

• **Sets the region for the ratings:** Determines the national standards to use for defining explicit content.

• **Movies:** Specifies the maximum rating allowed for movie content to play on the device.

• **TV Shows:** Specifies the maximum rating allowed for TV show content to play on the device.

• **Apps:** Specifies the maximum rating allowed for Apps to install and launch on the device.

### Single-app mode (Kiosk)

• **Enable kiosk mode:** Also known as guided access, this option limits the device to only run the app specified. When kiosk mode is enabled, the device will only launch the app specified and will block other apps. To specify the app for kiosk mode, use the Apple ID. To exit kiosk mode, an administrator must modify the agent settings to turn off kiosk mode and update the device. Kiosk mode is only available for devices that are in Supervised mode. For more information, see your Apple documentation.

• **Apple ID of application to run:** The Apple ID of the application that is allowed to run in kiosk mode.

• **Disable Autolock:** Prevents the device from locking automatically.

• **Disable device rotation:** Disables the display from changing orientation when the device is rotated.

• **Disable ringer switch:** Disables any functionality associated with the ringer switch.

• **Disable sleep/wake button:** Disables any functionality associated with the sleep/wake button.

• **Disable touch:** Disables the touch functionality of the screen.
• **Disable volume button**: Disables any functionality of the volume button.

• **Allow Assistive Touch**: Allows the user to use Assistive Touch features to make the device more accessible. This option is for users who have problems touching the screen or pressing buttons.

• **Allow Assistive Touch adjustment**: Allows the user to configure Assistive Touch options.

• **Allow invert colors**: Allows the user to invert the colors on the screen.

• **Allow user to adjust color inverting**: Allows the user to configure color inversion options.

• **Allow mono audio**: Allows the user to switch the audio output to mono.

• **Allow Speak Selection**: Allows the user to select text and use the Speak Selection feature for text-to-speech.

• **Allow VoiceOver**: Allows the user to use VoiceOver features to make the device more accessible. This option is for users who need audible presentation of screen materials or menus.

• **Allow user to adjust VoiceOver**: Allows the user to configure VoiceOver options.

• **Allow zoom**: Allows the user to use zoom features.

• **Allow user to change zoom**: Allows the user to change the zoom settings.

• **Autonomous permitted App IDs to run**: Allows apps identified by the bundle IDs to enter Single App Mode. This option only applies if you have apps that have the ability to enter Single App Mode. Mobility Manager does not make apps enter Single App Mode, it only allows the app to do it.

**iCloud page**

• **Allow backup**: Allows the user to back up the device using iCloud.

• **Allow document sync**: Allows the user to store documents in iCloud.

• **Allow Photo Stream**: Allows the user to use Photo Stream. If Photo Stream is disabled after the device user has shared photos using Photo Stream, photos already shared are removed.

• **Allow shared photo streams**: Allows the user to share his photo stream and view others’ photo streams.

**Security and Privacy page**

• **Allow unlocking by Touch ID**: Allows the user to use Touch ID to unlock the device.
- **Allow Host Pairing (Supervised only):** Allows the device to pair with computers other than the computer used to put the device in Supervised mode.

- **Allow diagnostic data to be sent to Apple:** Allows the device to send diagnostic data to Apple.

- **Allow user to accept untrusted certificates:** Allows the user to accept TLS certificates that can't be verified. This setting is enforced for Safari, Mail, Contacts, and Calendar.

- **Allow open from managed to unmanaged Apps/Accounts:** Allows the user to switch to unmanaged applications or accounts from a managed app or account. For example, if the email app is managed but the browser app is not, the user would be allowed to click on a link in an email that launches the browser.

- **Allow open from unmanaged to managed Apps/Accounts:** Allows the user to switch to managed apps or accounts from an unmanaged app or account. For example, if the email app is managed but the browser app is not, the user would be allowed to click on a link on a web page that launches the email app.

- **Allow Over-The-Air PKI updates:** Allows public key infrastructure updates. If this option is not enabled, the user may experience issues with any application that depends on certificates, including Internet browsers.

- **Allow interaction while install config profile (Supervised only):** Allows the administrator to send down configuration profiles silently, without user interaction.

- **Force encrypted backups:** Forces the user to encrypt any backups using iTunes.

**Android Restrictions page**

The Android restriction options allow you control over how the device is used. Certain settings only apply to specific profiles, such as those related to Android for Work.

This page contains the following options:

- **Enable Android restrictions settings:** Applies the settings on the Device Functionality, Application, and App Lists pages.

**Device Functionality page**

**Standard Mode tab**

- **Allow use of camera:** Allows the user to launch the camera application.

- **Allow settings changes:** Allows the user to launch the settings app and alter configurations.

- **Allow Bluetooth:** Allows the user to activate Bluetooth and connect to wireless devices.
Profile Owner Mode tab

- **Allow installing apps**: Allows the user to install new apps on the device.
- **Allow use of camera**: Allows the user to launch the camera application.
- **Allow screen capture**: Allows the user to save a screenshot of the display.
- **Allow NFC**: Allows the user to use NFC functionality on the device.
- **Allow apps control**: Allows the user to manage apps on the device.
- **Allow config credentials**: Allows the user to alter credentials for accessing the device.
- **Allow cross-profile copy/paste**: Allows the user to copy and paste data between managed and non-managed apps.
- **Allow modify accounts**: Allows the user to modify individual user accounts on the device.
- **Allow share location**: Allows the user to share their device location with apps.
- **7==7**: Allows the user to remove apps from the device.

Device Owner Mode tab

- **Allow installing apps**: Allows the user to install new apps on the device.
- **Allow use of camera**: Allows the user to launch the camera application.
- **Allow screen capture**: Allows the user to save a screenshot of the display.
- **Allow settings changes**: Allows the user to launch the settings app and alter configurations.
- **Allow Bluetooth**: Allows the user to activate Bluetooth and connect to wireless devices.
- **Allow Microphone**: Allows the user to access the microphone.
- **Allow NFC**: Allows the user to use NFC functionality on the device.
- **Allow USB**: Allows the user to access device contents from a computer via a USB cable.
- **Allow USB Debug**: Allows the user to debug the device from a computer via a USB cable.
- **Allow Tethering (Bluetooth, Wifi, USB)**: Allows the user to tether peripheral devices to the Android device, such as Bluetooth headsets.
- **Allow add user**: Allows the user to add user accounts to the device.
- **Allow adjust volume**: Allows the user to change volume levels on the device.
- **Allow apps control**: Allows the user to manage apps on the device.
- **Allow config cell broadcasts**: Allows the user to configure broadcasts the device receives.
• **Allow config credentials**: Allows the user to alter credentials for accessing the device.
• **Allow config mobile networks**: Allows the user to alter mobile network settings.
• **Allow config vpn**: Allows the user to set up or alter VPNs on the device.
• **Allow config Wi-Fi**: Allows the user to configure Wi-Fi networks.
• **Allow create windows**: Allows the user to create windows.
• **Allow factory reset**: Allows the user to reset the device to its original factory state.
• **Allow install unknown sources**: Allows the user to install apps from unknown sources.
• **Allow modify accounts**: Allows the user to modify individual user accounts on the device.
• **Allow mount physical media**: Allows the user to mount physical external storage volumes.
• **Allow network reset**: Allows the user to reset all network settings.
• **Allow outgoing calls**: Allows the user to perform outgoing calls from the device.
• **Allow remove user**: Allows the user to remove individual user accounts from the device.
• **Allow safe boot**: Allows the user to boot the device using Safe mode.
• **Allow share location**: Allows the user to share their device location with apps.
• **Allow sms**: Allows the user to send SMS messages from the device.
• **Allow uninstall apps**: Allows the user to remove apps from the device.

**Applications page**

• **Allow Web applications**: Allows the user to launch the default Web browser. When this option is disabled, the user cannot launch that app, but is still able to launch other Web browsers.
• **Allow Mail applications**: Allows the user to access mail apps on the device.
• **Allow use of YouTube**: Allows the user to access the YouTube app.
• **Allow Play Store**: Allows the user to access the Play Store app.

**App Lists page**

• **Use App List**: Allows administrators to list specific applications that will be allowed or blocked on the device. Apps must be identified by name and package ID.
• **White List**: Allows administrators to globally restrict what apps can be installed or used on the device.
• **Black List**: Allows administrators to globally restrict what apps cannot be installed or used on the device.

**Agent settings: Other security settings**

Tools > Security and Compliance > Agent settings > Security > Other security settings

Use the **Other security settings** dialog box to specify and save a collection of security settings.

**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 that 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 computer.

**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 isn’t 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 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.

**Agent settings: Portal manager**

**Tools > Configuration > Agent Settings > Portal manager**

Use the Portal manager settings dialog box to specify and save a collection of portal manager settings. The name you give to the settings will appear in the list on the Portal manager page of the Agent configuration dialog box.

**About the General page**

The options on this page determine how the Portal Manager window appears and whether end users can change it.

- **Allow resize**: The end user can change the size of the window.
- **Allow close**: The end user can close the window. If you clear this check box, the Portal Manager stays running as long as the user is logged in.
- **Launch maximized**: The Portal Manager window opens full-screen.
- **Set as default**: The Portal Manager settings you’ve configured should be the default for new agent configurations.
- **View**: Select the default view when Portal Manager opens, **List**, **Small icons**, or **Large icons**.
- **Available types**: The types of content you want visible in Portal Manager. You can select **Apps**, **Docs**, and **Links**.

**About the Applications page**

Use this page to determine which applications appear in the Portal Manager for the end user to select.

- **Available applications**: Select an application from this list and click >> to display it in Portal Manager.
- **Show in portal manager**: The applications in this list are displayed for the end user in Portal Manager. To remove an application, select it and click <<. To change the order in which the applications appear, select an application and click **Move up** and **Move down**.
- **New**: Click this button to define a new application that you can show in Portal Manager.
- **Edit**: Select an application and click this button to change its definition.
- **Copy**: Select an application and click this button to create a new application that is similar to an existing one.
- **Delete**: Select an application and click this button to remove it from the list of available applications.

**To define an application for use in Portal Manager**

1. Click the **New** or **Edit** button on the Applications page.
2. Type the **Application name** you want to appear on the Portal Manager.
3. Enter a **Tooltip** if you want to include additional help for the end user.
4. Type the path to the application.
5. For executable applications, you can specify parameters to run when the application starts in the **Parameters** box.
6. For WPF DLL applications, you can specify a class name in the **Class name** box.
7. Click **Browse** to select an icon to display for the application. Your selection is displayed in the **Image** box.
8. When you've finished, click **Save**.

**About the Branding page**

Use this page to customize how the Portal Manager window looks.

- **Application title**: The name displayed in the title bar. Click **Choose title color** to select a color for the title and user name displayed in the Portal Manager window.
- **Choose taskbar icon**: Click to select an icon for the taskbar. Choose a Windows icon (.ico) file.
- **Choose corporate logo**: Click to select an image that is displayed in the upper left corner of the window. The preferred size is 135 x 52 pixels or smaller.
- **Choose background image**: Click to select an image that is displayed in the background of the window.
- **Preview branding**: Click to view your branding options in an empty window.

**Agent settings: Power management**

**Tools > Security and Compliance > Agent Settings > Power Management > Power Management settings**

Power management uses policy-based management to send stand by, hibernate, shut down, and turn on instructions to your managed computers. Power management policies enable you to control specific computers and groups of computers.
To specify the settings of a new power management policy

1. In the Agent settings window, click **Power Management** to expand it. Right-click **Power management settings**, then click **New**.
2. Enter a name and description for the policy.
3. Add at least one power scheme to the policy. Select settings from the six lists (**Action**, **Device**, **Inactivity trigger**, **Source**, **Day**, and **Time**) and then click **Add power scheme**.

   You can add multiple power schemes as needed. To remove a power scheme from a policy, click the **Delete** button (x) next to the scheme.
4. Expand **Options** in the left column. Select settings on the six options pages.
5. When all options are defined, click **Save**.

**About the Power configuration page**

- **Action**: Select the action to take on the managed computer — hibernate, standby, turn on, turn off, or alert.
- **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** list, the title of this list changes from **Inactivity trigger** to **Shutdown type** (hard or soft).
- **Source**: Select the power source the device is using (plugged in, on batteries, 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.

**About the Options pages**

- **Options**: Disable screen saver, Enable local wakeup, Delay shutdown, Monitor.
- **Process-sensitive trigger**: Enable this option to delay the power policy if any of the listed processes are detected. The policy will continue if no policies are detected after the number of minutes specified. To add processes to this list, use the **Process sensitive trigger list** toolbar button.
- **Usage monitor**: Enable this option to 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.
- **End process**: Enable this option to end the processes in the list during a shutdown. To add processes to this list, use the **End process list** toolbar button.
- **Power buttons**: Enable this option to configure the actions that result when a user presses power buttons on a managed device. Select which action to complete for each type of button when the machine is plugged in or on battery. For each situation, the actions you can choose are **Do nothing**, **Sleep**, **Hibernate**, or **Shut down**.
• **CPU throttling**: Enable this option to configure the CPU throttling (restricting the power levels of the CPU) of a deployed power policy. Select a level of performance when the machine is plugged in or on battery. Performance options are **Highest** (minimum 100 maximum 100), **Adaptive** (minimum 5 maximum 100), **Low** (minimum 5 maximum 50), or **Lowest** (minimum 5 maximum 33).

**Using the Turn On action with Wake on LAN**

Power management uses wake on LAN (WOL) technology, or Intel vPro wake up, 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 adapters that support WOL.

Power Management can’t 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.

**Agent settings: Mac power management**

Use the **Mac power management settings** dialog box to select power management profiles that you want to apply to Macintosh devices.

**About the General setting page**

Use the **General setting** page to specify the following settings:

- **Policy name**: Enter a unique identifier for the new policy. This name will appear in the Inventory.
- **Policy description**: Enter a brief description of the policy for future reference.
- **Battery tab**
  - **Computer sleep**: Specify the amount of time the computer will be inactive before it goes to sleep.
  - **Display sleep**: Specify the amount of time the computer will be inactive before the display goes to sleep.
  - **Put hard disks to sleep when possible**: Enables the hard disk to sleep after a period of inactivity.
  - **Slightly dim the display while on battery power**: Enables the display to dim once the computer is running on battery only.
  - **Enable Power Nap (Applied to solid state disk)**: Enables the use of Power Nap on compatible devices.
• Power Adapter tab
  • Computer sleep: Specify the amount of time the computer will be inactive before it goes to sleep.
  • Display sleep: Specify the amount of time the computer will be inactive before the display goes to sleep.
  • Put hard disks to sleep when possible: Enables the hard disk to sleep after a period of inactivity.
  • Wake for network access: Enables the computer to wake up when the network activity is directed toward the computer. For example, for a patch deployment.
  • Allow power button to put computer to sleep (Applied to OS X pre 10.9): Enables the power button to put the computer to sleep.
  • Start up automatically after a power failure: On Mac desktop computers, you can set OS X to automatically restart if its AC power connection becomes unavailable. For example, if there is a power outage, or someone inadvertently disconnects the AC power cord, your computer starts up again on its own once power is reconnected. This is useful if you normally have your computer set to perform tasks when its left unattended. In OS X Lion and later, you can also set OS X to automatically re-open documents you were working on when you log in.
  • Enable Power Nap (Applied to solid state disk): Enables the use of Power Nap on compatible devices.

About the Schedule page

Use the Schedule page to specify the following settings:

  • Start up or wake: Specify the frequency and time of day that the computer will power up.
  • Sleep/Restart/Shut Down: Use the drop-down menus to schedule when the computer will sleep, restart, or shut down.

Agent settings: Remote control

Tools > Configuration > Agent Settings > Remote control

Use the Remote control settings dialog box to specify and save a collection of remote control settings.

About the General settings page

The Remote control settings dialog box's General settings page contains the following features:

  • Allow HTML access: Allows the remote control agent to receive HTML remote control requests. For more information, see "HTML remote control" (448).
• **Allow legacy remote control access**: Allows the remote control agent to receive legacy remote control requests from the Windows-based remote control viewer application. For more information, see "Using the remote control viewer" (436).

There are two sets of remote control permissions you can grant, one set that affects only the legacy Windows remote control viewer application/agent, and another set that affects both the windows remote control remote control viewer/agent and the HTML remote control viewer/agent.

**Legacy permissions**

- **Remote control**: Grants permission to control the device.
- **Draw**: Grants permission to use the viewer window's drawing tools on the device.
- **Chat**: Grants permission to chat with the device.
- **Run programs on remote device**: Grants permission to run programs on the device.
- **Run as administrator**: Starts programs with administrator permissions.

**Legacy and HTML permissions**

- **Remote control view only**: Remote control sessions are view only. The remote control viewer can only see the remote computer and can't take control of it.
- **Restart**: The remote control viewer can reboot the remote computer.
- **File transfer**: The remote control viewer can exchange files with the remote computer.

**About the Indicator settings page**

The Remote control settings dialog box's Indicator settings 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.

**About the Permission settings page**

The Remote control settings dialog box's Permission settings page contains the following features:

- Permission not needed, full access
- End user must grant permission and must be logged in
- End user must grant permission, but only if they are logged in
- End user must grant permission
• **Display a custom message:**

Prompts the user with a custom message created here for permission to do one of the following:

- Remote control
- Chat
- Remote execute
- File transfer
- Restart
- All permissions
- Ask permission to use all features at one time

• **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 Security settings page

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:** Allows only 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 Permission settings page of this dialog box.

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.

- **Smart card required:** This option is only available when Windows NT security is selected. When you deploy an agent setting with this option selected to managed devices, those devices will require SmartCard hardware authentication before you can remote control them. For more information, see "About SmartCard security" (314).

- **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.

**About Windows NT security/local template**

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 it 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 Ivanti 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 users 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 SmartCard security

SmartCard security requires a hardware SmartCard reader on the device initiating remote control sessions. When a remote device’s agent setting requires a SmartCard for remote control, the session won’t start unless a SmartCard is inserted and the SmartCard PIN is provided. The SmartCard user must also be in the Remote Control Operators or View Only group.

SmartCard security only works on Windows 7 or newer devices. SmartCard authentication also requires the Windows remote control viewer application. HTML remote control doesn’t support SmartCard authentication.

About the Session settings page

The Remote control settings dialog box’s Security settings page contains the following features:

- **Lock the remote control computer when the session ends**: Locks the managed device to secure mode whether the user is logged in or not.
- **Terminate remote access if the user logs out or locks the machine**: Automatically ends the remote control session if the user logs out or locks the machine.
- **Allow the end user to terminate the session**: If this option is selected, users being remote controlled can use the remote control floating icon or the system tray icon to stop an active remote control session. If this option isn’t selected, users won’t be able to stop an active session.
- **Close inactive session after**: If no mouse or keyboard activity is transmitted via the remote control viewer for the duration of this timeout, the session will end.
Agent settings: Tenant

Use the Tenant dialog to manage tenant configurations. For more information, see "Tenant management overview" (982).

This dialog box has the following options:

- Assign a Tenant to this configuration:
- Available Tenants
  - Choose a Tenant:

Agent settings: Windows Firewall

Tools > Security and Compliance > Security > Windows Firewall

For information on these dialog box pages, see "Configure Windows Firewall settings" (156).

Agent settings: Trusted file lists

Tools > Security and Compliance > Security > Endpoint Security > Trusted file lists

About the Trusted file list dialog box

Use this dialog box to manage your trusted file lists. Trusted file lists are comprised of files configured with a specific set of rights (privileges or authorizations) that allow and deny certain actions that can be performed on that file by an application.

This dialog box contains the following options:

- Name: Identifies the trusted file list with a unique name. You can use the Find feature to search for items in a list containing a specific word or phrase. The resulting list displays only those items that matched your search criteria.
- Add: Opens a file explorer dialog box where you can browse and select a file you want to configure with file certifications.
- Edit: Lets you edit the selected file's certifications.
- Delete: Deletes the selected file and its certifications.
- Move: Opens a dialog box that lets you select one or more trusted files and either move or copy them to another list.
- Set as default: Assigns this list as the default trusted file list for tasks that use this HIPS (or Firewall) setting.
- ID: Identifies this particular list. This information is stored in the database and can be used to keep track of each list.

About the Trusted file dialog box

Use this dialog box to configure HIPS and/or Ivanti Firewall rights for a specific application file.
This dialog box 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 Ivanti® Endpoint Manager powered by Landesk 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 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 this 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 Ivanti® Endpoint Manager powered by Landesk software distribution tool, and can be applied to other software distribution applications as well.

• **Learning options**
  - **Lock trusted file (file rights will not be updated via learn mode)**:
  - **Match this entry based only on file name**:
    - **OK**: Saves the file certifications and adds it to the list of certified files in the main HIPS settings dialog box.
    - **Cancel**: Closes the dialog box without saving the file certifications.

**Related topics**

**Agent Settings overview**

Agent Settings control how Ivanti® Endpoint Manager powered by Landesk services and other components operate on managed devices. These components 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.

If a component is installed on a managed device, changes to that component's settings don't require redeployment of the whole agent. Settings are stored as XML files and the managed device only needs an updated XML file to reconfigure how an installed component operates. Changes to a component setting are propagated to all devices with that setting installed automatically.

Use agent configurations to initially deploy or change installed Endpoint Manager components. Use agent settings to modify how installed Endpoint Manager components operate.
Agent Watcher

Agent Watcher overview

Ivanti Agent Watcher is a tool that allows you to proactively monitor the status of selected Ivanti® Endpoint Manager powered by Landesk 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 any time 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.

Agent Watcher monitors Ivanti® Endpoint Manager powered by Landesk agent services and files specified by a device's Agent Watcher settings.

Agent Watcher settings also determine 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.

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.

Monitor services and files with Agent Watcher

You can use Ivanti Agent Watcher to monitor the following services and files.

Monitor services

The following agent services can be monitored:

- Local scheduler
- Ivanti Antivirus
- Policy Invoker
- Remote Control
- Software Monitoring
- Targeted Multicast

CAUTION: 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 can’t be restarted
- Sends alerts to the core server when a service's startup type can’t be changed back to automatic

**Monitor files**

The following files can be monitored:

- Ldiscn32.exe
- Vulscan.dll
- Vulscan.exe
- Sdclient.exe

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

**Enable and configure Agent Watcher**

The Agent Watcher utility is installed with the standard Endpoint Manager 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.

**Enable 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 agent configuration** 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 the 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 new settings or edit existing settings. The applied settings determine 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.

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 new settings or edit existing settings. The applied settings determine 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 you click the OK button, all the selected target devices are updated with the new settings, and a status message appears.

Disable 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 check box is cleared.
3. Click OK.

Generate 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.

**IMPORTANT: 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.

**IMPORTANT: Required rights and roles in order to use the Reports tool**

In order to access the Reports tool, and generate and view reports, a user must have the Ivanti Administrator right (implying full rights) and the specific Reporting roles.

For more information about using the Reports tool, see "Using reports" (381).

**Configure Agent Watcher settings**

Use Agent Watcher settings (click **Tools > Configuration > Agent Configuration > New Windows agent configuration > Security and Compliance > Agent Watcher**) 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.
Agent Watcher help

This section contains the following help topics that describe Agent Watcher dialog boxes.

**About the Setting list dialog box**

Use this dialog box 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 box contains the following options:

- **New**: Opens the settings dialog box where you can configure the options.
- **Edit**: Opens the settings dialog box 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.
- **Use selected**: Closes the dialog box and makes the selected setting the default for that agent configuration.
- **Close**: Closes the dialog box, without applying any settings to the task.

### About the Agent Watcher settings dialog box

Use this dialog box to create and edit 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 box 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 select 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 the Agent Watcher settings.
- **Monitor these files**: Specifies which critical files will be monitored with the Agent Watcher settings.
- **Polling interval**: Specifies how often you want Agent Watcher to monitor the selected services and files. The minimum value 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 have been modified during that time span, the new settings are 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.

**IMPORTANT: 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
About the Update Agent Watcher settings dialog box

Use this dialog box 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, select the **Use Agent Watcher** check box, 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 box.

With the Update Agent Watcher Settings dialog box you can also deactivate the Agent Watcher by clearing the **Use Agent Watcher** check box and clicking **OK**.

This dialog box contains the following options:

- **Use Agent watcher**: Enables the Agent watcher service on target devices.
- **Choose an Agent Watcher setting**: Specifies which setting is used for the task. Select one of the settings from the list, or click **Configure** to create new settings.

Once the **OK** button is selected, all the selected devices are updated with the new settings, and a status message appears.
Inventory

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 Endpoint Manager 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 Windows scanner executable is named ldiscn32.exe.

There are two types of inventory scans:

- **Hardware scan**: Scans hardware data 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**: Scans software installed 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, right-clicking it, 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" (330).

Optimizing inventory scanning

The following information describes some of the options available for optimizing your inventory scans.
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 Ivanti Software Services applet (Configure > Services).

1. Delete the invdelta.dat file from the device. 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 > Ivanti 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 > Ivanti > Ivanti 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 (ldiscn32.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

By default, inventory scans are encrypted (TCP/IP scans only). You can disable inventory scan encryption by changing a setting in the Configure Ivanti Software Services applet (Configure > Services).

1. At the core server, click Start > All Programs > Ivanti > Ivanti 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 the 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 inventory data are stored in the core database, and include hardware, device driver, software, memory, and environment information. You can use this inventory data to help manage and configure devices, and to quickly identify system problems.

You can view inventory data either as a summary or as a full device inventory. You can also view inventory data in reports that you generate. For more information, see "Using reports" (381).

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 before you can see its inventory.

To view summary inventory

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

Show/Hide image
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. The search field searches text in both panes, including values. The search isn't case-sensitive and you can use F3 to go to the next occurrence.

To view a full inventory

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

Show/Hide image
For detailed information, see "Inventory help" (342).

**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 box" (344).

**Tracking inventory changes**

Ivanti can detect and record changes in 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.

**Show/Hide image**
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:

- "Configure inventory change settings" (331)
- "Viewing, printing, or exporting inventory changes" (333)

**Configure 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. Select the appropriate check 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 box" (345).
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 box" (345).

Viewing a device's inventory change log

When the inventory scanner runs it creates a delta file containing changes from the last scan. The scanner sends this delta file to the core server. The scanner also uses this delta file to create a change log on each managed device. The change log is in XML format and is stored on the managed device in the LDCClient\Data\changeslog.xml file.

The change log stays on the device. If you want to see it, you'll need to remote into the device to access the changeslog.xml file directly.

By default the changes log stores 90 days of data. You can change this in the inventory agent settings.

To change the logged data period

1. Click Tools > Configuration > Agent Settings.
2. Under Inventory settings, double-click the inventory setting you want to change.
3. Click Scanner settings, and set the Change history storage (days) option to the value you want.
4. Click Save.

The changes log stores this information:

- Last hardware scan date
- Memory - Physical - Bytes available
- Memory - Page file - Available
- Last software scan date
- OS - NT info - Last boot up time
- OS - Last start up time
- Processor - Speed
- Scheduled task - Last run
- Scheduled task - Next run
• Mass storage - Logical drive - Available storage
• OS - Drivers and services - Service*

Here’s a sample logged change:

```xml
<inventorychanges>
  <changes timestamp="2014-04-30T09:43:08-7:00">
    <change newvalue="255.255.224.000"/>
  </changes>
</inventorychanges>
```

**Agentless inventory scanner**

The self-electing subnet service (SESS) agentless inventory scanner is new to Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk 2016.3. When enabled on a subnet (it's disabled by default), the SESS-elected device uses credentials an administrator provides to attempt full inventory scans on unmanaged and Ivanti-agentless devices found by extended device discovery (XDD). By default the elected device attempts these scans for unmanaged devices on its subnet once per day.

The agentless scanner does this by periodically getting a list of unmanaged devices from the core server. The elected device remotely uses credentials an administrator provides to map a drive to an unmanaged device's C$ share. The credentials provided should ideally be domain administrator credentials. By default Windows typically disables C$ share access to local accounts.

If the mapping is successful, the elected device copies scanner files to a temporary folder, C:\Landesk_AGLS\scanner. From there the scanner runs and reports results to the elected device, which uploads the scan to the core server. After the scanner finishes, the elected device removes the files and folder it copied, leaving behind the scan file or error file in C:\Landesk_AGLS.

When the agentless inventory scanner runs successfully on a device, that device is moved from the Unmanaged devices database table to the Computers table. You can view agentless devices in the Network view under Devices > Agentless devices. Devices in the Agentless devices view will still be scanned by the agentless inventory scanner once a day if you haven’t changed the default scan frequency.

Use the dashboard editor tool to create charts that monitor device discovery. These charts include information on agentless scan status, new agentless devices scanned, and unmanaged devices discovered. For more information, see “Dashboard editor” (398).

Follow these steps to enable the agentless inventory scanner on a subnet.

**1. Enable the agentless inventory scanner in an agent setting**

   1. Click Tools > Configuration > Agent settings.
2. In the Agent settings tree, click Client connectivity and double-click an existing agent setting or right-click and create a new one.

3. In the agent setting, click Self-electing subnet services > Agentless scanner service.

4. Select Enable agentless scanner service.

5. Click Save.

6. In the Agent settings toolbar, click Create a task > Change settings.

7. On the Change settings page, select the client connectivity setting you modified.

8. Click Save.

9. Add targets to the new change settings task and run it. You can target multiple (or all) devices on a subnet and let SESS manage which device runs the agentless scanner service on that subnet.

2. Enable extended device discovery

The agentless inventory scanner relies on XDD for a list of unmanaged devices that should be scanned. XDD is enabled by default in version 2016.0 and newer.

1. Click Tools > Configuration > Self-electing subnet services.

2. In the tree select Extended device discovery (ARP).

3. Right-click the subnet you want to modify and click Enable.

4. The default polling interval is 15 minutes and it may take that long for the change to propagate.

3. Enter credentials that the scanner should use

These credentials are for Windows devices. Macs aren't supported yet.

1. Click Tools > Configuration > Self-electing subnet services.

2. On the toolbar click the Manage credentials button.

3. Click Add.

4. Enter the credentials and click Save. Credentials will be attempted in the order they appear in the list. Put the most likely credentials at the top of the list for efficiency. Use the arrows to reorder credentials if necessary.

5. Repeat as necessary and click Save when you're done.

4. Enable the agentless scanner on a subnet

1. Click Tools > Configuration > Self-electing subnet services.

2. In the tree select Agentless scanner service.

3. Right-click the subnet you want to modify and click Enable.

4. The default polling interval is 15 minutes and it may take that long for the change to propagate.
Configure agentless scanner behavior on a subnet

If you just enabled the agentless scanner service on devices, it may take a while for the subnet to appear in the self-electing subnet services tree.

1. Click **Tools > Configuration > Self-electing subnet services**.
2. In the tree select **Agentless scanner service**.
3. Right-click the subnet you want to modify and click **Service settings**. The settings apply only to the subnet you selected.
4. Set the polling and scan frequency you want. The polling frequency is how often an elected scanner asks the core for an updated list of new unmanaged devices on the subnet.
5. Change other settings if necessary.
6. Click **Save**.

Viewing application and OS crash data

The inventory scanner now retrieves application crash data from managed Windows devices. This data comes from the Windows event logs. You can view this information in the device inventory under Diagnostic Data.

- Date and time of the last crash
- Application name, version, and date
- Module name, version, and date
- Last exception code
- 30-day count of crashes for this application
- 90-day count of crashes for this application

OS crash data comes from Windows minidumps. Minidumps must be enabled for this to work. This data includes:

- Last crash date
- 30-day count
- 90-day count

Additional inventory tasks and troubleshooting

This topic provides additional information about inventory scanning, as well as some troubleshooting tips. It includes the following information:

- "Launching the inventory scanner" (337)
- "Scheduling an inventory scan task" (337)
- "Scanning standalone devices" (337)
- "Adding inventory records to the core database" (338)
"Creating MIF files" (338)
"Scanning for custom data on Macintosh devices" (338)
"Troubleshooting the inventory scanner" (342)

**Launching the inventory scanner**

Launching LDISCN32.EXE directly with no parameters triggers a default command line that is the equivalent of:

```
LDISCN32.EXE /NTT={server} /S={server} /I=HTTP://{server}/ldlogon/ldappl3.ldz
```

To disable the default command line above, use /L-

To scan only to an output file use the following:

```
LDISCN32.EXE /L- /v /o=output.txt
```

**Scheduling an inventory scan task**

If a device is running the Endpoint Manager agents, you can schedule a script that triggers an inventory scan on the device.

**To schedule an inventory scan**

1. Click **Tools > Distribution > Scheduled tasks**.
2. On the toolbar, click the **Schedule inventory scan** button.
3. 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.

**Scanning standalone devices**

**To scan a standalone device**

1. Copy the inventory scanner utility, a software description file (usually LdAppl3.ini), and the following files to a thumb drive or other accessible location: ldiscn32.exe, elogapi.dll, loc32vc0.dll, and processrunner.dll.
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 appears in the Description field in the core database. For example:

```
LDISCN32.EXE /F /V /L- /O=c:\\computername%.scn
```
4. Copy the resulting scan file to the core server's `..\ManagementSuite\dscan` folder so it gets added to the database.
To scan a device that has network access to the core server

1. Map a drive (N: for instance) to the Idlogon directory of the core server you want the scan to show up in.
2. Click **Start > Run** and paste in this command after substituting your core server name where necessary:

   N:\LDISCN32.EXE /NTT=CORESERVERNAME:5007 /S="CORESERVERNAME" /I=HTTP://CORESERVERNAME/ldlogon/ldappl3.ldz /F /V /L- /SYNC

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.

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 for custom data on Macintosh devices

You can gather custom data from devices running the Ivanti 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 [https://community.landesk.com/support/docs/DOC-1570](https://community.landesk.com/support/docs/DOC-1570).

**NOTE:** The implementation of custom data with the Ivanti agent for Macintosh doesn’t use custom data forms. Custom data form tasks can’t be deployed successfully to devices running the Ivanti agent for Macintosh.
Custom data XML file

Before you can add custom data to an inventory scan from a device running the Ivanti 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
  <?xml version="1.0" encoding="UTF-8"?>
  ```
- All start tags within a custom data XML file must have a corresponding end tag. For example:
  ```xml
  <Home>(123) 456-7890</Home>
  ```
- All tags within a custom data XML file must not have spaces. For example:
  ```xml
  <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:
  ```xml
  <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:
  ```xml
  <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:
  ```xml
  <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
<?xml version="1.0" encoding="UTF-8"?>
<Phone_Numbers>
  <Work>(123) 456-7890</Work>
  <Mobile>(123) 456-7890</Mobile>
  <Home>(123) 456-7890</Home>
  <Other>N/A</Other>
  <Preference>Work</Preference>
</Phone_Numbers>
```
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
<?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>
```
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 Ivanti 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 Idscan: 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 Idscan: 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 Ivanti 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.

**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.

**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.

**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**.

**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 computer's 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.

- **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 Ivanti 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.

- **Ivanti Management**: Information about the Ivanti agents. 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.

- **Modems**: Modem information including manufacturer, model, number, and port.

- **Motherboard**: Motherboard information including bus speed and slot information.

- **Mouse**: Type of mouse attached to the device. Mouse type values include PS/2, serial, and infrared.

- **Multimedia files**: Number of files with extensions that match common multimedia file types (jpg, .mp3, and so on) and how much space those files are using.

- **Network**: Network adapter, NIC address, and the adapter's node address information. The Network object includes information for each protocol.
• **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 computer’s 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.
• **System Capability**: Miscellaneous system technologies, such as ASIC capability or virtual machine software.
• **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 box**

Use this dialog box 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 box**

Use this dialog box 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. Select the Inventory option to log inventory changes in the device's Inventory changes history dialog box. Select the NT Log option to log inventory changes in the Windows NT event log. Select 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 box**

Use this dialog box to view a device's inventory changes. You can also print and export the inventory changes history from this dialog box.

- **Device Name:** Displays the name of the devices 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 box 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 box where you can print the contents of the inventory changes history.

- **Export:** Opens a Save As dialog box 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 box

Custom data forms are not supported in Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk

Custom data forms aren’t available with a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk only license. You must have a full Ivanti® Endpoint Manager powered by Landesk license in order to use the custom data forms feature.

Use this dialog box 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 box where you can create a new question for the form.
- **Edit:** Opens the Edit question dialog box 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 box

Use this dialog box 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 want 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 box

Use this dialog box 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 list.
- **Items list**: Lists all the items that appear in the question's 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 box

Use this dialog box 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 box.
- **Cancel**: Closes the dialog box without saving the group.

Adding software and data items to inventory scans

Use the Manage software list tool to configure the software and data that you want to include in inventory scans. The choices you make with this tool define what items are scanned for when the inventory scanner runs.

![Manage Software List](image)

The inventory scanner uses the data items you specify to identify software files and custom data items such as registry values, WMI data, and URLs. You can specify the following items:

- **Files**: Files that are included in software scans are included in the To be scanned list. Files in the To be excluded list are not included in software scans. Files in the To be dispositioned list have been discovered and need to be moved to one of the other lists.
- **Registry items**: The inventory scanner can identify items in the Windows registry on managed devices. These items are then displayed in the section of the inventory list that you specify.

- **WMI items**: The inventory scanner can scan for WMI (Windows Management Instrumentation) data items, with the results displayed in the section of the inventory list that you specify.

- **URLs**: The inventory scanner can scan for URLs, which is useful to track the use of Web-based applications and software as a service (SaaS).

---

**IMPORTANT**: Endpoint Manager 9.6 and later no longer use the ldap3.template file. Setup migrates the data in this file to the core database. To change settings that used to be in this file, use the Manage software list tool (Tools > Configuration > Reporting / Monitoring) or the Inventory settings agent setting (Tools > Configuration > Agent settings).

See the following topics for information about changing items included in inventory scans:

- "Add or remove files for inventory scans" (348)
- "Add custom registry items to inventory scans" (350)
- "Add custom WMI items to inventory scans" (352)
- "Add URLs to inventory scans" (354)
- "Modeling attributes" on page 355

### Making inventory scan changes available to clients

When you make changes in the Manage software list tool, you need to deploy the changes to managed devices in order to change the way inventory scans run. The changes will be applied if the /i scanner command line parameter is used on your managed devices.

**To deploy scanning changes to managed devices**

1. In the console, click **Tools > Reporting/Monitoring > Manage Software List**.
2. Make your changes.
3. 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.

### Add or remove files for inventory scans

Modify the files in the **Manage software list** tool to determine which files are included in or excluded from inventory scans.

**NOTE**: After you have changed any items in the core's Manage software list, 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.
Software files in inventory scans

The scanner recognizes software applications in three ways:

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

Use the Manage software list tree view to specify which files should be scanned and which should be excluded from inventory scanning. The Files item in the tree displays three categories that help you organize the files:

- **To be scanned**: Files that the scanner will 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**: As the inventory scanner adds software data to the database, it finds many software files that are not recognized; these files are added to this list. You can move files out of this list into either of the other two lists.

- **To be excluded**: The scanner ignores all occurrences of each file that you move here. If you delete a file from **To be excluded**, it appears in the **To be dispositioned** category.

By default, the inventory scanner only scans for files listed in the Manage software list. The files that are specified as scanned or excluded are saved in the Manage software list tool (Tools > Configuration > Reporting / Monitoring).

After the initial scan, the inventory scanner sends only delta scans, which will be much smaller.

Scan or exclude software files

Complete the following tasks to determine which software files are included in inventory scanning.

**To include a file in inventory scans**

1. Find the file by searching in the **To be dispositioned** list.
2. Drag the file to the **To be scanned** list.

**To exclude a file from inventory scans**

1. Find the file by searching in the **To be dispositioned** list.
2. Drag the file to the **To be excluded** list.

**To exclude a file that is not found in the To be dispositioned list**

1. Click **To be excluded** and then click the **Add** button on the toolbar.
2. Enter the name of the file to be excluded, and then click **OK**.
To change a file's status from scanned to excluded

1. Find the file by searching in the To be scanned list.
2. Drag the file to the To be excluded list.

You can also move files from the excluded list to the scanned list.

Scanning application files that don’t have .exe extensions

The default To be scanned list contains descriptions of executables, but only with .exe file extensions. If you want the scanner to also identify other types of application files (.dll, .com, .sys, and so on), see "Adding software and data items to inventory scans" (347).

About the File properties dialog box

Use this dialog box to add files to Manage software list. A filename is the only required field. You can expand the dialog to supply more information if necessary.

- **Filename**: Enter a filename. The field defaults to a wildcard file.
- **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.

Add custom registry items to inventory scans

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.

The Manage Software tool lets you specify registry keys to add to inventory scanning. Results are displayed in whatever section of the inventory you specify.

Several registry items are provided with Endpoint Manager. You can view the properties for these items to see an example of how to create registry items. To view an item's properties, right-click it and select Properties.
To add a registry key for inventory scanning

1. Click **Tools > Reporting/Monitoring > Manage software list**.
2. Expand **Custom Data** and click **Registry items**.
3. Click the **Add** button on the toolbar.
4. Select and enter data as described below.
5. Click **OK**.

Registry scan items include the following data:

- **Root key**: Select the type of registry key you want to scan.
  
  - HKLM = HKEY_LOCAL_MACHINE
  - HKCC = HKEY_CURRENT_CONFIG
  - HKCR = HKEY_CLASSES_ROOT
  - HKU = HKEY_USERS
  - HKCU = HKEY_CURRENT_USER

- **Key**: The path in the registry that defines the location of the key. Items must be separated with a backslash (\), and each item between backslashes represents a level in the tree hierarchy of the registry (as viewed in the registry editor).

- **Value**: The search value that the inventory scanner looks for.

- **Attribute name**: The description of where the data will be displayed in the inventory tree. Items are listed in hierarchical order and must be separated with " - " (space dash space) to accurately be displayed in the inventory. The first item you type here is the name in the inventory tree that will contain the data, such as "Custom Data".

For example, the attribute name **Custom Data - MDAC - Version** is displayed in a device's inventory summary as follows:

![Inventory tree screenshot](image-url)
NOTE: After you have changed any items in the core's Manage software list, 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.

### Add custom WMI items to inventory scans

The inventory scanner can scan for WMI (Windows Management Instrumentation) data items and add their values to the core database. This data is then displayed in the inventory summary.

Use this option if there are inventory items for Windows devices that you can't find in the standard inventory summary provided with Endpoint Manager.

To add WMI items to the inventory scan, you'll need to be familiar with the WMI classes and instances, and you'll need to know which namespace a class is part of. Use a tool like Microsoft CIM Studio or PowerShell (in Windows 7 and later) to browse the WMI classes.

For each class, you can scan for one or more properties and return those values in the inventory tree.

For example, the following is a WMI class for a media port connector. It contains three properties. The namespace, class, and inventory display path are defined in the top section of the dialog box. The properties are added individually and are all listed in the Properties box in the middle of the dialog box.
After this custom data item is defined and it has been made available to managed devices (by clicking the **Make available to clients** button on the toolbar), a managed device that has a media port connector will include this item in the inventory summary. In the inventory tree, the item is listed under **Mass Storage > Media Changer**. It will display three data items: Adapter Name, Disk Name, and Enclosure Type.

**To add a WMI item for inventory scanning**

1. Click **Tools > Reporting/Monitoring > Manage software list**.
2. Expand **Custom Data** and click **WMI items**.
3. Click the **Add** button on the toolbar.
4. Enter **Object** data as described below.
5. To add a property, click **Add**. Enter a the **Property Name** and **Display Name** as described below. Click **Apply** to add the property.
6. When all data is complete, click **OK**.

WMI items include the following data:
• **Namespace:** The WMI name space. Typically this is `root\CIMV2`, but it can be another namespace.

• **Class Name:** The WMI class name.

• **Display Object:** The description of where the data will be displayed in the inventory tree. Items are listed in hierarchical order and must be separated with " - " (space dash space) to accurately be displayed in the inventory. The first item you type here is the name in the inventory tree that will contain the data, such as "Custom Data".

Each item can have one or more properties that the scanner searches for.

• **Property Name:** The name that identifies the WMI property.

• **Display Name:** The name used in the inventory tree to identify the WMI property. This name appears one level below the Display Object in the inventory tree.

NOTE: After you have changed any items in the core's Manage software list, 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.

### Add URLs to inventory scans

The inventory scanner can scan for URLs, which is useful to track the use of Web-based applications and software as a service (SaaS). For example, if your organization uses Salesforce to track sales and customer service, you would add a monitored URL that matches the URL you use to log in to Salesforce.

For each URL you add, the inventory scanner will save data such as:

• How often the URL is visited

• The amount of time spent viewing pages at the URL

• The last date/time the URL was visited

**To add a URL for inventory scanning**

1. Click **Tools > Reporting/Monitoring > Manage software list.**
2. Click **Monitored URL Items.**
3. Click the **Add** button on the toolbar.
4. Enter a domain name in the URL box.

You can enter a domain name with subdomains, separated by dots, but you can't include specific paths. The domain name can't include invalid characters. If you enter a path or invalid characters, an error message will appear and you'll need to correct the URL.

You can include up to 10 levels of subdomains with no more than 60 characters per level. You can use a maximum of 260 characters total in the domain name.
NOTE: After you have changed any items in the core's Manage software list, 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.

Modeling attributes

One of the strengths of the inventory database is that it's automatically extendable. If the Ivanti agent on a device discovers new information, the Ivanti inventory service can add it to the database without requiring you to reconfigure anything. This process is handled by a catch-all table where unknown or "unmodeled" attributes are placed.

Unmodeled attributes can become an issue if you’re using SQL or a third-party tool to access the inventory database directly. To read the data properly for an unmodeled attribute, the database requires a 5-table join, which most people can’t create unless they’re familiar with SQL.

With the Model attributes dialog, you can “model” this data, so that it’s no longer stored in an UNMODELEDDATA1 table but rather in its own column in a table that you can easily query using an application such as Crystal Reports.

The Model attributes dialog also enables you to change the data type of an attribute. When an attribute is created via a scan file, by default it’s added as a string to the inventory database. However, you may want the attribute stored as integer for sorting and comparison purposes.

On the Tools > Reporting/Monitoring > Manage software list toolbar, click the Model Attributes button to open the dialog.
**About the Model Attributes dialog box**

**Attributes in the database in unmodeled data list box:** This list shows all components in the database that currently have unmodeled attributes. The attribute data type is also shown. Select the attribute you want modeled.

**Model for me button:** Click this button to map the unmodeled attribute to the proper table in the inventory database. The attribute will use the data type it was assigned.

After clicking the **Model for me** button, the following **New table information** will auto-populate:

- **Component:** The component in the database (for example, Computer or Computer.Memory) associated with the unmodeled attribute.
• **Table name:** The name of the table that the unmodeled-attribute data will be moved to. If the component is not part of an existing table, a name such as UNMODELEDDATA1 will appear. Change this name to something meaningful to create a new table. If the component is part of an existing table, do not change the name.

• **One-to-many class:** If the component is a one-to-many, this option is automatically selected. In this case, you'll need to add special columns to the table using your own DATAMART.XML file, not this tool. (DATAMART.XML is the file that contains all of the database table information for Endpoint Manager. It's used in conjunction with COREDBUTIL.EXE to create tables in the database.)

• **Add to existing table:** If a table already exists for this component, select this option to add a new column to it for the unmodeled-attribute data.

The resulting list shows all modeled and unmodeled attributes for the component in this particular table. Unmodeled attributes are in **bold**. Attributes that already exist as columns in the table are not in bold and cannot be edited. Click the **Model now** button to add the unmodeled attribute(s) "as is" to the specified table. You can also click the **Edit** button to modify an attribute's values, or click the **Add** button to add other attributes to the table as well.

The attributes list shows these columns:

• **Attribute:** The name of the attribute as it will appear in the Endpoint Manager console.

• **Column:** The name of the column that will be created in the table.

• **Data Type:** The DBMS data type of the new column.

• **Size:** The length of the new column, in characters.

• **Mask:** A read-only column in this list, which shows a display mask that modifies how the data appears.

• **Key:** A read-only column in this list. For one-to-many attributes, one field must be set as the key.

**Move existing data:** In the case of an UNMODELEDDATA1 table, this option moves the data to the new table you specified. The data will then be deleted from the UNMODELEDDATA1 table.

**Model now button:** Updates the table with the changes you specified.

**Clear all button:** Clears all of the information for one component so that you can choose another one with attributes to model.

### Changing inventory scan parameters

This topic describes different ways to change the parameters of inventory scans. It includes the following information:

• "Scanning custom information" (358)

• "Specifying the software scanning interval and history" (358)

• "Scanner command-line parameters" (358)
Scanning custom information

The Windows inventory scanner utility 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

NOTE: Custom field subkeys
The inventory scanner doesn’t scan for any subkeys below Custom fields.

NOTE: 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.

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.

NOTE: The core server and software scanning
This feature affects only devices. It doesn’t affect the core server, which is always scanned daily.

Scanner command-line parameters

You can add command-line parameters to the inventory scanner’s (ldiscn32.exe) shortcut properties to control how it functions.

Running ldiscn32 /? shows the scanner’s command-line parameters:
Managing software list settings

The Manage software list tool (Tools > Reporting / Monitoring > Manage software list) has a settings branch where you can adjust inventory scan behavior.

If you used Endpoint Manager before version 9.6, you may recognize many of these settings from the ldappl3.template file. Endpoint Manager 9.6 moved the settings in that file to the database, and the Manage software list is where you can change them now.

CfgFiles

Add text files that you want the inventory scanner to gather from managed devices and store in the database. Starting the text file path with a backslash makes the inventory scanner look at each local drive for the file. If you only want a specific drive searched, include the drive letter in the path.

These files will be visible in the device inventory under Configuration files, which as at the inventory tree root. The scanner also gathers the file date, size, and path. Double-clicking File data shows the Attribute properties dialog box, and clicking the Extended value tab shows the file contents.

Text file contents aren’t queryable.
DataFileExtensions

DataFileExtensions lists the extensions that will be scanned for inclusion in a computer software report. This information can be found under the Software.Data Files database attribute and will include the file name, path, file date, and file size.

ScanExtensions

ScanExtensions lists the extensions that will be searched for. Regardless of what is entered in the Applications section, if the extension of the file is not listed here, the application will not be found.

MultimediaExtensions

MultimediaExtensions lists the extensions that will be scanned for inclusion in a computer software report. This information can be found under the Multimedia database attribute and will include the total number of multimedia file, the extensions found and how much dispsace is being used for multimedia files.

Ignored MACs

Ignored MACs is a space delimited list of up to 40 MAC addresses that the scanner should not consider as a candidate when choosing an address to be used for identification. This is the address assigned to "Network - NIC Address" and is used on the core to identify duplicate device ID's. The addresses in this list must match EXACTLY with addresses found in the "Bound Adapter" section of a scan file. For this reason, it is best to copy these addresses from a scan file.

A typical address to ignore is the one that is consistent between machines for VPN client.

This example is for a 64 bit Cisco VPN client

Ignored MACs=00059A3C7a00

Usage Files

If the Usage files list is blank (the default), usage data will be sent for all monitored products. If you add files to this list, usage data will only be reported for those files.

MacScanExtensions

MacScanExtensions is a list of extensions gathered by inventory. If the file extension is not in this list, the file is not found, no matter what is in the Applications section.

MacMultimediaExtensions

MacMultimediaExtensions lists the extensions that will be scanned for inclusion in a macintosh computer software report. This differs from the previous section as this is specific for the Apple OS X platform. Note: Extensions are case-sensitve and will not be collected if the correct case is not used.

MacSearchFolders

MacSearchFolders is a list of additional folders to scan on Macs.
The scanner searches the /Library/Applications/System/User folders by default. The scanner only searches folders listed in the MacSearchFolders section for files specified in MacScanExtensions section. Note that this only affects the MacScanExtension section and will not affect the scanning of Applications.

Example: MacSearchFolders=/johndoe

**MIFPATH**

MIFPATH is the directory that the scanners will look in to find MIF files.

MIFPATH=C:\DM\DOS\MIFS

**Exclude Folders**

Excludes folders from being scanned. These folders are already included by default:

- ExcludeDir=\recycled\n- ExcludeDir=\recycler\n- ExcludeDir=%USERPROFILE%\LOCAL SETTINGS\TEMP\n- ExcludeDir=%USERPROFILE%\LOCAL SETTINGS\TEMPORARY INTERNET FILES\n- ExcludeDir=%USERPROFILE%\Application Data\Thinstall\n- ExcludeDir=%windir%\$ntservicepackuninstall$\n- ExcludeDir=%windir%\installer\n- ExcludeDir=%windir%\lastgood*\n- ExcludeDir=%windir%\driver cache\n- ExcludeDir=%windir%\registeredpackages\n- ExcludeDir=%windir%\temp\n- ExcludeDir=%windir%\system32\dllcache\n- ExcludeDir=%windir%\$NtUninstall*\n- ExcludeDir=%windir%\ServicePackFiles\i386\n- ExcludeDir=%windir%\i386\n- ExcludeDir=\i386\n- ExcludeDir=\$LDCFG$\n- ExcludeDir=\SYSTEM VOLUME INFORMATION\n- ExcludeDir=\SP3\n- ExcludeDir=\SP4\n- ExcludeDir=\Library\n- ExcludeDir=\DOCUMENTS AND SETTINGS\LOCALSERVICE\LOCAL SETTINGS\TEMP\n- ExcludeDir=\DOCUMENTS AND SETTINGS\LOCALSERVICE\LOCAL SETTINGS\TEMPORARY INTERNET FILES\n- ExcludeDir=%ProgramFiles%\landesk\ldclient\bkupcfg\n

- ExcludeDir=%ProgramFiles%\landesk\ldclient\cache\n- ExcludeDir=%ProgramFiles%\landesk\ldclient\data\n- ExcludeDir=%ProgramFiles%\landesk\ldclient\sdmcache\n- ExcludeDir=%ProgramFiles%\LANDESK\SHARED FILES\n- ExcludeDir=%ProgramFiles%\COMMON FILES\MICROSOFT SHARED\n- ExcludeDir=\LDClient\Temp\n- ExcludeDir=\LDCLIENT\SDMCACHE\n
**SMBIOS Ignore**

Include strings in this section that you want inventory to ignore from the SMBIOS scanner. The four values shown in the example below are included by default and are not necessary to include again.

- Unknown
- N/A
- Not Available
- None

**Using custom data forms**

Ivanti 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.

**Show/Hide image**

![User computer information form](image)

**NOTE:** Custom data forms aren’t supported in Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk

Custom data forms aren’t available with a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk only license. You must have a full Ivanti® Endpoint Manager powered by Landesk license in order to use the custom data forms feature.

The inventory scanner can’t gather certain types of personalized user-specific information, such as:
• Location of a user's desk
• Asset number of a computer
• 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.

**NOTE:** 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.

### Create a custom data form

Custom data forms provide a way for you to collect information from users and add it to the core database. 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. (The description you enter will appear as a help tip when the user clicks F1 on the field while filling out the form.)
5. Click **Add** to open the **Add question** dialog box.
6. In the Add Question dialog box, type in the **Question text**, **Inventory name**, and **Description**.
7. Select the **Control type**.
8. Select 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.

Show/Hide image

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.

Create 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.
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*.

**Show/Hide image**

Once you have created a group of forms, you can right-click on the group 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 choose 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” (127).

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 Ivanti program folder**: The form viewer can be launched manually from the Endpoint Manager 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

**IMPORTANT:** You can schedule custom data forms (or form groups) for deployment to devices using the Scheduled tasks tool ([Tools > Distribution > Scheduled Tasks](#)). Before forms will display on the device, you will also need to enable display of forms in the Agent Configuration tool ([Tools > Configuration > Agent Configuration > (double-click the applicable configuration in the list) > Custom data forms > select the display option you want to use](#)).

When the custom data 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.

**Show/Hide image**
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.
Queries/Directory manager

Database queries

Queries are customized searches for managed devices. Ivanti® Endpoint Manager powered by Landesk 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.

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 the My queries group and selecting New query or New group, respectively.

A Ivanti® Endpoint Manager powered by Landesk administrator (user with Endpoint Manager Administrator rights) can view the contents of all of the query groups, including My queries, Public queries, and All queries.

When other Endpoint Manager 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.

Create a database query

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.

Run a database query

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.

Import and export queries

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

- Endpoint Manager 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 querying the core database, Endpoint Manager also provides the directory 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” (369).

**Configure LDAP directories**

Use the **Active directory source** dialog box to manage the LDAP directories you use with Ivanti® Endpoint Manager powered by Landesk. 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 this dialog box.

> **NOTE:** The account you configure in directory manager must be able to read the users, computers and groups that you use for management with Endpoint Manager.

**To configure a new directory**

1. Click **Configure > Manage Active Directory sources**.
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 box closes.

**To modify an existing directory configuration**

1. Click **Configure > Manage Active Directory sources**.
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 box closes

To delete an existing directory configuration
1. Click Configure > Manage Active Directory sources.
2. Click the directory you want.
3. Click Delete.

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

Create an LDAP 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. From the Network view, click Directory > (your configured active directory) > Browse directory.
2. Right-click an object in the LDAP directory and click New query. You’ll create an LDAP query that returns results from this point in the directory tree down.
3. The Basic LDAP query dialog box appears.

To create, test, and save the query
1. From the Basic LDAP query dialog box, 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.
Auditing

Welcome to auditing

The auditing tool audits console user activity and stores the auditing information in the core database and optionally the Windows event log.

The auditing tool isn’t enabled or visible by default. Before you can use auditing, you must give a user auditing configuration rights and then configure what activities you want audited.

If you haven’t configured auditing, only auditing configuration changes are audited, such as giving or removing auditing rights.

For more information, see these additional topics:

- “Configuring auditing” (373)
- "Sending auditing events to the Windows Event Viewer" (376)
- "Viewing auditing events" (378)
- "Creating filters for auditing event queries" (379)

Configuring auditing

The auditing tool isn’t enabled or visible by default. Before you can see the auditing tool or make auditing configuration changes, an administrator must give you the auditor or auditing configuration role.

There are two auditing roles:

- **Auditing configuration**: Users with this role can configure what gets audited. This role also includes the auditor role rights, so users with this role can also see the auditing tool and view auditing data.
- **Auditor**: Users with this role can view auditing data and create auditing custom queries, but they can’t change what gets audited.

There are three main steps to configuring auditing:
1. Give a user the auditing configuration role
2. Configure what gets audited
3. Assign the auditor role to additional users if necessary

**To give a user the auditing configuration role**

1. Click **Tools > Administration > User management**.
2. In the **Roles** tree, double-click **Auditing configuration**.
3. On the **Users and groups** page, select users that will have the auditing configuration role.
4. Click **OK**.
5. Have the console user that you gave the auditing role restart their console so that they can see the auditing tool. A user's rights and roles are loaded once when the console starts, making a console restart necessary.
To configure what you want to audit

1. Click **Tools > Configure services**.

2. In the **Configure Ivanti software services** dialog box, click the **Auditing configuration** tab. If you don’t see this tab, make sure you have the auditing configuration role and that you’ve restarted the console after being assigned that role.

3. Select the console features or sub-features that you want to audit.
4. Click OK.

5. Click Tools > Administration > Auditing to view the auditing data.

NOTE: It can take up to two minutes for changes to the Write auditing events to the event log option to take effect. You can restart the console if you don’t want to wait.

To assign the auditor roles to other users

1. Click Tools > Administration > User management.
2. In the Roles tree, double-click Auditor.
3. On the Users and groups page, select the users that will have the auditor role.
4. Click OK.
5. Have those users restart their consoles so that they can see the auditing tool.

Sending auditing events to the Windows Event Viewer

Ivanti® Endpoint Manager powered by Landesk stores auditing events in the core database. You can also optionally send auditing events to the Windows Event Viewer application. Note that any user with rights to view the Event Viewer will then be able to see auditing log entries. If this is a security issue in your environment, consider securing the Event Viewer auditing log entries or not enabling this option.

Endpoint Manager logs auditing events to this Windows Event Viewer path:

- Applications and Service Logs > LANDESK Software > LANDeskAuditing
To send auditing events to the Windows Event Viewer

1. Click Tools > Configure services.
2. In the Configure LANDesk software services dialog box, click the Auditing configuration tab and select Write auditing events to the event log. If you don’t see this tab, make sure you have the auditing configuration role and that you’ve restarted the console after being assigned that role. When you enable this option, you’ll see a DOS box briefly flash. This is normal.
3. Click OK.

Enabling Event Viewer logging only affects events that happen after you enable it.

NOTE: It can take up to two minutes for changes to the Write auditing events to the event log option to take effect. You can restart the console if you don’t want to wait.
Viewing auditing events

Auditing events are stored in the core database in XML format. When you double-click an auditing event to view it, you see the logged XML items associated with that event. The items logged depend on the auditing event.

The default auditing event queries cover these time periods:

- Last 30 days
- Last 7 days
- Last day

To view auditing events with the default queries

1. Click **Tools > Administration > Auditing**.
2. In the **Default queries** tree, click the query you want.

You can also create custom filters for the auditing queries. For more information, see "Creating filters for auditing event queries" (379).
Identifying what changed in an auditing event

Some auditing events can involve many changes, such as those involving agent setting changes. In these cases, it can be hard to identify in the XML what changed in the audited event.

To help with this, the auditing tool includes support for a diff tool of your choice that you can use to compare an audited event XML file with the event’s state before it was changed.

To configure auditing diff tool support

1. Click Tools > Administration > Auditing.
2. In the auditing toolbar, click the Enter diff tool configuration button.
3. Enter the Compare tool path to your diff tool executable.
4. Customize the command line for your diff tool if necessary. %1 is the selected auditing event’s original XML data and %2 is the selected auditing event’s current XML data. You must include both the %1 and %2 parameters for the diff to work.
5. Click the Save button.

To view auditing event XML data differences

1. Double click the auditing event you want to check for differences.
2. In the Audit entry detail dialog box, click the Differences button.
3. View the differences in the diff tool you configured.

Creating filters for auditing event queries

The auditing event history appears inside the auditing tool (Tools > Administration > Auditing). You must have either the Auditing configuration role or the Auditor role to see this tool in the console.

You can create filters for custom auditing queries. You can choose from these auditing event filters:

- **Username**: Show auditing events for the specified username.
- **Device name**: Show auditing events for the specified device name.
- **Modified date**: Show auditing events between the specified date range or within the last number of days specified.
- **Features**: Show auditing events for the selected features. You must select **Features** before you can expand the **Events** tree.

If you select multiple filters they will be query AND options. For example, if you select a username and a feature, the results will only show devices matching both that username and that feature.

**To create a custom auditing query**

1. Click **Tools > Administration > Auditing**.
2. Click the **Custom queries** tree item.
3. Click the **New query definition** toolbar button.
4. Modify the filters you want.
5. When you’re done click **Create**.

**Archiving and restoring auditing data**

The auditing tool lets you archive and restore auditing data.

- **Archive**: In archive mode, the tool saves auditing data to the file you specify. You specify the number of months of data (beginning now) to leave in the database and the filename. All data outside of that time period will be saved to the file and removed from the database.

- **Restore**: In restore mode, the tool reinserts previously archived data from the file you specify into the database. The default timeout and batch size is 500 seconds and 200,000 records. Use these defaults as a baseline if you need to adjust either parameter. No auditing data will be inserted if the database insertion times out.

**To archive auditing data**

1. Click **Tools > Administration > Auditing**.
2. In the Auditing window toolbar, click the **Archive data** or **Restore from archived file** buttons.
3. Enter your preferences and depending on the mode you chose, click **Archive** or **Restore**.
Reports

Using reports

The reporting tool can be used to generate detailed reports that provide critical information about the devices on your network. This tool takes advantage of the Endpoint Manager inventory scanning utility, which collects and organizes hardware and software data, in order to produce useful, up-to-date reports.

Several types of reports are available:

- **Standard (predefined) reports:** Default reports that ship with Endpoint Manager.
- **Custom reports:** Custom reports that define a unique set of information to generate a report. You can also customize any of the standard reports using the integrated Data Dynamics report designer.
- **Ad hoc reports:** Automatically generated reports available from various areas of Endpoint Manager. For example, you can right-click a query and click New report to generate a report based on the query.

You can schedule reports so they run at a regular interval. Scheduled reports can be published and saved to a secure file share location on the core server, where anyone with proper login credentials can access and view the reports. You can also schedule the published reports to be e-mailed to designated recipients.

**To launch the reporting tool**

Click Tools > Reporting / Monitoring > Reports.

**To use reports in the Web console**

Click Reports under the Reporting group.

**Report groups**

Open the Reports tool to access predefined reports.
Reports are organized with a tree structure, grouped in the following folders:

- **My reports**: Reports that the current user has created or copied from another folder. These are typically reports that you run on a regular basis and have organized for your own use. You can organize reports in folders that you create. An administrator has access to each user's reports groups and can add and remove reports.

- **Standard reports**: Predefined reports that are installed with Endpoint Manager. The reports are preformatted, have query properties and chart types assigned, and are ready to be used.

- **Public reports**: Custom reports that are made available to all users on the core server.

- **All reports**: All reports that can be used by the current user. This view includes a Find box that filters the list of reports when you type a search string and select a column. (For example, type "license" and select the "Description" column to view reports related to software licenses.)

Administrators can view the contents of all of the report groups. Users with the Reports right can also see and run reports, as well as publish reports, but only on the devices included in their scope. Users with the Report designer right can create custom reports.

Reports are run against the currently logged-in user's scope and rights. If a user doesn't have permissions to use a tool, that user can't run reports that include that tool. Similarly, the only devices that appear in a report are those included in a user's scope.

**Report sources**

Predefined reports gather data from the Endpoint Manager database. If you create a custom report, you can specify other available data sources to be included in the report.
Report formats

When running a report, you can save the report using one of the following formats:

- **HTML**: Standard HTML. You can click charts in HTML reports to view detailed information about an item.
- **Image**: Bitmap image file
- **PDF**: Adobe PDF file
- **XML**: Text file in XML format
- **DOC**: Microsoft Word
- **XLS**: Microsoft Excel

When you schedule a report in the Reports tool, you can use the following formats:

- **PDF**: Adobe PDF file
- **XLS**: Microsoft Excel
- **DOC**: Microsoft Word
- **CSV**: Comma-separated value text file

Additional resources for reports

For more information on using Endpoint Manager and Security reports, go to the Ivanti User Community reporting portal at https://community.landesk.com/community/systems/reporting. The reporting portal contains additional documentation, customer questions, and reports you can download. Any Ivanti user can submit a custom report to share with the community.

To quickly open the Ivanti User Community reporting portal, you can also click Tools > Reporting/Monitoring > Community reports.

Required rights for using reports

Not all users can view, edit, and deploy reports. Users must have the correct rights assigned in Role-based administration. Because report editing involves accessing the database, any user with Edit rights must be qualified to edit the database. You can also set up user credentials with read-only database rights if there are users that you want to run reports but not edit them.

Role-based administration and reports

Role-based administration includes Reporting rights that determine which users can view, run, modify, schedule, and create reports. In the User management tool, when you create or edit a role you can enable or disable the following reporting permissions.
### User database rights for reports

The report designer is a powerful tool that should be used with discretion. Users who have Edit rights for the report designer can access any portion of the database and can execute any SQL commands on that data, so you should make sure users with this right are qualified to manage the database. Data could be lost or corrupted if a user executes SQL commands that modify data.

The Reports tool accesses the database with the user credentials that were specified during product setup. These credentials can be managed in the **Configure Ivanti software services** dialog box (Configure > Services, General tab). If you prefer to set up different credentials for the users who have reports rights, you can create a second set of credentials for reporting database access.

For example, if you want report users to have read-only access to the database, you can create a database user account with read-only access. You would then enter that user account as the Reporting database user in the **Configure Ivanti software services** dialog box.

```
NOTE: If you're using an Oracle database and create a read-only reporting user, you'll need to create a public synonym for every table that will be referenced in reports by that user.
```

### Related topics

"Create a user with reports rights" (385)
Create a user with reports rights

The Reports tool accesses the database with the user credentials that were specified during product setup. If you prefer to set up different credentials for the users who have reports rights, you can create a second set of credentials for reporting database access.

To specify database user credentials for reporting

1. Create a user account for your database, assigning it the rights you want to use.
2. In the Endpoint Manager console, click Configure > Services.
3. Under Reporting database user, enter the user name and password for that account.
4. Click OK.

Creating custom reports

The reports tool includes an integrated Data Dynamics report designer that gives you full control over all aspects of reports. In the designer you use page layout elements linked to data objects to display the selected data. You can customize the report appearance, the underlying SQL query statements, the parameters available to users, and so on.

You can create or modify a report by doing one of the following:

- Copy a standard report, paste it into My reports, and edit it.
- Create a query in Endpoint Manager and use that query as the basis for a report.
- Create a completely new report using data sources, parameters, SQL expressions, page layout elements and images.

Report properties

When you create or edit a report, you first specify the report properties.
- **Title:** Type a descriptive title for the report.
- **Description:** Add any other descriptive information for the report.
- **Load from LDMS query:** Select a Endpoint Manager query and use it as the basis for a new report.
- **Chart type:** Select a chart style (pie or bar).
- **Query field:** Specify which field in the report is represented in the chart.
- **Report designer:** Open the report designer application to make detailed changes to the report data and layout. (If this button is dimmed, the user doesn’t have Report Designer rights.)
- **Preview:** View the report with the options you have selected in this dialog box.
If you have copied a standard report, you might simply change items in the Properties dialog box and save the new report. But it’s more likely that you’ll want to open the report designer and make more substantial changes.

**Report designer**

From the report properties dialog box you can open the report designer. This is a separate application, Data Dynamics Reports, that is integrated with the Reports tool and the database.

**NOTE:** To open the report designer a user must have the Report designer - Edit right.

The report designer gives you full access to all aspects of a report.

- **Page layout:** The center of the designer displays the report’s page design. Click the **Preview** button below the layout to open the report viewer and see how the report will look when you run it.
- **Toolbox:** Drag a tool onto the page layout to place the object.
- **Document outline:** View a content outline of the report in the left column (in place of the toolbox).
- **Data sources**: Specify the data sources you want to use when running the report. Define the source of the data and then add data sets (queries) and parameters that you will use in the report.
- **Parameters**: Define parameters that determine report results.
- **Properties**: The right column displays editable properties for the selected object.
- **Wizard**: Click **Open Wizard** to view all properties for the selected object, organized by option type.

**Basics of creating and editing reports**

The report designer is a flexible and feature-rich tool that gives you options for querying and displaying data from a variety of sources. When you create a report, you need the following basic items:

- A data source and defined data sets from which the report is populated
- A page layout to visually display the data
- Data regions and other report items that format the data

**Data sources and data sets**

Reports extract information from the *data source*, a database using a standard format such as SQL, ODBC, Oracle, or XML. In combination with the data source, you define the *data sets*, queries that are referenced in the report. The data explorer on the left side of the designer shows data sources and data sets in a tree view. In the example below, LDMS is the data source (the Endpoint Manager database) and Windows Devices is a data set. Name and Version are names of fields (database tables) referenced in the data set query.
The Endpoint Manager database appears as a default data source when you create a new report. You can add any other source by specifying a data type, a connection string, and any credentials needed to access the data. This allows data to be extracted not only from the Endpoint Manager database but any other source as well when you create a custom report.

Parameters pass information between data sets. In the report viewer, parameters can be displayed to let the user narrow down the selection of data displayed.

Adding data elements

The report designer includes wizards to help you link to data sources and define data sets and parameters. For example, when you click on a data source (such as LDMS), click the Add button and select Data Set.

The DataSet wizard is displayed with properties organized in six groups.
On the Query page of the wizard, for example, you can add a SQL query. Click the green check mark to check syntax, and click the function symbol (fx) to open the expression editor.
The expression editor lists all fields available for the selected element and lets you insert these items, such as parameters and fields from data sets, into an expression. In addition to the fields related to your data sets, there are commonly used values that are defined globally, and standard operators and functions you can insert into an expression.

After you have added at least one data set, you can define parameters based on your data sets. When a user runs a report, the parameters you add are displayed in the report viewer so the user can select which data will be displayed in the report.

In the following example, the **Suites** data set has been created, and it references the **product** table with fields **product_idn**, **title**, and **version**. A parameter called **Suite** is created. On the **General** page of the dialog box, the name is added and a prompt text (Select a suite) is specified. This is the prompt that users will see in the report viewer. On the **Available values** page, values from the query are specified. The value field is **product_idn** (a unique identifying number from the database) and the label field is **title**, which means the title (name) of the suite is displayed for the user.
When the report is run, this parameter appears to the user with a list that allows selection of a suite product:

The third page in the Parameters dialog box lets you specify a default selection for the parameter.

**Representing parameter selections in a query**

When you allow users to select a parameter, you can refer to that selection in a query by using a SQL statement unique to the Data Dynamics report editor: "in (?)". This statement uses the currently selected parameter value as it runs the report. One example of this is shown in the following code sample.
The following query uses fields from the `product` table and the `slm_productsuiteref` table to select products that are included in a product suite. In this case, a single product suite is included, identified by its ID number (615).

```
select p.product_idn, p.title, p.version from slm_productsuiteref r
left outer join product p on p.product_idn = r.product_idn where r.productsuite_idn = 615
order by p.title
```

Instead of specifying one suite, you can replace the specific product suite reference with "in (?)" to include the suite that the user selects when running the report.

```
select p.product_idn, p.title, p.version from slm_productsuiteref r
left outer join product p on p.product_idn = r.product_idn where r.productsuite_idn in (?)
order by p.title
```

You’ll find other examples of this usage in some of the standard reports that require the user to select a parameter value.

**Layout**

Report layouts define page outputs, using standard page sizes. You can specify page size, orientation, a repeated header and footer, and format for the body of the report.

Standard reports use a header with a Ivanti logo that is suppressed on page 1. The body layout begins with a larger logo which only appears once, while data below the logo fills as many pages as needed.
As you work on the page layout, you can quickly add formatting and data region elements by dragging tools from the toolbox.

![Toolbox](image)

Drag an item onto the layout, then move and resize it. Define the object in detail by using the properties pane (on the right side of the editor), or click Open Wizard to edit the same properties in a wizard format, with items grouped by property type.

**Data regions**

Data is formatted using *data regions*, which are standard format elements defined for specific types of display. Data regions include:

- **Table**: Rows and columns, with a field from a data set for each column. You can also group rows by a field, such as grouping data by device, where you have a header row for each device and supporting data grouped below the header. (See the Hardware inventory report for an example of grouped rows.)

- **List**: Items are repeated in a list for every record in the data source. You can use any type of formatting for lists, and for complex groupings you can nest lists or put a list inside another data region.

- **Banded list**: A collection bands (header, detail, and footer) where data is repeated in the detail band. Banded lists are useful because you can insert elements freely without being constrained by table or list formats.

- **Matrix**: Also rows and columns, but formatted with both row and column headers, like a cross tab or pivot table.
Data regions are included in the toolbox. They can be combined, nested, and included in any other layout elements.

**Report items**

Items in the toolbox are used to format the page layout and place data on the page.

- **Lines** are used for visual format.
- **Rectangles** are a visual element that contains other items.
- **Text boxes** can be used to place static text or dynamic data anywhere on the page.
- **Images** can be placed anywhere on the page.
- **Charts** summarize selected data.
- **Barcodes** can render data in 23 bar coding styles.
- **Sparklines** are small charts that summarize data and can be inserted inline into text.
- **Calendars** can be added to a page and linked to data to display events within a range of dates.

These and other elements are fully customizable and can be combined in many ways to group and display data.

For ideas on how you can define your own reports, view the properties for any standard report and click **Report designer** to see how the report has been defined.

**Additional help**

For more detailed help on the report designer, see the Ivanti User Community Web site [community.landesk.com](http://community.landesk.com).

**Using reports [Web console]**

When you use the Web console, all the reports found in the Windows console are available to you, but there are minor differences in the way you view and select parameters. You can’t edit or create a custom report in the Web console, or move reports between folders, but you can view, print, and export reports.

When a user runs a report from the Web console, the user’s scope is applied to the report. The report will contain only data from devices within the user’s scope.

To use reports in the Web console, a user must have at least the Reports - View right.

**To run a report from the Web console**

1. In the Web console toolbox, click **Reporting > Reports**.
2. Expand the folder structure and find the report you want to run.
3. Click the report.

In a new browser window, the report opens in the reports viewer.
4. Select the parameters you want and click **View report**.

5. To view details of any portion of a chart, click that area of the chart. The view changes to the section of the report with the data you want.

6. Use buttons on the toolbar to search for data, export the data in a different format, print the report, and so on.

7. When you have finished, close the preview browser window.

**To save a report in the Web console**

1. Run a report.
2. On the viewer toolbar, select the report format you want to use from the **Select a format** list, then click the **Export** button.
3. Save the file using the settings for your browser.

**NOTE:** If you save a report and plan to e-mail it, use the PDF format rather than HTML output.

**Web console report viewer**

The report viewer in the Web console lets you view, print, and export reports. The toolbar consists of the following buttons:

- **Back to parent report:** If you are viewing a sub-report, return to the parent report that launched the sub-report.
- **Hide/Show Side Bar:** Toggle the sidebar pane, which displays search and parameter options and document map view.
- **Page setup:** Change page, orientation, and margin settings.
- **Print:** Opens the printer dialog box associated with the output type you chose.
- **Print preview:** Toggle print preview (page view) mode. When this is not selected, the report displays as a single HTML page.
- **Viewer mode:** View the report in HTML or PDF format. Select a format from the list and click the **Viewer mode** button to change the format.
- **Go to first page:** View the first page of the report.
- **Back:** View the previous page in sequential order.
- **Page box:** Insert a specific page number, which takes you directly to that page.
- **Forward:** View the next page in sequential order.
- **Go to end page:** View the last page of the report.
- **Select a format:** Select the format in which you want to save the report (PDF, HTML, DOC, XML, or XLS file)
- **Export:** Save the report in the format you selected.
The side bar includes three options, represented with icons. As you select options and their respective parameters, the report is refreshed in the viewer.

- **Parameters:** Change parameters of the report, which vary between reports. Once you've selected different parameters, click **View report** to refresh the report with the new parameters.

- **Find:** Search for a string in the report results. Specify the string and select any criteria (such as Match case), then click **Search**. A list of occurrences of the string are shown. Click an occurrence to move to that section of the report. The occurrence is highlighted.

- **Document map:** Displays a content outline of the report, if there is a document map defined for the report. This option is not displayed if there is no document map. Click an item in the list to go to that location in the report.

**Selecting parameters from a list**

When the sidebar includes a list with parameters, you can include all list items in the report by selecting (All). When you do this, the individual items in the list are not selected but all are included in the report.

To select a subset of the items, select each item you want to include in the report. Make sure that (All) is not selected. Use Ctrl+click or Shift+click to select multiple items, then click **View report**.
Selecting devices, groups, or locations

Parameters vary with each report. However, all reports include a device selection option that specifies individual devices, queries, groups, scope, or location. This lets you generate a report for a query, group, or scope that you have defined in the network view, or for a location in your network.

For example, you can select devices in a location based on the device network location. When you select Location, the list displays locations in your network by domain name.

Dashboard editor

The Dashboard editor provides a way to manage customized charts. You can use the Dashboard editor to view charts in a separate window, change chart properties, print charts, and drill-down to view detailed information and run queries. You can also copy charts to the clipboard, and then paste them into another application, such as an email.

The dashboard editor displays pre-defined dashboards for various tools, such as Patch and compliance. You must have previously launched a tool in order for its dashboard to appear in the dashboard editor. You can also create new dashboards.

To open the Dashboard editor, click Tools > Reporting/Monitoring > Dashboard editor. The Dashboard editor opens in the lower panel of the console. From the Dashboard editor toolbar, you can access the following features. Many of these features are also available from the menu that appears when you right-click a chart.
• **New dashboard:** If you have a folder selected in the console, click the **New dashboard** button to create a new dashboard.

• **Add charts...** If you have a dashboard selected in the console, click the **Add charts...** button to add a new chart to the dashboard. You can add the same chart to a dashboard multiple times. For example, you may want to add the same chart more than once in order to apply custom properties to each chart and then view them side-by-side. To see if you already have a chart included in your dashboard, look for a message appended to the title that says, “on dashboard n times,” where n is 1 or greater. To change the order of the charts in a dashboard, simply click and drag the chart to the desired location.

• **Properties:** Click to open the **Properties** dialog for the selected chart. The **Properties** button is only enabled if the selected chart can be edited. You can also edit a chart by right-clicking the chart and clicking **Properties...**. Some charts allow you to apply filters, some charts have editable properties, and some charts don’t have either. For example, with some charts, you can specify a color palette and other charts have hard-coded colors that are defined in the **Properties** dialog. The options in **Properties** dialog vary by chart.

• **Delete selected items:** Click to delete a chart. The **Delete selected items** button is only enabled if the selected chart or dashboard can be deleted. You can’t permanently delete the pre-defined dashboards.

• **Refresh:** Refreshes the data in the charts in the dashboard. The charts in other dashboards will automatically synchronize.

• **Display dashboard in a separate window:** Click to pop out the dashboard as a new window. When you view a dashboard in a separate window, you have access to additional functionality, including filtering by definition type, filtering by scope, applying custom filters, and customizing the auto-refresh. You can view multiple dashboards at a time. For example, you may want to view multiple dashboards for the same tool but employ different filters for each one. For more information about using filters, see [Customize item lists with filters](#).

**NOTE:** Separate dashboard windows remain on top of the console. If you double-click a chart to drill down, you may need to reposition the dashboard in order to view the chart-generated query in the console.
Running reports

Use the Reports tool to run reports, organize them, and create new ones. You can schedule reports to run one time or on a recurring basis. You can also import and export reports for use on other Endpoint Manager consoles.

The quickest way to view report data is to run the report from a console. The report viewer displays the data as a preview of the printed page or as continuous data. You can change views and formats in the viewer. You can also change report parameters to select a subset of the data.

Reports in the Web console

When you use the Web console, the reports found in the Windows console are available to you, but there are minor differences in the way you view and select parameters. You can't edit or create a custom report in the Web console, or move reports between folders, but you can execute, view, and export reports.
Changing report properties

You can make a copy of a predefined report and modify items in the Report properties dialog box. You can change the type of chart displayed in the report and specify a different query field as the key element in the query. You can also select an LDMS query to use as the basis of the report. You can change the name and description as well.
If you want to make more extensive changes to the report, you’ll need to open the report designer. See “Creating custom reports” (385) for details on using the report designer.

**Report viewer**

When you run a report, the report viewer launches and displays the generated report. This report viewer provides controls that let you display the report according to your viewing preferences. You can also export a report from the report viewer or save it in a different format for distribution.

The report viewer includes a toolbar and a sidebar. The toolbar consist of the following buttons:
- **Open**: Open a saved report in the viewer.
- **Export**: Save the report as an image (in BMP, EMF, GIF, JPEG, TIFF, or PNG format), or in HTML, PDF, XML, XLS, or DOC format.
- **Copy**: Copy the contents of the report for the selected page.
- **Print preview**: Toggle print preview (page view) mode. When this is not selected, the report displays as a single HTML page.
- **Page setup**: Change page, layout, and watermark settings.
- **Print**: Opens your standard default printer dialog box.
- **Sidebar pane**: Toggle the sidebar pane, which displays search and parameter options and thumbnail view.
- **Back to parent report**: If you are viewing a sub-report, return to the parent report that launched the sub-report.
- **None**: Use standard mouse movement for viewing.
- **Pan mode**: Drag the hand pointer to pan in any direction on the page.
- **Selection mode**: Drag the pointer to select a portion of the page. You can paste the selection in another application that supports pasted text.
- **Snapshot mode**: Drag the pointer to select a rectangle. You can paste the rectangle in another application that supports pasting images.
- **Zoom in**: Increases the size of the report.
- **Zoom out**: Decreases the size of the report.
- **Zoom percentage**: Selects the viewing size of the report.
- **First page**: View the first page of the report.
- **Previous page**: View the previous page in sequential order.
- **Page box**: Insert a specific page number, which takes you directly to that page.
- **Next page**: View the next page in sequential order.
- **Last page**: View the last page of the report.
- **Cancel**: Stops the report from running. If the report has completed running, this button is dimmed.
- **Refresh**: Return to the initial view.
- **Find**: Open the search pane to find a specific text string in the report data.

The sidebar includes three options, accessed with icons at the bottom of the sidebar:
### Parameters

Change parameters of the report to select a subset of the data and vary the results depending on how the report is defined. Once you've selected different parameters, click **View report** to refresh the report with the new parameters.

### Search results

Find a string in the report results. Specify the string and select any criteria (such as Match case), then click **Search**. A list of occurrences of the string are shown. Click an occurrence to move to that section of the report. The occurrence is highlighted. You can also click a green bar along the right side of the report to move between occurrences.

### Page thumbnails

View thumbnails of the report pages. Click a thumbnail to move to that page.

### Selecting parameters from a list

When the sidebar includes a list with parameters, you can include all list items in the report by selecting the **All** check box. When you do this, the check boxes for individual items are not selected but all are included in the report.
To select a subset of the items, clear the All check box and then select the check box next to each item you want to include in the report.

**Selecting devices, groups, or locations**

Parameters vary with each report. However, all reports include a device selection option that specifies individual devices, queries, groups, scope, or location. This lets you generate a report for a query, group, or scope that you have defined in the network view, or for a location in your network.

For example, you can select devices in a location based on the device network location. When you select Location, the list displays locations in your network by domain name.

**Sub-reports**

Some reports can open secondary reports, or sub-reports. Under the Security folder, there are dashboard-style reports for Antivirus and Vulnerabilities. If you open the dashboard report (or parent report), you can click one of the charts to open the corresponding sub-report (or child report).

For example, if you run the Antivirus dashboard report, click the “Real-time scanner status” chart to open a separate report with device scan status. You can then click the **Back to parent report** button to return to the dashboard report.
Run a report

When you run a report, the report viewer displays the data as a preview of the printed page or as continuous data. You can change views and formats in the viewer. You can also change report parameters to select a subset of the data.

1. In the Reports tool, select a folder from the Reports tree structure and find the report you want.
2. Double-click the report.

   The report preview dialog box opens. Some reports have configurable parameters that let you select a subset of data for the report. If there are no default parameters, you need to enter at least one (such as specifying a device name) or there will be no data in the report.

3. If there are parameters you can choose, specify the parameters you want.
4. Click View report.
5. To view details of any portion of a chart, click that area of the chart. The view changes to the section of the report with the data represented in that area of the chart.
6. On report pages, click column arrows to sort data by that column.
7. Use buttons on the toolbar to search for data, export the data in a different format, print the report, and so on.
8. When you have finished, close the preview browser window.

NOTE: When you select devices using the Device parameter, no wildcard is used. Type any number of characters that are common in the device names you want to select, and click View report. All device names with that string of characters will be included in the report.

Selecting parameters from a list

When the sidebar includes a list with parameters, you can include all list items in the report by selecting the All check box. When you do this, the check boxes for individual items are not selected but all are included in the report.

To select a subset of the items, clear the All check box and then select the check box next to each item you want to include in the report.

Save a report to a file

After you run a report, you can save the results to a file location. The report can be saved as an image (in BMP, EMF, GIF, JPEG, TIFF, or PNG format), or in HTML, PDF, XML, XLS, or DOC format.
1. Run a report.
2. On the viewer toolbar, click the Export button.
3. Click the report format you want to use.
4. In the Export dialog box, change any parameters for the report. (Parameters vary depending on the format you selected.)
5. Browse to the location where you want to save the report, type a name for the report, and then click Save.
6. Click Export.

**NOTE**: If you save a report and plan to e-mail it, use the PDF format rather than HTML output.

### 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. When you schedule a report, it is saved to the LANDesk Reports share (Idmain\reports) and also sent to any users on the core server who have Report rights and who have an e-mail address associated with their user name (in the User management tool). E-mailing reports requires an SMTP mail server.

A report that is saved to the Reports share is based on the scope of the person who scheduled it. In the case of reports sent to other recipients, the report uses the scope of each recipient to filter the data.

To schedule a report, a user must have the Reports - Deploy right.

If you want to distribute a report that you have run, save the report in the format you want and then attach that file to an e-mail message. The report will use your scope. Users with rights to the Reports share can also view the report from that file location.

**NOTE**: If you save a report and plan to e-mail it, use the PDF format rather than HTML output.

**NOTE**: Running reports with extensive data can consume large amounts of system resources on the core server. Because of this, only one report can be scheduled at a time. If one report is running and you schedule other reports at the same time, the second and subsequent reports will be delayed until the first report has completed.

### Schedule a report

1. In the Reports tool, expand the tree and select a report to schedule.
2. Click Schedule on the toolbar, selecting the format you want to use.

The Scheduled tasks tool opens with the report selected.
3. Click the **Properties** button on the toolbar.
4. In the **Schedule task** dialog box, enter or edit the information on each page.
5. Click **Save**.

You can view the progress of the report in the Scheduled tasks tool (click the **My tasks** folder).

For descriptions of the options in the Schedule Task dialog box, see **About the Schedule task dialog box**.

### Modify a report's properties

1. In the **Reports** tool, copy a report and paste the copy into a folder.
2. Right-click the report and select **Properties**.
3. In the **Report properties** dialog box, change any properties.
4. Click **Preview** to view the customized report in the report viewer.
5. Click **OK** to save the modified report.

### Customize a report template

All reports are based on templates provided with Ivanti® Endpoint Manager powered by Landesk. If you want to customize a report template, you need to open the master template file in the report designer. For example, you might want to add your company name and logo to the template, or change the basic page layout, font, or other elements.

There are three template files, one with a portrait orientation, one with a landscape orientation, and one for dashboard templates.

**NOTE:** Report templates are installed on every device that you install a console on. If you change a template on the core server, that template is used when you run reports on the core and from the Web console. However, other consoles will use the template that was installed on them. If you want to use the revised template on other consoles, you'll need to copy the template file to each additional console or create a distribution job to distribute the template files.

#### To customize a report template

1. In the **Reports** tool, click the **Edit template** button on the toolbar.
2. Select the portrait, landscape, or dashboard option.

   The template opens in the report designer.

3. Make any changes in the report designer. When you have finished, click the **Save** button on the toolbar.
Running ad hoc reports

Simple reports are available for most items in the Windows console. Any group or container (such as a query) has a context menu option to run a report. The report displays the data in the current view, organized using the data columns displayed in the console.

For example, an ad hoc report from a group in the network view shows a list of devices in that group. The columns in the network view (such as IP address, owner, and so on) are displayed in the report. To change the organization of the report data, modify the column set (add or remove columns or change their order) before you run the report.

You can run a report for many tools, showing the items in a particular view (such as a list of alert rulesets in the Alerting tool). You can run a report for any query you create or for any group you have created in the network view or elsewhere.

There are three ways to create reports quickly from the console:
• **View as report:** Right-click an item and select this option to view the data in a standard report format. A report preview window opens, and you can select different options before printing, saving, or sending the report.

• **Export as CSV:** Right-click and select this option to save the data in a comma-separated value file.

• **New report:** Right-click a query and select this option to create a new report based on the query. You can use a standard format or open the report designer to further customize the report. The new report is saved in My reports.

**Run an ad hoc report**

Simple reports are available for most items in the Windows console. Any group or container (such as a query) has a context menu option to run a report. The report displays the data in the current view, organized using the data columns displayed in the console.

1. In the Windows console, right-click a tree item, such as a group in the Network view or an item in a tool pane.
2. If there's a **View as report** menu item, click it and select the report format you want.

If there's no **View as report** menu item, the item you right-clicked doesn't support this option.

**Save a report as a CSV file**

You can save data as a CSV (comma-separated value) file for most items in the Windows console. Items with this feature have a context menu option that saves report data in this format.

1. In the Windows console, right-click a tree item, such as a group in the Network view or an item in a tool pane.
2. Select **Export as CSV** and specify a location to save the CSV file.

If there's no **Export as CSV** menu item, the item you right-clicked doesn't support this option.

**Create a report from a query**

You can run a report for any query you create or for a group you have created in the network view or elsewhere.

1. Right-click a query in the network view.
2. Select the **New report** menu item.
3. Type a name and description for the report and make any other custom changes you want.
4. Click **OK** to save the report.

If there's no **New report** menu item, the item you right-clicked doesn't support this option.
Organizing reports

As you use standard reports and create custom reports, you’ll need to organize and modify them to meet your needs.

Copy and modify

Standard reports can’t be deleted, but you can copy and paste them to other folders. For example, you might create a folder under My reports that contains the reports you use most often.

You can also copy a standard report, edit it, and save it as a unique report. This is usually easier than creating a report from scratch. Each time you copy a report, a number is appended to the report name to distinguish it from other copies. When you edit the report you can give it a unique name.

NOTE: You should make a separate copy of a report for each revision you create. If you have copied and modified a report, and then make additional changes to it and save it again, your previous modifications will be lost. We recommend that you make a new copy every time to ensure that queries or parameters aren’t lost.

Share with other core servers

Reports are run using a core server’s database. If you have multiple core servers, you can share reports between them so reporting is standardized in your organization.

Share a report one time only by using the Copy to other cores option. This saves a copy of a report in the same folder structure of the other core server’s reporting tool.

To share a report on a permanent basis, you can synchronize reports between core servers. Any time a report is modified, a copy of the modified report is automatically saved to the other core servers you have selected for content synchronization. This feature is part of the Core synchronization tool.

Import and export

You can import and export reports, either to save copies of your reports or to share reports and templates with others. For example, if you save exported copies of your reports, and you’ve deleted a report and later decide you want it back, you can re-import it.

Reports are stored in plain-text XML files with an .ldms file extension in the location you specify. These files can only be read by Ivanti® Endpoint Manager powered by Landesk.

The folder and file names of exported reports generally match the way they appear in the reporting tool.
Copy, move, and delete reports

You can copy any report, edit it, and save it as a unique report. This is usually easier than creating a report from scratch. When you copy a standard report, a number is appended to the report name to distinguish it from other copies. When you edit the report you can give it a unique name.

NOTE: You should make a separate copy of a report for each revision you create. If you have copied and modified a report, and then make additional changes to it and save it again, your previous modifications will be lost. We recommend that you make a new copy every time to ensure that queries or parameters aren’t lost.

To copy and move reports

1. Click Tools > Reporting/Monitoring > Reports.
2. Expand the tree structure to find the report you want.
3. Drag the report to another folder.

NOTE: While you can copy any type of report, only custom or copied reports can be cut and pasted. To do this, right-click the report and click Cut, then open the destination folder, right-click, and click Paste.

To delete a report

1. Click Tools > Reporting/Monitoring > Reports.
2. Expand the tree structure to find the report you want.
3. Select the report and click the Delete button on the toolbar.

Only custom or copied reports can be deleted.

Synchronize reports between core servers

Reports can be synchronized between multiple core servers. With core synchronization, you can copy configurations and tasks from core to core, either manually or automatically. Synchronization lets you copy items on a regular basis and ensure that multiple core servers are using the same tools and data.

1. Click Tools > Administration > Core synchronization.
2. Under Components, right-click Reports and select Auto sync.

To synchronize one report with other cores, right-click the report and click Auto sync. For more information, see "Core synchronization" (105).
Copy reports to other core servers

Synchronize a report on demand with the Copy to other cores option. When you do this, you can select the servers you want to receive the copy. The copy only happens once, and the item you copied is available on the remote cores immediately.

1. In the Reports tool, expand the tree and select a report to copy. Use Ctrl+click or Shift+click to select multiple reports.
2. Right-click the report and click Copy to other cores.
3. Select the core servers you want to receive the copy.
4. Click Copy content to immediately start the copy operation.

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 report will be created automatically.

Import and export reports

Exported reports are stored in plain-text XML files with an .ldms file extension in the location you specify. These files can only be read by Ivanti® Endpoint Manager powered by Landesk.

The folder and file names of exported reports generally match the way they appear in the reporting tool.

To export a report

1. In the Reports tool, expand the tree and select a report to export.
2. On the toolbar, click the Export button.
3. Browse to the location where you want to export the report to and click Save.

To import a report

1. In the Reports tool, select the folder in which you want to save imported reports (My reports or Public reports).
2. On the toolbar, click the Import button.
3. Browse to the location of the report you want to import, and click Open.
4. In the Import options dialog box, select an import option.
   - **Update**: Adds reports to the groups specified in the .ldms file, keeping the same ID. If the report already exists it is not duplicated.
   - **Insert items into selected group or owner**: Adds reports to the group you selected, assigns a new ID, and updates the owner. If the report already exists a second copy is saved with a version number appended.
- **Insert items into groups specified in the .ldms file:** Adds reports to the groups specified in the .ldms file, and assigns a new ID. If the report already exists a second copy is saved with a version number appended.

5. Click the **Import** button.
Scheduling tasks

Scheduling tasks

Ivanti® Endpoint Manager powered by Landesk includes a powerful scheduled task system. Both the core server and managed devices have services/agents that support scheduled tasks. Endpoint Manager consoles and Web consoles can add tasks to the scheduler.

A software distribution 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

Schedule a task

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 Ivanti 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" (95).

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.

Before you can schedule tasks for a device, it must have the standard Ivanti agent and be in the inventory database.

To schedule a task

1. In the Scheduled tasks window, click one of these toolbar buttons: Schedule custom script, 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.

**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.

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 Endpoint Manager 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.
Tasks also have a right-click menu that you can use. The right-click Start now menu option has these choices:

- **All**: Runs the task on all targeted devices.
- **Devices that did not succeed**: Runs the task only on targeted devices that tried to complete the task but weren’t successful.
- **Devices that did not try to run the task**: Runs the task only on targeted devices that didn’t try to run the task, such as devices that were powered off or not connected to the network.
- **Waiting or currently working**: Runs the task on devices that are in a waiting or currently working state. This is useful when devices are stuck in one of these task states and you want to try the task on them again.

### 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 lists of devices to be configured, devices being configured, and devices completed.

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.

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.
Changing default scheduled task settings

You can change many default scheduled task settings. These default settings are applied every time you schedule a task. You can change the following defaults:

- How many devices accelerated push should process simultaneously
- APM policy maintenance cleanup interval for targets from the LD_LDAP_TARGETS database table
- Task type (policy-supported push, policy, or push)
- Frequency, such as run once or run hourly
- Additional push options, such as accelerated push or wake up devices
- Download options, such as run from source or pre-cache
To change default scheduled task settings

1. Click **Tools > Distribution > Scheduled tasks**.
2. In the scheduled tasks toolbar click the gear icon and click **Default scheduled task settings**.
3. Change the default settings and click **Save**.

Scheduled task templates

Tasks have many configuration options. If there’s a task configuration that you tend to reuse, you can make it a task template. The next time you create a new task, you can create it from the template and have that template's task settings automatically applied.

Endpoint Manager ships with some default task templates that are preconfigured with recommended settings.

To create new scheduled task based on an existing template

1. Click **Tools > Distribution > Scheduled tasks**.
2. From the tree's **Task Templates** group, open the shortcut menu for the template you want and click **Create scheduled task(s)**.
3. The **Schedule task** dialog box opens with the template's settings preconfigured. Customize the settings as necessary and click **Save**.

To create new scheduled task based on a template

1. Click **Tools > Distribution > Scheduled tasks**.
2. Click the **Task templates** tree item.
3. On the toolbar, click **New > Software distribution template** or **New > Patch template**.
4. Configure the template settings and click **Save**. Your new template will appear in the tree under **Task templates**.

Understanding task 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.

### Cancel 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**.

### Using the default scripts

Endpoint Manager ships with a default set of scripts that are listed below. You can use them to help you complete some Endpoint Manager 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.
- **Data Analytics - Import and delete users**: Runs a Data Translation Services rule to archive the devices of specified users into Asset Control while deleting the devices from the Endpoint Manager database.
- **Disable Windows write filter**: Disables the Windows write filter; initiates a reboot on the client.
- **Enable Windows enhanced write filter**: Enables the Windows enhanced write filter; initiates a reboot on the client.
- **Enable Windows file-based write filter**: Enables the Windows file-based write filter; initiates a reboot on the client.
- **inventoryscanner**: Runs the inventory scanner on the selected devices.
- **MSI service deployment**: Deploys the MSI service required for a legacy PXE representative.
- **multicast_domain_discovery**: Does a Targeted Multicast domain representative discovery.
- **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 named 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 Endpoint Manager prior to version 8.

### Managing scripts

Ivanti® Endpoint Manager powered by Landesk uses scripts to execute custom tasks on devices. You can create scripts from the **Manage scripts** window (Tools > Distribution > Manage scripts).

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.

### Assigning targets to a task

Once you’ve added a script to the Scheduled tasks pane, it becomes a task that you can assign targets to by dragging them from the network view onto the task. Targets can include individual devices, device groups, LDAP objects, LDAP queries, and inventory queries. Queries and groups are powerful options that enable you to 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 automatically target the new devices in the list.

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 to select task targets, the query doesn’t run until the task has started. The Scheduled task properties dialog won’t show the target devices until after the task is launched.

You can also add targets directly from the task properties Targets page. Targeting from this page gives you a single point of access to all available target types and possible targets. Just select the target type you want and click Add.

### Applying scope to tasks

Multiple Endpoint Manager users can add targets to a scheduled task. However, in the Scheduled tasks pane, each Endpoint Manager user will only see targets within their scope. If two users with scopes that don’t overlap each add 20 targets to a task, each 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 needs a set of targets to 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 edit 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 target devices that policy-based distribution tasks check periodically for any changes. As new devices meet the query criteria, recurring tasks using those queries get applied to the new devices. Dynamic lists include query results and LDAP groups/containers or network view groups.

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, device, 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.

**Target devices through a directory**

In order for devices to receive policies that are targeted through Active Directory, 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.

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 button.
5. Create your query. For more information, see "LDAP queries" (371).

**Using time zone awareness with task targets**

Ivanti® Endpoint Manager powered by Landesk version 9.6 added time zone awareness. There are over 30 time zones in the world, and if you are a global company it can be difficult managing time-sensitive tasks that target devices in multiple time zones. For example, if your company has a maintenance window of 2 AM to 3 AM and your company has offices in both Europe and America, it would be nice if you didn’t have to create separate tasks to target the devices in each time zone so the task happens during that window. Now you can easily do all this in a single task.

Among the inventory data Endpoint Manager maintains for each managed device is the time zone the device is in. If you want it to, the task scheduler can use this data to automatically run the task based on the device’s time zone instead of the core server’s time zone.
To use time zone awareness in a task

1. Schedule a task and add targets to it.
2. Right-click the task and click Properties.
3. On the Target devices page, review the Targeted time zones list to see the list of targeted devices sorted by time zone.
4. On the Schedule task page, select Target time zone aware so the task runs based on the target time zone.
5. Save your changes and run the task. As the scheduled time arrives in each time zone, the core server runs the task on targets in that time zone.

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 statuses the device can have, 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

When a device is processing a task, it will move through these stages (visible in the Stage column):

- Core initiated
- Starting
- Downloading
- Installing
- Completed
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.

Viewing task scheduler status charts

Ivanti® Endpoint Manager powered by Landesk 9.6 SP1 added task scheduler status charts. In the Scheduled tasks tool (Tools>Distribution>Scheduled Tasks), click the root Scheduled tasks item to view the charts, which provide information on many items, such as:

- **Task summary**: Configurable by days or hours. Administrators can see all tasks, scoped by owner, starter, or otherwise.
- **Summary**: Administrators can see all tasks, scoped by owner, starter, or otherwise.
- **Tasks by type**: Shows tasks by type (such as policy-supported push, policy, or push). Administrators can see all tasks, scoped by owner, starter, or otherwise.
- **Stale tasks**: Configurable by days or hours. Shows tasks with devices that haven’t responded.
- **Top failure codes**: Shows top seven failure codes.
- **Task failures by stage**: Shows failure counts by task stage, such as initiated, starting, downloading, or installing.
- **Client state**: Shows client state across tasks, such as in progress, downloading, or installing.
- **Top task owners**: Shows the top seven task owners.
- **Top task by scoped user**: Shows the top seven task starters.
- **Tasks by component**: Shows the task counts for Endpoint Manager components, such as Antivirus, Change settings, Installer, Patch, Provisioning, Reboot, Software Distribution, or Unknown.

For users that aren’t console administrators, all charts are scoped by owner, starter, or the device. Scope doesn’t apply to charts for the top task owners or top tasks by scoped user.

Each chart has a toolbar that enables you to do the following:

- Refresh the chart data
- Copy the chart to the clipboard as an image
- Print the chart
- Change the chart view between pie and bar types
- Edit the properties, if possible, for that chart
To configure which task scheduler charts are visible

1. Click **Tools > Configuration > Scheduled tasks.**
2. In the main Scheduled tasks window toolbar, click the **Charts** button.
3. Move charts that should be visible to the Selected charts box.
4. Select a chart and use the up and down arrows to change the display order.
5. Click **OK.**

Viewing devices and status in task scheduler charts

Ivanti® Endpoint Manager powered by Landesk 9.6 SP1 added task scheduler status charts. In the Scheduled tasks tool, click the root **Scheduled tasks** item to view the charts. When you double-click a bar or pie slice in a chart, you can get additional information on devices inside the item you clicked. All charts have one of two drill-down options: failures or status. Devices in the drill-down view have the same right-click menu options that you get in the Network View. Additionally, when you select a device in the drill-down view, you can use the toolbar to access these features:

- **Real-time discovery:** Discovers the device's fully-qualified domain name, IP and MAC address, and the Endpoint Manager device ID.
- **Remote event viewer:** Launches the Windows Event Viewer locally with data from the selected device.
- **Remote file system:** Launches the windows file explorer and shows the device's C$ share.

Using the Diagnostics tool

The Diagnostics tool facilitates the troubleshooting of software distribution and patching tasks by providing convenient access to critical information in real time. To access the Diagnostics tool, right-click a device in the network view and then click **Diagnostics.** Alternatively, in the Scheduled tasks pane, double-click the “Top failure codes” chart. You can also drag and drop devices from the network view into the Diagnostics tool, which opens in a separate window.

The Diagnostics tool toolbar has the following features:

- **Logs:** From this drop-down menu, you can pull logs in real time from both the client and the core server. If you select logs based on a task, the tool will automatically pull the logs for the highlighted task. From the **Client** menu, you can choose to download all of the logs from the device as a zip file, or to get SCAP reports. Logs appear with highlighted syntax and are searchable. You can view a truncated version of the log within the Diagnostics tool if the log file is larger than 50 KB, or view the log in an external viewer. All sdclient return codes are linked to
related content on the Ivanti Community website, which is especially helpful for diagnosing failed logs. If the log-viewing area has focus, pressing F5 will redo the last action and enable you to watch client log updates in real time.

- **Real-time discovery:** Discovers the device in real time and then verifies that it’s available on the network and that Ivanti can communicate with it.

- **Inventory:** Open an Inventory window for the selected device.

- **HTML5 Remote control:** Opens an HTML5 Remote Control window for the selected device.

- **View task client policy:** Displays the client policy settings for the selected task, which is useful in debugging.

- **View Security and Patch information:** Displays detected vulnerabilities.

- **Client inventory change history:** Displays the newly downloaded items.

- **Client task history:** Displays a history of all of the tasks and their status.

- **Enable remote file system access:** Allows you, when working with devices that are running Windows 8 and later, to avoid a popup window requesting credentials if the username and password are the same. (Earlier versions of Windows do not support this feature.)

- **Remote event viewer:** Displays the selected device’s Event Viewer for simplified troubleshooting using the logged-on user’s credentials.

- **Remote file system:** Opens Windows Explorer to the C$ share of the selected device using the logged-on user’s credentials.

- **Synchronize policies:** Manually kicks off a policy sync on the device.

- **Rerun task on selected device:** Runs the task again, overriding the settings specified in the local scheduler.

- **Terminate process:** Allows you to terminate a process on the device by entering a process ID and clicking OK. If you’re viewing a client’s running processes, you can highlight and right-click the process ID and stop it from the viewer.

- **View local scheduler tasks:** Displays the client local scheduler tasks.

- **View running processes:** Displays processes that are running on the device and highlights the Ivanti processes. Allows you to highlight the process ID and terminate it with a right-click option.

- **View services:** Displays the current state of all services installed on clients.
• **Search Ivanti Community website:** Takes text you’ve highlighted in the log file and searches the Ivanti Community to help find more information.

• **Search the web for highlighted log file or the current error code (F3):** Takes text you’ve highlighted in the log file and enters it into a web search to find more information. This is helpful when investigating return codes from common programs like Microsoft Office, or an MSI install that uses standard MSI return codes.

• **Find:** Provides real-time searching in the device list view.

• **Export to CSV:** Creates a CSV export of the clients and task lists.

• **Refresh:** Refreshes the content displayed in the Diagnostics tool window.
Local scheduler

About 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 Endpoint Manager tasks, such as running the inventory scanner periodically. Other tasks that you schedule, such as software or OS provisioning, 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 Endpoint Manager 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.

Installing the local scheduler service on an unmanaged device

The Ivanti 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 Ivanti Local Scheduler service on an unmanaged server or workstation, follow the steps below.

1. Create this 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 Ivanti 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.

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 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.

/req=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.

Create a local scheduler command

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.
To create 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.

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 Ivanti use. Task ID values 1001-2000 are reserved for use by the management console’s local scheduler interface.

LocalSch.exe command-line parameters

In addition 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.

```
[/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 device. The local scheduler service should be stopped before you remove it.

/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

Local scheduler 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 not 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 third for 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, the 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

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.

If the device agent has been configured to do so (in the device's agent configuration), you can also require the user to give permission before each new session can be initiated.

Once the connection is established, the Remote status icon appears in the top left corner of the user's window.

This alerts the user that their machine is being remote controlled. The user can right-click the icon to end the session at any time, to see if it is still active, to find out who is remote controlling it, etc.

You can do more than just remote control a device from the viewer window. Once the viewer connects to a device, you can choose from these tasks on the Toolbar.

- **Connect/Disconnect**: Initiate or end a remote control session.
- **Start/Stop viewing**: Display or hide the remote device's screen in the remote control viewer.
- **Chat**: Remotely chat with a user at a remote 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 perform 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.

The toolbar also lets you control how the remote device appears on your screen. For example:

- **Full remote screen**: Use this option to completely fill your local monitor with the remote device's screen. If the remote screen's resolution exceeds yours, Autoscroll (see below) may be necessary unless you have enabled the **Fit to screen** option.
• **Fit to screen:** Since the viewer window may not be as big as the remote device's screen, you can use this to dynamically make the user's screen fit within the viewable area on your monitor.

• **Multi-monitors:** If the remote user has more than one monitor, this button will be activated automatically, allowing you to quickly switch between monitors (up to 8) in your Remote window. You can minimize or resize any of the remote monitors to make them easier to work with inside of your Remote control window.

If you select the **All** option, all monitors will be automatically resized so they all fit within the remote control viewer window. You can then select and drag to resize any monitors to make them easier to work with.

The toolbar also includes a Run option, which lets you browse to and run an executable program on the remote device.

You can use the **Autoscroll** feature (**Tools > Options > Change settings > Allow autoscroll**) to scroll up, down, and side to side. Autoscroll automatically scrolls the window as the mouse pointer approaches the viewer window's edge.

You can also increase the viewer window's displayable area by disabling items in the View menu, such as connection messages, the toolbar, or the status bar.

If you want to speed up the viewing rate or change the viewer window settings, use the options on the **Optimize** button on the toolbar.

## Connect to Remote devices

Before you can do any remote control tasks, you must connect to the target device. You can choose to connect directly or through a Ivanti Management Gateway. 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, right-click the device you want to remote control, and 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 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.

**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:

- **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.

- **Scribble**: Use the scribble tool to draw an arrow, circle an object, make a freehand drawing, etc. You aren’t limited to a shape with the scribble tool.

- **Box**: Use the box tool to draw a rectangle around an object on the screen. Click where you want a corner of the rectangle to be. Drag to draw a box around the area you want to highlight, then release the mouse button.

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 Tools > Options dialog’s Change settings tab 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 the remote keyboard and mouse**: Locks the remote device’s keyboard and mouse so that only the person 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 person running the remote viewer can see the screen 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 this is 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. This enables the remote control operator to complete their work and then leave the user's system in a secure state while the user is away or until they are ready to resume following a remote control session.

Auto keyboard mapping: You should keep this option selected. It remaps the target device's keyboard so it matches the administrator's. 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.

Use 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.

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 (Tools > Options > Hot key settings):

- **Enable hot keys** (Ctrl+Alt+H): Enable/Disable hot key availability. Hot keys are enabled by default.
- **Close viewing session** (Ctrl+Alt+S): Disconnect the current viewing session. The remote control viewer window stays open.
- **Send Ctrl-Alt-Delete** (Ctrl+Alt+D): Send Ctrl+Alt+Delete to the target device.
- **Lock out remote keyboard and mouse** (Ctrl+Alt+K): Enable/Disable the target device's local mouse and keyboard.
- **Toggle full-screen** (Ctrl+Alt+M): Toggle the remote control viewer between windowed mode and full screen mode.
- **Send Ctrl+Esc** (CTRL+Alt+E): Send Ctrl+Esc to the target device.
- **Toggle mouse and drawn mode**: Toggle between drawing mode and normal mouse pointer mode.
- **Fit to screen**: Define a default hot key sequence for toggling the Fit to screen option on and off.
- **Refresh screen**: Retransmit screen data from the remote computer.
- **Refresh data**: Send a refresh command (F5) to the remote computer.
- **Disconnect session**: End 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 Windows 7 and newer devices**

The default local security policy on Windows 7 and later devices won’t allow Ctrl+Alt+Del from a remote control viewer. To change this, do the following.

**To allow Ctrl+Alt+Del on Windows Windows 7 and newer devices**

1. In the Start menu’s search box, type gedit.msc and press Enter.
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.

**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 "Using the mirror driver" (439)

**Interact with remote control device users.**

During a remote session, you will be interacting directly either with the remote controlled end user or with the device itself, or both. The remote control tool lets you open a chat window, transfer files, run programs on the device, or reboot the device. You can also save a transcript of a chat session for your own reference or as a copy for the user.

**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 in a chat window 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.
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 or 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

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 Ivanti 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

Endpoint Manager 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 “About the Remote control page” (134).

Using remote control logging

By default, Endpoint Manager logs remote control actions, including the device being 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.

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 operator
- Remote Control Summary
(The list of default reports may vary from one release to another)

To enable or disable remote control logging

1. In the Endpoint Manager console, click **Configure > Remote control logging**.
2. Select 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.

Enabling remote control logging to a text file.

You can enable remote control logging to a text file by creating the following registry keys on managed devices:

- Create the following DWORD value and set it to 1: HKLM\SOFTWARE\LANDesk\Instant Support Suite Console\Container\LogSessionMessages.
- Create the following string value and set it to a UNC-accessible path (including a trailing backslash) from a managed device: HKLM\SOFTWARE\LANDesk\Instant Support Suite Console\LogPath.

The log’s filename is issuser.log.

Changing the remote control mode on target devices

The Ivanti remote control agent on devices accepts two types of connections:

- Direct connections from the Ivanti 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.

### 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/a&lt;address&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
| /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:  
<p>|                | isscntr /agamma /c&quot;remote control&quot; /c&quot;file transfer&quot;                                                                                     |
|                | You can choose from these features:                                                                                                        |
| <strong>Remote control</strong>: | Open a remote control window                                                                                                                 |
| <strong>Reboot</strong>:    | Reboot the given device                                                                                                                     |
| <strong>Chat</strong>:      | Open a chat window                                                                                                                         |
| <strong>File transfer</strong>: | Open a file transfer session                                                                                                                  |
| <strong>System info</strong>: | Open a window displaying information about the device, including OS, memory, and hard drive space.                                       |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/l</td>
<td>Limit the viewer interface so it only displays the features you specify with /c.</td>
</tr>
<tr>
<td>/s&lt;core server&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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"`

**Example 4**

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"`

**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 Ivanti agents loaded.
To check that the Ivanti 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.
HTML remote control

HTML remote control is a new feature introduced in Ivanti® Endpoint Manager powered by Landesk 9.5. HTML remote control uses your browser as the remote control viewer. The HTML remote control viewer requires no software installation or browser plugins. After using the HTML remote control viewer, there's nothing to uninstall. This lets administrators easily start an HTML remote control session at someone else's desk if necessary.

HTML remote control works from most HTML 5 browsers, such as current versions of the following:

- Chrome
- Firefox
- IE 10 or later
- Safari
- Opera

You can run these browsers on any operating system they support and HTML remote control should work:

- Windows
- Linux
- OS X
- iOS and Android mobile devices

Compared to classic remote control, HTML remote control does require slightly more network bandwidth and CPU usage. To reduce bandwidth, you can adjust the bits per pixel sent or use the new grayscale mode. For more information, see "Performance settings" (455).

Enabling HTML remote control on managed devices

HTML remote control is part of the existing client remote control agent and it isn't enabled by default. Once you enable it, the client remote control agent hosts a small custom web server on port 4343. There are no extra programs to install or configure.
Enabling HTML remote control doesn't disable classic remote control. You also don't need to manually switch between remote control modes on clients. The remote control agent automatically detects which type of remote control session is being requested.

HTML remote control supports all of the same security models that classic remote control supports.

**To enable HTML remote control**

1. Click **Tools > Configuration > Agent configuration**.
2. Double-click the agent configuration you want to modify.
3. On the **Remote control** page, click **Configure**.
4. Select the remote control settings configuration that you want to modify, and then click **Edit**.
5. On the general settings page, select **Allow HTML access**.
6. Click **Save** and exit the dialogs.
7. Redeploy the agent configuration you modified to managed devices.
After enabling HTML remote control and deploying updated agents (or agent settings) to managed devices, you’ll have to wait for the devices to send an inventory scan before the right-click **Network view** menu shows an HTML remote control option. You can still remote control the device directly from a browser. For more information, see "Starting an HTML remote control session" (450).

**Using remote control from a mobile device**

A larger tablet or iPad mobile device works well with HTML remote control. Because mobile devices tend to have slower CPUs than desktop devices, your remote control sessions may have a slightly slower frame rate than an equivalent desktop HTML remote control session. Consider enabling grayscale mode to improve performance.

Older Android mobile devices may have older browser versions that won’t work as well with HTML remote control. In particular, remote controlling another computer from a mobile device running an older browser and then letting the mobile device sleep while the session is active can cause the mobile browser to freeze. If this happens, you may be able to type a new URL for the browser to navigate to and that will release the HTML remote control page.

**Multiple viewer support**

HTML remote control allows multiple viewers to view the same target device. Any viewer can control the target, so you will want to choose one person to operate the remote mouse and keyboard.

The number of remote viewers is limited by the target device’s CPU speed and available network bandwidth. Generally, up to three viewers will work acceptably. If you add more than that, you may notice framerate reductions.

Enabling grayscale mode may allow you to add more viewers because of the reduced network bandwidth requirements.

**Starting an HTML remote control session**

You can launch HTML remote control from the Endpoint Manager Windows console or directly from a browser.
To launch HTML remote control from the Windows console:
  - Right-click a device and click HTML remote control.

To launch HTML remote control directly from a browser
  - Enter this URL: https://<device name or IP address>:4343

NOTE: The URL uses https:// and not http://.

When you manually launch remote control from a browser, you will need to provide domain credentials for a user authorized to use remote control.

Using the HTML remote control window

Once you’ve logged in, your browser shows the HTML remote control session viewer. The viewer has a toolbar along the bottom that gives you access to these controls:

- **Keyboard**: Toggles the on-screen keyboard that you can use to press keys that your browser can’t normally pass to the remote computer. The ctrl, alt, and shift (up arrow) keys are sticky.
and will stay down until you click the key again. On a Macintosh device, the Command key is also sticky.

- **Screenshot**: Creates a screenshot and allows you to save the image.
- **Monitors**: If the remote computer has multiple monitors, this button lets you choose which monitor you want to see. The monitor thumbnails show what was on each monitor when the session started. For more information, see “Controlling devices that have multiple monitors with HTML remote control” (453).
- **Tools**: Displays the Tools dialog, which contains the following options:
  - **Remote Execute**: Enter a file name or click Browse... to locate a file to execute, then click Run.
  - **File Transfer**: Enter the Remote Machine name and browse to the file by selecting a drive from the list.
  - **Restart**: Enter the notification timeout in seconds and a message for the user and then specify whether to shut down or restart the computer. Enter a reconnect timeout in minutes, and then click Restart.
  - **Chat**: Click Start Chat to begin the chat session.
- **Clipboard**: Displays text and files that have been in the remote device's clipboard during the current session. You can use this to copy remote text and files to your local device. For more information, see "Using the HTML remote control clipboard to transfer text and files" (452).
- **Settings**: Displays the Settings dialog. For more information, see "Configuring HTML remote control settings" (454).
- **Zoom**: Toggles zoom mode. When zoomed out, the viewer scales the remote session to fit in your browser’s window. If the window size is too small, the scaled session text and other session elements may be hard to see. When zoomed in, scroll bars appear that you can use to see session parts that don’t fit in the window.
- **Exit**: Exits the remote control session and returns to the login screen.

**NOTE**: Currently, File Transfer, Clipboard, Drag and Drop and Chat are not supported on Macintosh devices.

### Using the HTML remote control clipboard to transfer text and files

The HTML remote control clipboard tool lets you transfer text and files from the remote device to your local device. When you add a file or folder to the remote devices clipboard, either with Ctrl+c or a right-click and Copy, that item is added to the remote control clipboard queue.
You can then click the **Clipboard history** button on the remote control toolbar and see a list of items that you’ve added to the clipboard in the current remote control session.

![Clipboard History](image)

By default, the Clipboard History dialog box shows text items on the clipboard. If you add a file or folder to the clipboard, **File List** and **Text List** tabs appear in the dialog box. You can use these tabs to switch between file and text clipboard views.

If you want to transfer text to your local clipboard from the remote device, click the text in the list then click the clipboard button in the top right corner of the Text List tab.

Files that you’ve added to the clipboard appear in the **File list** view. You can click a link to download that file. Note that the downloaded filename changes to “getcbfile”. You’ll need to manually rename the file to match its original filename.

You can also drag and drop files onto remote devices. If you drag the file into a focused Explorer window on a Windows device, the file will be transferred into the folder that is currently displayed in that Explorer window. Otherwise the files will be transferred to the desktop.

### Controlling devices that have multiple monitors with HTML remote control

HTML remote control supports devices that have multiple monitors attached to them. When you remote control such a device, the remote control window only shows the primary display.

The toolbar’s **Monitors** button lets you select the displays you want to see. In the image below, the right monitor is selected on a device with three monitors.
Clicking a monitor will toggle its selection. You can change your monitor selections at any time during a session. If you select more than one monitor, all monitors between your selection will be visible, even if they aren’t selected in the Monitors thumbnail. The monitor thumbnails are generated when the remote control session starts and they don’t dynamically update.

There are two viewing modes when you have multiple monitors selected. The toolbar’s **Zoom** button toggles between them.

- **Unzoomed**: In unzoomed mode, all selected monitors are visible at once. Because of the amount of scaling this requires, the remote view may be very small.
- **Zoomed**: In zoomed mode, the view isn’t scaled. A horizontal scrollbar lets you move among the selected monitors.

### Configuring HTML remote control settings

Generally, the HTML remote control settings match the classic remote control settings. You can still toggle view only, blank screen, lock keyboard and mouse, and so on, along with the performance and hotkey settings.

**To adjust the HTML remote control settings**

1. In an active HTML remote control session, click the **Settings** button on the session toolbar.
2. Adjust the settings you want.
3. Click outside the dialog box to close it and apply your changes.

You can also adjust HTML remote control settings at the HTML remote control login screen by clicking the **Settings** button there. Your setting preferences are stored in a local browser cookie and will be remembered between remote control sessions on that browser.

### General settings

- **Blank screen**: Hides the remote device’s screen so only the person running the remote control viewer can see the screen on the remote device.
• **Lock out keyboard and mouse**: Disables the remote device’s keyboard and mouse. Only the remote control viewer’s keyboard and mouse will work.

• **Auto-hide menu bar**: Hides the HTML remote control toolbar at the bottom of the window. The toolbar reappears when you move the mouse to the bottom.

• **Use 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 will appear in the remote control status dialog on remote devices. However, if auditing is enabled, the audit trail will reflect the real computer or user name, not the one specified in the settings.

• **Keyboard language**: Specifies the keyboard language. Click the desired language in the list.

### Performance settings

• **Suppress wallpaper**: Substitutes a solid color for the remote device’s wallpaper. When you do this, remote control doesn’t have to send wallpaper updates when 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.

• **Grayscale mode**: Switches the session to grayscale mode, halving the amount of data transmitted. This preserves a high-fidelity desktop session.

• **Bits per pixel**: Reduces the amount of color information transmitted. The maximum is 15 bits per pixel, the default. 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. Grayscale mode is usually a better choice if you want to optimize performance and don’t require a color session.

### Hotkey settings

• **Close viewing session**: Ends the current remote control session. The browser returns to the login screen.

• **Send Ctrl-Alt-Delete** (Ctrl+Alt+D): Sends Ctrl+Alt+Delete to the target device.

• **Send Ctrl+Esc** (Ctrl+Alt+E): Sends Ctrl+Esc to the target device.

• **Refresh screen**: Retransmit screen data from the remote computer.

• **Restart computer**: Reboots the remote computer if the remote computer’s remote control agent settings allow it.

• **View monitors**: Shows the monitor selector. Use this if the remote computer has multiple monitors. This is the same as clicking the Monitors toolbar button.

• **Print screen**: Copies a screen shot of the remote control session to the viewer’s clipboard.
- **Screen capture**: Saves a .png screenshot of the remote control session to the browser's default download folder. If the device being controlled has multiple monitors, there is a separate .png file for each active monitor.
Software distribution/Distribution packages/Delivery methods

About software distribution

The software distribution technology in Ivanti® Endpoint Manager powered by Landesk helps IT staff implement controlled automation for fast and efficient software distribution and installation, security and virus update, and application patch management across mixed network environments. The technology is based on a modular, task-based model that can substantially improve overall efficiency in planning, scheduling and managing software distributions. Packages, delivery task types, deployment scripts and target selection are managed separately to increase overall flexibility.

Key Features and Benefits

- **Return code mapping**: Defines return codes to improve application installation accuracy.
- **MSI native support**: Copy and paste MSI command line calls.
- **Simplified work flow**: Makes for easier, faster scheduling of package installations.
- **Simplified bandwidth controls**: Customize configurations appropriately.
- **Task-based modeling**: Separates package building and delivery task types to improve efficiency.
- **LANDesk® Targeted Multicast™**: Distribute large packages to multiple users with minimal bandwidth and without dedicated hardware or router reconfigurations.
- **LANDesk® Peer Download™**: Allows you to access packages already delivered to a subnet.
- **Prerequisite checking and package chaining**: Installs prerequisite packages and enables you to automatically install multiple packages in a single operation.
- **Task scheduler**: Integrates with directory-service and asset-inventory databases to help you easily select targets.
- **Package-agnostic distribution**: Deploys any package type and provides access to multi-file MSI support.
- **Self-service portal**: Reduces help-desk incidents, empowers users to initiate approved installations, and enables faster troubleshooting via detailed histories.
- **Policy-based distribution**: Deploys multiple software packages in a single policy and ensures the packages are available for future updating and reapplication if necessary.

In Endpoint Manager, 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, and so on. 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. **Schedule the distribution job in the Scheduled tasks window** (Tools > Distribution > Scheduled Tasks). Specify the distribution package, the delivery method, the devices that need to receive the distribution package, and when the task should run.

4. When the scheduled time occurs, the scheduler service will start the scheduled task handler which deploys the package using the options selected in the task type. These may include the following:
   - If a policy-supported push or push task type 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 based task type is selected, the package becomes available for download.

5. 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.

6. After the package is processed, the software distribution agent sends the result to the core server, where it’s recorded in the core database.

### Understanding distribution package types

Software distribution supports these package types:

**Bundle**

A collection of software distribution packages and/or bundles that you can schedule and run as if it were just a single package. For more information, see “Using software distribution bundles” on page 461.

**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.

**SWD**

These are packages built with the legacy Ivanti Enhanced Package Builder (installed separately). Although the Enhanced Package Builder is no longer shipped with Endpoint Manager, Ivanti continues to support the distribution of files created with it. They are executable files that have properties that uniquely identify them as software distribution (SWD) packages.

**Actions**

Windows package actions can perform custom operations during package installation. Actions you create in the action interface then get combined into a package that runs a single PowerShell script on targeted devices. For more information, see “Windows package actions” on page 464.

**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.

**Windows Script Host**

Windows Script Host Packages (WSH) are Microsoft Software’s alternative to batch files that 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 can often be created in Notepad, an HTML editor, Microsoft Visual C++, or Visual InterDev.

**PowerShell**

Windows PowerShell scripts are based on Microsoft’s .NET framework and allow you to perform administrative tasks on computers.

**Linux**

These are packages in Linux RPM format. These packages must be stored on a Web share for Linux RPM distribution to work.

**Macintosh**

Any Macintosh file can be downloaded, though Endpoint Manager 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, Endpoint Manager 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.)
Store application

Android mobile

iOS mobile

Universal link

Links are shortcuts to applications. You can link to a distribution package, an executable, or a URL. Links can appear in the client Fuse portal or LaunchPad, on the desktop, or in the Start menu. This package type is new in Endpoint Manager 9.6 and replaces the old LaunchPad link manager tool.

Universal provisioning

Provisioning packages deploy an OS provisioning template that you've previously created in the provisioning tool.

Universal streamed document

Streamed documents are viewable with the new Ivanti Portal Manager on managed devices. A streamed document must be hosted on a UNC or HTTP share that managed devices can access. The streamed document file extension must have an application associated with it that can display that document type. Streamed documents aren't cached locally.

Streamed documents are generally used with package bundles to provide users with additional instructions or information.

Working with distribution owners and rights

In environments where there are many Endpoint Manager users, it can get confusing knowing which distribution packages, delivery methods, and scheduled tasks each user is responsible for. To help with this problem, Endpoint Manager 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” (68).
Using software distribution bundles

A bundle is a collection of software distribution packages and/or bundles that you can schedule and run as if it were just a single package. A bundle can also be used in place of a package. For example, when scheduling a distribution task, you can use bundles in the package order (preliminary, main, and final).

It’s possible to create bundles within bundles, but you can only adjust the installation order for items at the selected bundle’s root level. Each bundle and sub-bundle has its own installation order.

In the bundle properties you can specify that the bundle can’t be scheduled. This is useful for bundle organization and helps prevent accidental deployments of those organizational bundles. For example, you could have a "Microsoft" bundle that contains all of the Microsoft applications you support.

The bundle properties also allow you to insert Reboot and Continue on install failure inter-package actions. A reboot action on a package will reboot the device after that package installs and the bundle then continues where it left off. If it's OK for a particular package to not install correctly, assign it the Continue on install failure action.

A bundle can contain both Windows and OS X application packages. If an application is available on both operating systems, you can provide a package for each operating system in the same bundle. In this case, the bundle will automatically install the correct package for the target device.

To create a bundle

1. Click Tools > Distribution > Distribution packages.
2. In the Distribution packages tree, right-click a category or a bundle in a category, and click New package bundle.
3. Edit the bundle name and click enter.
4. Drag packages and other bundles onto the bundle you created to add them.

To change the package order in a bundle

1. Right-click the bundle you want and click Properties.
2. On the Bundle package settings page, use the Up and Down buttons to reorder the root-level items in that bundle.

To add an inter-package action

1. Right-click the bundle you want and click Properties.
2. On the Bundle package settings page, in the right pane select the package needing an inter-package action.
3. In the left pane under Inter-package actions, select the action you want and click >>.
Using MSI distribution packages

Endpoint Manager supports MSI installation with full status reporting and MSI package recognition. The MSI distribution package type is the Endpoint Manager 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, Endpoint Manager leverages the MSI API calls. MSI installations use two different types of command-line parameters:

- Option parameters
- Property reference parameters
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 box, 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: https://support.microsoft.com/en-us/kb/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: https://support.microsoft.com/en-us/kb/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 Endpoint Manager, running an MSI silently is automatically handled under the Install/Uninstall options for a distribution package. To run an MSI silently, go to the Install/Uninstall options page for the desired distribution package 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 distribution package.

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.

**Handling reboots with an MSI installation**

Endpoint Manager handles MSI reboots using the Reboot page in the delivery method properties. Ivanti 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 to reboot. It is important to know that MSIs support custom actions. If a custom action initiates a reboot, Endpoint Manager 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.

**Windows package actions**

Use Windows package actions to perform custom operations during package installation. Actions you create in the action interface then get combined into a package that runs a single PowerShell script on targeted devices. Available actions include the following:

- Copy, rename, delete, or move a file
- Create or delete a directory
- Stop, start, or restart a Windows service
- Add, delete, or update a registry entry
- Connect or disconnect a UNC share
- Launch an executable
- Pop up a window
- Custom PowerShell commands that you've created
To create a Windows action package

1. Click **Tools > Distribution > Distribution packages**.
2. Right-click the **Distribution packages** category you want and click **New Windows package > Actions**.
3. In the **Windows actions properties** dialog box **Actions** page, click **Add**.
4. Select the action you want and click **OK**.
5. Configure the action properties.
6. Add and configure other actions if necessary.
7. Click **Save**.

Update 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, Endpoint Manager 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 Endpoint Manager, 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 package hash**. This can take a few minutes on large packages.

Run distribution 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. Create a scheduled task for an existing package.
2. In the Scheduled tasks window, right click the task for that package and click Properties.
3. Open the Task settings page.
4. In the Download options section, click Run from source (execute on share).
5. Click Save.

Updating package run-as credentials

Each software distribution package has an Accounts properties page. The default is to use the LocalSystem account to distribute the package. You can also choose to use the current user’s account.

The final accounts option is to Run as a specified user and provide that user’s credentials. If you have a lot of packages that use run-as and you need to update those credentials, it can be tedious editing each package individually. In this case, use the Bulk package credentials update tool.

This tool shows a list of all packages and lets you provide credentials. You can select the packages you want to use the new credentials. Shift and Ctrl multiselection is supported. Only checked packages will have their credentials updated.

To bulk update run-as package credentials

1. Click Tools > Distribution > Software distribution.
2. On the toolbar, click the Bulk package credentials update button.
3. Enter the new credentials.
4. Select the packages that should use the new credentials.
5. Click Update.

Processing software distribution 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 Endpoint Manager 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.

- **REMMKDIF:** 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.

### HTTP and UNC paths in scripts

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]
REMEEXEC=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=http://<web server>/packages/test package.exe -g={6DD454C0-11D3A0D1-a000B3B5-9BACB9C9CFC6D-9CE3504B01A0D4B2F0829F08} -Ac -Ab
```

**UNC path script file:**

```
; This file was generated by Desktop Manager

[MACHINES]
REMEEXEC=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=\\sample_core\onefile\test package.exe -g={6DD454C0-11D3A0D1-a000B3B5-9BACB9C9CFC6D-9CE3504B01A0D4B2F0829F08} -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:

```ini
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe
/p="http://computer_name/95Packages/Acro32_11D3766F-0F9751AC966F808-66E3BC2DF01A0D4B2F88670DE4"
/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.

**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 Ivanti 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 each 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 Ivanti 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 dialog boxes.

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 box, 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 box. Checking a dependency in this dialog box tells software distribution to not prompt you about it again. You can check dependencies you know are installed on managed devices. This dialog box 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.

**Understanding the available distribution delivery task types**

Once you schedule a package for distribution, you can use one of these delivery task types:

- **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.
- **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.

- **Push**: The packages may be multicast out to the managed devices. The core server then initiates package installation at the managed devices.

- **Multicast (cache-only)**: Copies one or more files to the local distribution cache folder but doesn't install the file or do anything else with it. This option can be useful when you know users will need to install a package soon, and you don't want them to have to wait for the download.

### Distribute 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 devices must have the software distribution agent installed.

NOTE: As of Ivanti® Endpoint Manager powered by Landesk 9.6, the Delivery methods tool is only used for distribution to devices running pre-9.6 device agents. Now you can choose a delivery task type directly from the task’s Task settings page. Devices will then automatically optimize the delivery method details.

There are two main steps required to distribute a package to devices.
**Step 1:** Create the package you want to distribute.

![MSI properties window](image)

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)**

**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**

Enter command line or select options above and edit command line for MSI package:

`/quiet /norestart`
Step 2: Schedule the package for distribution and customize the delivery task type if necessary.

To create a distribution package

1. Click **Tools > Distribution > Distribution Packages**.
2. From the **New** drop-down menu, click the package type you want to create.
3. In the configuration dialog box, enter the package information and configure the options as needed. Note that you must enter the package name, description, and primary file. For more information about each page, click **Help**.
4. Click **OK** when you’re done. Your script appears under the tree item for the package type and owner you selected.
To schedule a distribution task

1. Click **Tools > Distribution > Scheduled tasks**.
2. In the tree, click the **Scheduled tasks** category you want.
3. Click the **New** toolbar button and click **Scheduled task**.
4. On the **Distribution package** page, select the distribution package you created.
5. On the **Task settings** page, select the distribution task type you want to use.
6. Click **Save** to save your changes.
7. 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.
8. From the task’s shortcut menu, click **Properties**.
9. The **Targets** page shows the devices that will receive this task.
10. On the **Schedule task** page, enter the task name and the task schedule.
11. Return to the **Overview** page and confirm the task is properly configured.
12. Click **Save** when you’re done.

View the task progress in the **Scheduled tasks** window.

About file downloading

Software distribution has several methods for getting a file down to the device for installation. These include:

- Obtaining the file from the multicast cache
- Obtaining the file from a peer
- Obtaining the file from a preferred server
- 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 stored at `C:\Program Files (x86)\LANDesk\LDClient\sdmcache`.

The structure of files in the cache is identical to the structure of the files on the web or network server, which allows multiple packages to have files with the same name and not cause problems.

If the file isn’t in the cache, SDClient typically attempts to download the file from a peer in the network. You can configure the distribution agent settings to require a peer download.
If the file can’t be obtained from a peer, SDClient downloads the files directly from the UNC or URL source. Preferred servers are the best location for package files. For more information, see "Preferred servers and content replication overview" (963). Preferred servers help ensure that clients use network credentials that allow them access to the distribution package files. If the file to be downloaded is URL-based, SDClient downloads the file from the website.

In either case, SDClient puts the file in the multicast cache, then processes the downloaded file.

When a file is downloaded into the cache, it remains there for several days but is eventually deleted from the cache. The amount of time that the file remains in the cache is controlled by the delivery method used when deploying the package.

**About byte-level checkpoint restart and dynamic bandwidth throttling**

Endpoint Manager 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 (x86)\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.

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.

**Using accelerated push distribution**

Accelerated push was added in Ivanti® Endpoint Manager powered by Landesk 9.6. Enabling it greatly speeds up distribution tasks. The default push distribution task type builds target lists of up to 241 devices and processes these devices one target list at a time, waiting until jobs complete before moving on to devices in the next target list.
Accelerated push distribution makes this process asynchronous. As the core discovers and communicates with target devices, it tells them what to do and then moves on to the next targeted device without waiting for the job to complete. This discovery and communication process uses multiple processor cores and threads. Each device then processes the job on its own and sends job status to the core server when necessary.

Accelerated push scheduled tasks use a single target list internally, and by default accelerated push processes up to 64 targets concurrently from the list. You can adjust this if necessary based on your core server resources. Generally you won’t need to change the default.

Accelerated push also works well with multicast. Accelerated push contacts target devices much more quickly than normal push jobs, so a multicast distribution can include even more devices at once. The device acting as the multicast representative in each subnet waits the configured amount of time before beginning the multicast and all other devices using that representative will receive the multicast once it starts. Any devices late to the multicast will still get what was left of the multicast when they joined and then they will backfill what they missed from their peers or the source.

Supported task types:
- Policy-supported
- Policy
- Push

Supported download options:
- Run from source (execute on share)
- Download and execute
- Pre-cache—just download the package or bundle without installing.

Supported platforms:
- Mac OS X
- Windows

**Using self-organizing multicast with software distribution**

Ivanti self-organizing multicast technology makes it possible to distribute large packages to many users across the network with a minimum of network traffic. Self-organizing 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.

Self-organizing multicast is designed to work with your existing software distribution packages. When you use self-organizing multicast, you can easily distribute software, even in WAN environments with multiple hops and low connection speeds. Self-organizing multicast uses HTTP for delivery from a Web site to a volunteer subnet representative. Endpoint Manager’s inventory scanner provides all the subnet information to the multicast service.
When compared to conventional software distribution methods, self-organizing 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.

Ivanti® Endpoint Manager powered by Landesk supports multicast for Windows and Macintosh OS X distributions. Additionally, you can multicast OS provisioning images.

Here is the self-organizing multicast workflow:

1. A task using multicast begins and targeted devices look for an existing multicast session for that task on their subnet. If there isn’t one, a device offers to become the multicast domain representative for that task. The representative on each subnet starts downloading.
2. Other devices receive the task, see that there is an existing multicast session for that task, and wait for the multicast domain representative’s session start delay to pass (the default is one minute). The multicast domain representatives begin multicasting to their subnets.
3. Devices receiving the task after the multicast session has begun join the multicast and start caching multicast data. At the end of the multicast they ask their peers for the parts they missed.

To enable multicast in the Distribution and Patch agent setting

1. Click Tools > Security and Compliance > Agent settings.
2. In the Agent settings tree, right-click Distribution and Patch and click New, or double click an existing Distribution and Patch agent setting.
3. On the Network settings page, select Use multicast. If necessary change the Delay. This is how long the device that volunteered to be a multicast domain representative for a task will wait before multicasting the distribution job to peers on its subnet.
4. Save your changes.
5. Devices already using the distribution agent setting you modified will receive your changes the next time they run the vulnerability scanner, usually within 24 hours.

You can also create a new distribution agent setting and associate it with tasks that you want, temporarily overriding the device's default distribution setting. Do this from the task's Agent settings page.

Copying files to the local distribution cache folder

You have the option of copying one or more files to the local distribution cache folder. This doesn’t install the file or do anything else with it. This can be useful when you know users will need to install a package soon and you don’t want them to have to wait for the download.
To copy files to the local distribution cache folder

1. Right-click package you want copied and click Create scheduled task.
2. In the scheduled task window, right-click the task you created and click Properties.
3. On the Task settings page in the Download options section, click Pre-cache (download for a future task or portal-initiated action).
4. Finish scheduling the task.

Assigning distribution 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, Endpoint Manager 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, Endpoint Manager would indicate failure.

Vendors maintain lists created by product developers of all possible return codes and the specific outcome that the codes indicate. Now Endpoint Manager 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.

In addition to using this feature with third-party vendor applications, return code templates can also be created for proprietary applications written by internal developers. Endpoint Manager 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.
There are two default templates included with Endpoint Manager:

- **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.

### Assign distribution 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.

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.
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 Package return code mappings 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 box, 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.

Export and import distribution 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.

Troubleshooting distribution failures
Software distribution lets you 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 could cause problems for 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 rollouts occur should be based on the variety of devices the enterprise has and the load your help desk can handle.

In 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.
For more information see this community article on troubleshooting software distribution:
https://community.landesk.com/support/docs/DOC-5096.

**Software distribution SDCLIENT.EXE command-line switches**

Software distribution is facilitated by a deployment script. SDCLIENT.EXE manages the packages using command-line switches from the script file that are passed to the application.

For more information, see this community article on SDCLIENT.EXE command-line switches:
https://community.landesk.com/support/docs/DOC-13759.
Portal Manager

About the Portal Manager

Ivanti Portal Manager delivers apps, documents, and links to end users so they can install items that are approved for use in your organization or required for that user’s hardware.

When the end user launches Portal Manager, it synchronizes with the policy server. If there are any required policy-based tasks that haven’t yet run on the user’s device, these tasks are initialized without any further action from the end user.

The end user can also choose from recommended and optional policy-based tasks that have been added to Launchpad.

When an end user opens the Portal Manager, the following dialog displays the available options.

Installing the Portal Manager

The Portal Manager is installed as part of an agent configuration that you define and then deploy to managed devices. You also need to configure agent settings for Portal Manager before deploying the agent.

NOTE: To implement the Portal Manager on a managed device, the device must have Microsoft .NET 4.0
You can install this as part of the agent deployment process. If you don’t want to require .NET 4.0 to be installed, use the legacy Desktop Manager, which doesn’t have this requirement.

Related topics

"Configuring the Portal Manager” (483)

"Adding applications to the Portal Manager” (484)

Configuring the Portal Manager

Ivanti Portal Manager is configured and deployed as part of the standard Ivanti agent.

The Portal Manager lists the available applications, documents, and links. You can change how these are displayed on managed devices by changing the Portal Manager agent configuration.

To configure how the Portal Manager displays applications

1. Click **Tools > Configuration > Agent configuration**.
2. Create a new configuration, or double-click a configuration to edit it.
3. Expand **Distribution and Patch** in the configuration’s tree structure and click the **Portal Manager** page.
4. Click the **Configure** button. Either select an existing agent configuration and click **Edit**, or click **New** to create a new one.
5. On the **General** page, select options that determine how end users can interact with the Portal Manager.
6. On the **Applications** page, select the applications you want to appear in the Portal Manager. Click **New** to define applications. Choose from items in the **Available applications** list and click **>>** to show them in the Portal Manager.
7. On the **Branding** page, you can customize the title color, taskbar icon, the corporate logo, and the background image that are displayed in the Portal Manager.
8. When you’ve finished, click **Save**. Select the settings and click **Use selected**. You are returned to the agent configuration dialog.
9. Under **Shortcut configuration**, select where on the end user’s device you want to display a shortcut to the Portal Manager.
10. Select **Run Portal Manager when the user logs on** if you want the Portal Manager to always open when the end user logs on to the device. This can be useful if you want to make sure that required policies are downloaded in a timely way.
11. When you’ve finished the configuration, click **Save**. You can then schedule the agent to be deployed to selected devices.
Related topics

"Adding applications to the Portal Manager" (484)

Adding applications to the Portal Manager

The Portal Manager displays two applications by default: LaunchPad and Task History. You can add other applications that display on the Portal Manager (rather than in the list of LaunchPad apps).

To add applications for use in the Portal Manager

1. Click **Tools > Configuration > Agent configuration**.
2. Create a new configuration, or double-click a configuration to edit it.
3. Expand **Software distribution** in the configuration’s tree structure and click the **Portal Manager** page.
4. Click the **Configure** button. Either select an existing agent configuration and click **Edit**, or click **New** to create a new one.
5. Click the **Applications** page, and then click the **New** button.
6. Type the application name and a tooltip that displays when the end user points to the application.
7. Select the application type.
8. Specify the path to the application.
9. For executable apps, specify any parameters.
10. For WPF DLLs, specify any class names.
11. Click **Browse** to select an image.
12. When you’ve finished, click **Save** to add the application to the **Available applications** list.
Application policy management

About policy-based management

Policy-based management helps you easily manage sets of applications on groups of devices. Like any other scheduled task, policies require:

- A distribution 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.

The task flow for policy-based management is as follows:

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 "About software distribution" (457).
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 that the policy-based Delivery methods dialog box 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.

### Create a policy-based distribution

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.

#### To create a policy-based distribution

1. In the console, click **Tools > Distribution > Delivery methods**.
2. Right-click either **Policy-based distribution** or **Policy-supported push distribution**, then 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.

### Adding policy 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.

### 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. Queries are stored only in the core database. For more information on queries, see "Database queries" (369).

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, 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.

In order to target a device from LDAP, each Windows 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 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" (371).

**Understanding how scopes affect policy target visibility**

Multiple scopes can filter the policy-based management target details pane for a target list. 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 Endpoint Manager 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.
Software license monitoring

Audit and compliance data in the dashboard

The dashboard pages are designed to give you quick access to useful data that is calculated from your product and license information, such as current summaries of important audit and license-compliance data.

Dashboard pages display report summaries with charts and Advisor data. In the following example, the chart displays the five best opportunities to reclaim (or “harvest”) licenses that are not being used. The Advisor box at the bottom of the console shows the total number of installed products that have never been used.

The Advisor section gives you a quick summary of data. Charts show more details, and you can click through sections of a chart to see the details for specific products.

Viewing details of chart data

When you point to a section of the chart, a box shows the data for that section.
Click a chart section to view a list of related data. For example, when you click a product bar in the harvest opportunities chart, you’ll see a list of devices with that product installed.

![Image of chart showing software harvest opportunities]

![Image of device list for Adobe AIR 2]
Viewing details of Advisor data

When the Advisor box contains data, click the number to open a full report of the data's source. In the example above, the Advisor reports the number of installations that have never been used. Click the green number to open a report that shows which products are counted in that total.
Never used installations
Products that have been installed, but never used.

Total number of never used installations: 51

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Quantity</th>
<th>Never Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7 Enterprise Edition, 64-bit</td>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>Adobe AIR 2</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>Microsoft® Windows® Operating System</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Firefox 3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Adobe AIR 1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

4/19/2012

Report generated by LANDesk® Management Suite 9
Exporting data to CSV and creating reports

When you click a chart to view the detailed data, or any time you are on a product detail page, you can export the data as a CSV file or create a report of it.

To export data in CSV format

1. Click a section of a chart.
2. In the new window, select the devices that you want to include in the exported data. (Click in the list and press Ctrl+A to select all the devices.)
3. Click the Export button.
4. Specify the location to save the CSV file in, and then click Save.

To create a report of selected data

1. Click a section of a chart.
2. In the new window, select the devices that you want to include in the report. (Click in the list and press Ctrl+A to select all the devices.)
3. Click the Report button.
4. On the report viewer toolbar, select a format to save the report in, and then click the Export button.
5. Specify the location to save the report in, and then click Save.

Software license monitoring overview

Software license monitoring (SLM) gives you the tools to manage your organization’s software assets so that you can track product usage, monitor license compliance, and ultimately control costs.

As an IT administrator or software asset manager, you may find it challenging to track products installed on numerous devices across a network. You run the risk of not only installing more products than you’ve purchased licenses for, but also of purchasing too many licenses. You can avoid these problems by using the SLM console to monitor and report on product licenses and usage across your organization.

The SLM console

The SLM console opens in a web browser. It has four distinct pages to view data (Dashboard, Products, Administration, and Reports).

The Dashboard pages display summary charts of key product and license data. These are useful for audit planning and optimizing your use of licenses.
The **Products** pages display detailed data for products that are installed on managed devices. These pages include license data that is used to calculate license compliance in your organization, as well as reclamation and allocation data. Reclamation data shows tasks set up to take unused product licenses and reassign them to devices that need them. Allocation data tracks the cost of providing IT support to groups across your organization.
As you work in the SLM console, you’ll spend most of your time in the **Products>Monitored** page, which displays the products you want to actively monitor. After you’ve moved important products into this view, the **Discovered** view is where you’ll look for new products that might need your attention. The products you don’t need to monitor can be moved to the **Ignored** view so they’re out of your way.

If you’re not sure where a product is, open the **Products>All installed products** page and search for it. You can then move the product to the appropriate view (Monitored or Ignored).

**NOTE:** The Ivanti® Endpoint Manager powered by Landesk Windows agent can detect and record the usage of Microsoft Metro-style apps (also known as Windows Store apps). As a result, you can now track and monitor that usage in SLM.

Use the **Administration** pages to set up computer groups, normalized manufacturers, and other defaults to customize the data appearing in the other SLM console pages.

Use the **Reports** page to run any number of predefined or customized reports that show license and product data for devices across the network.

**Opening the console**

Users with a role definition that includes software license monitoring can view and edit data in the SLM console. Administrative users are assigned this role by default. Other users can be assigned View and Edit permissions for the software license monitoring role.

For information about changing user permissions, see “Managing roles” (58)

**IMPORTANT:** The browser you use to view the SLM console must have pop-up blocking turned off. If it’s turned on, you may be unable to view dialogs that open from the SLM console. If you have problems viewing items, make sure that your browser’s pop-up blocking is turned off.

**Features**

SLM includes these features:

- Easily accessible reporting on product usage and license compliance, including number of times each licensed product was launched, last date used, and total duration of application usage.
- Product license sharing. 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 configured license parameters, including purchase and shipping 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.
- Passive, low-bandwidth monitoring. The software monitoring agent passively monitors product usage on devices, using minimal network bandwidth.
- Mobile device support. The agent monitors usage for mobile devices that are disconnected from the network and then sends data to the core server when the device is reconnected.
- Automatic discovery scans for installed products on managed devices that gather data based on the files associated with those products.
- License reclamation and allocations. You can set up a process that runs a reclamation task on licenses, freeing them for use on other devices. Allocate licenses to computer groups to establish chargeback costs for the IT support you provide.

**Getting started**

To begin using the SLM console to monitor product installation and license usage, you'll first need to do these general tasks:

**Ensure the Inventory service is configured and running**

Software license monitoring requires the Ivanti agent to be running on devices you want to manage. The agent gathers inventory data from managed devices about which products are installed and how often they are run. This data is delivered to the core server every time a software inventory scan is completed, by default once a day.

After inventory data is collected, product data appears in the SLM console's Products > Discovered page. As more inventory data is added, new product data is added to the Discovered view. As you review this data, you may find that some products are not found or not recognized correctly. You can use the SLM console to check for specific products, and you can add or correct product definitions if needed.

**Define device groups and queries**

If you want to monitor products on groups of devices (static groups) or by using queries (dynamic groups), first create them in the Endpoint Manager network view. These groups and queries will then be available in the SLM console, making it easier for you to review installed products organized by location, organizational group, hardware type, or any other criteria.

**Add product license data**

To monitor your organization's compliance with product license terms, you'll need access to accurate license data. You can add this data manually, or import data from another source such as Ivanti Data Analytics. Once you’ve added information about your licenses, such as how many seats you have purchased, purchase date and expiration dates, type of license, and how the licenses are consumed, you can begin to review compliance statistics and reports that compare the license data with actual product usage.
Choose which products to monitor

When you first open the SLM console, all products newly discovered by the inventory scanner are found in the Products>Discovered page. Select products from that list that you want to monitor and move them to the Monitored view. Monitored products can be linked to your license data and tracked in reports that show you how well your licenses match actual product usage. Some products may not be important to you, so you can move them to the Ignored view, excluding them from license compliance calculations.

Edit product details

Once a product is in the Products>Monitored page, you can edit its details, set up license allocations and chargeback costs, and define reclamation tasks.

Create reports

As you review the data associated with product and license compliance, you can generate a report of what’s displayed. Reports can be formatted as CSV, HTML, PDF, XML, DOC, XLS, or image files. Once license and product data is established in the database, you can also use the Endpoint Manager reports tool to generate predefined reports showing all aspects of license and usage data.

Audit and compliance data in the dashboard

The dashboard pages are designed to give you quick access to useful data that is calculated from your product and license information, such as current summaries of important audit and license-compliance data.

Dashboard pages display report summaries with charts and Advisor data. In the following example, the chart displays the five best opportunities to reclaim (or "harvest") licenses that are not being used. The Advisor box at the bottom of the console shows the total number of installed products that have never been used.
The Advisor section gives you a quick summary of data. Charts show more details, and you can click through sections of a chart to see the details for specific products.

**Viewing details of chart data**

When you point to a section of the chart, a box shows the data for that section.
Click a chart section to view a list of related data. For example, when you click a product bar in the harvest opportunities chart, you’ll see a list of devices with that product installed.

**Viewing details of Advisor data**

When the Advisor box contains data, click the number to open a full report of the data’s source. In the example above, the Advisor reports the number of installations that have never been used. Click the green number to open a report that shows which products are counted in that total.
Never used installations
Products that have been installed, but never used.

Total number of never used installations: 51

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Quantity</th>
<th>Never Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 7 Enterprise Edition, 64-bit</td>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>Adobe AIR 2</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>Microsoft® Windows® Operating System</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Firefox 3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Adobe AIR 1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

4/19/2012

Report generated by LANDesk® Management Suite 9
Exporting data to CSV and creating reports

When you click a chart to view the detailed data, or any time you are on a product detail page, you can export the data as a CSV file or create a report of it.

To export data in CSV format

1. Click a section of a chart.
2. In the new window, select the devices that you want to include in the exported data. (Click in the list and press Ctrl+A to select all the devices.)
3. Click the Export button.
4. Specify the location to save the CSV file in, and then click Save.

To create a report of selected data

1. Click a section of a chart.
2. In the new window, select the devices that you want to include in the report. (Click in the list and press Ctrl+A to select all the devices.)
3. Click the Report button.
4. On the report viewer toolbar, select a format to save the report in, and then click the Export button.
5. Specify the location to save the report in, and then click Save.

Viewing the audits dashboard

The Dashboard>Audits page includes reports that are useful when you’re preparing for an audit of your product license usage.

Report: Top total installations

This report lists the five products with the most installations on devices in your organization. Counted are the actual installations, not the number of devices, because you may have more than one installation on a device.

Advisor: Products and licenses with audit flags

This report alerts you to issues that could be flagged during a product license audit, such as problems with license documentation and products that have not been dispositioned (moved to the Monitored or Ignored product views). The Advisor counts items such as the following:

- Licenses without a purchase order
- Products without licenses
- Discovered products that have not been dispositioned
- Licenses without a manufacturer invoice

Click a number for any item to view a full report of that item.

NOTE: You’ll also find predefined reports for individual audit flag items on the software license monitoring Reports page.

**Viewing the compliance dashboard**

The **Dashboard>Compliance** page includes reports that show you products that are out of licensing compliance, as well as an estimate of the costs to ensure those installed products have valid licenses.

**Report: Top out-of-compliance by installation**

This chart shows up to five products that have the highest number of unlicensed installations.

**Report: Top out-of-compliance by true-up costs**

This chart shows the products that have the highest cost to bring them into compliance, determined by the number of unlicensed installations multiplied by the unit cost associated with the product.

**Report: Top out-of-compliance by manufacturer**

This chart groups products by manufacturer and shows which of those products have the most unlicensed installations. Use this report during an audit when you need to verify that installations match the licensing compliance terms of a manufacturer.

**Advisor: Estimated compliance costs**

The total estimated cost to bring installed products into compliance with license requirements, determined by the number of unlicensed products multiplied by the unit cost associated with each product.

**Advisor: Products out of compliance**

The number of products that are not in compliance with associated licenses. Click the number to view a complete list of products that are out of compliance.

**Viewing the license optimization dashboard**

The **Dashboard>License Optimization** page includes reports that estimate the savings you can gain by removing unused software from devices in your organization. These reports focus on installed products that have never been used or have not been used for a specified length of time.
NOTE: Products are considered “never used” when a value of 0 is returned in the inventory data for the amount of time the product has run. However, it is possible that a product is installed and the person using it has only launched the application one time and then closed it in less than one minute. In this case, the product will still show in the dashboard and in reports as “never used.”

Report: Estimated savings from never-used applications
This report lists the five never-used products that would save your organization the most if you uninstalled them from devices. This is based on the number of never-used product installations multiplied by the unit cost associated with the product.

Report: Top 5 software harvest opportunities
This report lists the five products with the highest number of never-used or infrequently used product installations. It does not estimate costs, but it lists the number of devices with each product unused within a certain number of days (31-60, 61-90, over 90, and never used).

Advisor: Number of installations never used
This report lists each product with the total number of installations that have never been used.

Monitoring software usage
The Ivanti® Endpoint Manager powered by Landesk software monitor scan runs when you schedule regular inventory scans. It monitors executable files that are running and compares product information on each device with the names and file sizes of executable files stored in the database.

Two other inventory scans help complete the picture with other data about products. These scans look at the Windows registry, uninstall keys, .msi files, shortcuts, and GUIDs to identify products. All the scan data is then compared to give as complete a picture as possible of what products are installed on each managed device.

The software license monitoring (SLM) console displays this summary of data in the Products view. Even if you don’t have license data available, you can view this product data to find out on how many managed devices a product has been discovered.

NOTE: The Ivanti® Endpoint Manager powered by Landesk 2016 and newer Windows agent can detect and record the usage of Microsoft Metro-style apps (also known as Windows Store apps). As a result, you can now track and monitor that usage in SLM.
Monitoring and ignoring products

When you first open the SLM console, all newly discovered products are found in the Products>Discovered page. As you manage product and license usage, you can choose which products are important for monitoring. Products you want to track can be moved to the Monitored view. Some products may not be important to you, so you can move them to the Ignored view, which leaves them out of license-compliance calculations.

To monitor a product

1. Click Products > Discovered.
2. Use the Search box to find the product.
3. Click the product. On the toolbar, click Actions > Move to > Monitored.

The product is now listed in the Products>Monitored page.

NOTE: You can also right-click a product and click Move to > Monitored.

To ignore a product or product group

1. Click Products > Discovered.
2. Use the Search box to find the product.
3. Click the product. On the toolbar, click Actions > Move to > Ignored.

The product is now listed in the Products>Ignored page.

NOTE: You can also right-click a product and click Move to > Ignored.

Filtering usage data that devices send

By default, managed devices send usage data for all monitored applications. If you only want usage data for specific files, follow the steps below.

To monitor usage only for specified files

1. In the Endpoint Manager console, click Tools > Reporting / Monitoring > Manage software list.
2. In the Inventory tree, click Settings and double-click Usage files in the settings list.
3. Click New and type the filename you want. Press the Enter key when you’re done. Repeat until you’re done adding files.
4. 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 **Usage files** list is blank, usage data will be sent for all monitored products. You can disable usage monitoring entirely from the **Inventory settings** agent setting.

Core synchronization can include usage file settings.

**Find a product**

In any of the Product views, a search box helps you find products quickly. You can search with a minimum of two characters, viewing results that match your string in the Product or Manufacturer columns.

**To use the search box to find a product**

1. Click **Products** and open one of the views (Monitored, Discovered, Ignored, or All).
2. In the **Search** box, type at least two characters and press **Enter**. The list contains any product or manufacturer with the string you entered.
3. Select one or more list items and either click a toolbar button or right-click the items to act on them. You can drag the items to another view to move them.
4. To see all products in the list again, click the **X** in the search box to clear the search.

**Advanced product search**

Filter a Product view's list by selecting a manufacturer, product, or computer group as a filter. You can use one or more of these filters to display a smaller number of products in a list. These filters are found in the column to the left of the product list.

- Select a **manufacturer** (or normalized manufacturer) to display only products that are associated with that manufacturer.
- Select a **product** (or normalized product) to display only products that match a product name.
Select a **computer group** to display only the products that are installed on devices in that group. This is useful to find products when you know they are installed on a certain group of devices in your organization.

**To filter a product search by manufacturer**

1. Click **Products** and open one of the views (Monitored, Discovered, Ignored, or All).
2. In the column to the left of the list, click **Select manufacturers**.
3. Type at least three characters in the manufacturer name box. Matching names are listed in the **Search results** box.

   ![Select Manufacturers dialog box](image)

4. Select the manufacturer names you want to use as filters, and then click **OK**.

**To filter a product search by product name**

1. Click **Products** and open one of the views (Monitored, Discovered, Ignored, or All).
2. In the column to the left of the list, click **Select products**.
3. Type at least three characters in the product name box. Matching names are listed in the **Search results** box. You can also specify strings to exclude from the search results. To do this, type one or more strings separated with a space in the **Product name does not contain** box. This can help you reduce the number of search results.

![Select Products dialog box](image)

4. Select the product names you want to use as filters, and then click **OK**.
To filter a product search by a computer group

1. Click **Products** and open one of the views (Monitored, Discovered, Ignored, or All).
2. In the column to the left of the product list, click **Computer group** and select a computer group.

   ![Computer Group Filter Screenshot]

   The list changes to display only products installed on the devices in the group you selected.
3. To remove the filter and view all products, click **Reset**.

   ![Reset Button]

**View all installed products**

After you have separated products into the **Monitored** and **Ignored** product views, you may need to find a product but be unable to locate which group it is in. You can search through all products that have been discovered by using the **All installed products** view.

To view all installed products

1. Click **Products > All installed products**.
2. Use the search box or filters to find the product you want.
3. To determine which product view contains the product, look at the **Status** column to see whether the product is monitored, discovered, or ignored.
**View all devices with a product installed**

When you look at any of the product views or at the dashboard charts, you can view a list of all devices that have a product installed. You can create a printable report of this list or export the data as a CSV file.

**To view devices for a product in a product list**

1. Click **Products**, and then click a product view (Monitored, Discovered, Ignored, or All installed products).
2. Find the product using the **Search** box or **Select products** link.
3. Double-click the product name. A list of devices is displayed in a new window.
4. To export a list of devices in CSV format, select the devices and click the **Export** button.
5. To create a report of the devices, click the **Report** button.

**To view devices for a product in a dashboard chart**

1. Click **Dashboard**, and then select one of the dashboard options (Audits, Compliance, or License optimization).
2. Click a segment of a chart that represents a product. A separate window opens with a list of devices.
3. To export a list of devices in CSV format, select the devices and click the **Export** button.
4. To create a report of the devices, click the **Report** button.

**Edit a discovered product**

1. Click **Products > Discovered**.
2. Find the product using the **Search** box or **Select products** filter.
3. Select the product and click the **Edit** button on the toolbar.

   The **Edit product details** dialog opens; some items are read-only and some items are editable.
4. Under **Status**, select **Monitored** or **Ignored** to list this new product in one of the product views.
5. Click **Installation detection**. Note that all options are read-only.
6. Click **Usage detection**. You can add files that indicate the product is being used.
7. Click the **Add (+)** button. In the **Add files** dialog, you can select an existing filename (one that exists in the inventory database), or you can click **Define new file** and specify the filename, size of the file, and version number for the product file. Repeat this for every product file you want to use to determine when the product is being used. When you have finished, click **OK**.
8. Click **Unit price**. If the options can be edited, select a method for calculating the unit price:
   - Select **Use automatically calculated unit price** if you have multiple licenses for the product with different unit prices. If you select this option, the unit price is an average of all unit prices from the different licenses.
   - Select **Specify a unit price** if you want to use the same unit price for all calculations. For example, if you have two licenses with different unit prices for the same product and you want to use the higher price for calculations, you can specify that unit price here.

9. If you add product information that will affect license and usage calculations, such as when a product is associated with a license that you are actively monitoring, select the **Calculate compliance after save** check box to initiate a recalculation so compliance reports stay up to date.

10. When all information is complete, click **Save**.

You can also set up license allocations or a reclamation process for this product. For more information, see "Allocating licenses and chargeback costs to a computer group" (543) and "Reclaiming product licenses" (537).

### Edit product details

After a product appears in one of the Product views (Monitored, Discovered, Ignored, or All), you can edit its details. Generally, you'll want to edit only the details of products you're actively monitoring and using in license-compliance calculations. These products appear on the **Products>Monitored** page.

Product details are a mix of read-only data or data you enter manually and include the following:

- **Definition**: The product name, version, and manufacturer (read-only), as well as the product status that you can change (Monitored, Discovered, or Ignored).
- **Installation detection**: The files associated with detecting the product on devices (read-only). If you've created a custom product, these options are editable. For more information, see "Specify files to detect product installation and usage" (512).
- **Usage detection**: Additional files you can add that indicate the product is being used on devices. For more information, see "Specify files to detect product installation and usage" (512).
- **Unit price**: The cost of licenses for the product used in software license monitoring's calculations. If the unit price is automatically calculated, it's an average of all unit prices from different licenses. If you specify a unit price, software license monitoring will use that price for all licenses of the product. For more information, see "Specify a unit price for a monitored product" (511).
- **Allocations**: If you have defined a computer group as an allocation unit, you can charge back the costs of IT support for product licenses that the group is using. For more information, see "Allocating licenses and chargeback costs to a computer group" (543).
• **Reclamation**: A process you can set up that runs a reclamation task on product licenses, freeing them for use on other devices. For more information, see "Reclaiming product licenses" (537).

### Specify a unit price for a monitored product

Software license monitoring (SLM) includes several different calculations related to license usage in your organization. For example, the Compliance dashboard includes an estimate of the cost to bring installed products into compliance with your license terms.

For every product that is monitored, you can specify the unit cost that is used in these calculations. The cost you specify may be different than the cost that is automatically calculated.

In situations where you have one license for one product, you can use the automatic calculation that takes the total price of the license and divides it by the number of licenses.

In situations where you have more than one license for a product, you might have different unit costs based on the terms of the license. For example, if you have purchased a license for one version of a product and then purchased a new license for a newer version, the newer product may cost more. If you can use these licenses for both the older and newer version of the product, you’ll need to determine which price represents the actual cost you want to use in calculations.

There are two options for specifying a unit price:

• **Use automatically calculated unit price in all calculations**: If you select this option, calculations are based on the license data for the product. If there is one license, the unit price is calculated by dividing the total cost by the number of licenses. If there are multiple licenses for a product, the unit price is the average of the unit cost of all licenses for the product (all total costs divided by the number of all licenses).

• **Specify a unit price for use in all calculations**: If you select this option, the price you enter replaces any automatic calculations for the product. For example, if you have several different licenses for a product, you can specify the current price per license because that is the price you would pay to add new licenses.

If you find calculations in the Dashboard that seem incorrect, you should check that all licenses for a product have correct cost information entered. You can then decide whether to change the unit price for the product to accurately represent the cost of licenses for the product.

---

**NOTE:** If you’re using the French-language version of SLM, Microsoft has a bug in their regional settings that affects French-language digit groupings. For numbers of one thousand and over, Microsoft has a default setting of a space character instead of a period for the digit-grouping symbol (for example, 1 234 567,00). Because of this bug, when entering numbers in the French-language version, SLM will not allow the period character to be used.

To fix this problem, you must change the setting in the **Control Panel > Region and Language** applet. Click the **Additional settings** button, and change the **Digit grouping symbol** from a space to a period (or...
To specify a product's unit price

1. Click **Products > Monitored** and select the product (using the **Search** box, if needed, to find the product).
2. On the toolbar, click **Edit**.
3. Click **Unit price**.
4. Select the automatically calculated price, or click **Specify a unit price** and enter a cost in the unit price box.
5. Click **Save**.

Note that if you select a normalized product, you should be sure that the unit cost represents all versions of the product that are included in the normalized product.

**Specify files to detect product installation and usage**

There are two ways to determine whether a product is installed and being used on a managed device. The Endpoint Manager inventory scanner identifies two types of files:

- Files that indicate the product has been installed
- Files that indicate the product has been used

Files are defined by file name, version number, and size (in bytes). Automatically discovered products are also uniquely identified by the GUID associated with the product, which is why there may appear to be duplicates of a product. Two products may share a similar name and version but have different GUIDs.

When you create or edit a product, you can modify the definitions used to detect files. The instructions below are for editing an individual product.

---

**NOTE:** If you're using the French-language version of SLM, Microsoft has a bug in their regional settings that affects French-language digit groupings. For numbers of one thousand and over, Microsoft has a default setting of a space character instead of a period for the digit-grouping symbol (for example, 1 234 567,00). Because of this bug, when entering numbers in the French-language version, SLM will not allow the period character to be used.

To fix this problem, you must change the setting in the **Control Panel > Region and Language** applet. Click the **Additional settings** button, and change the **Digit grouping symbol** from a space to a period (or whatever other character you want).

---

```markdown
To specfiy a product’s unit price

1. Click **Products > Monitored** and select the product (using the **Search** box, if needed, to find the product).
2. On the toolbar, click **Edit**.
3. Click **Unit price**.
4. Select the automatically calculated price, or click **Specify a unit price** and enter a cost in the unit price box.
5. Click **Save**.

Note that if you select a normalized product, you should be sure that the unit cost represents all versions of the product that are included in the normalized product.

**Specify files to detect product installation and usage**

There are two ways to determine whether a product is installed and being used on a managed device. The Endpoint Manager inventory scanner identifies two types of files:

- Files that indicate the product has been installed
- Files that indicate the product has been used

Files are defined by file name, version number, and size (in bytes). Automatically discovered products are also uniquely identified by the GUID associated with the product, which is why there may appear to be duplicates of a product. Two products may share a similar name and version but have different GUIDs.

When you create or edit a product, you can modify the definitions used to detect files. The instructions below are for editing an individual product.

---

**NOTE:** If you’re using the French-language version of SLM, Microsoft has a bug in their regional settings that affects French-language digit groupings. For numbers of one thousand and over, Microsoft has a default setting of a space character instead of a period for the digit-grouping symbol (for example, 1 234 567,00). Because of this bug, when entering numbers in the French-language version, SLM will not allow the period character to be used.

To fix this problem, you must change the setting in the **Control Panel > Region and Language** applet. Click the **Additional settings** button, and change the **Digit grouping symbol** from a space to a period (or whatever other character you want).

---

Copyright © 2017, Ivanti. All Rights Reserved. **Terms of Use.**

Page 512 of 1048
To specify files to detect product installation or usage

1. Click **Products > Monitored**. Click a single product name (not a normalized product).
2. On the toolbar, click **Edit**. The product details dialog opens; some items are read-only and some items are editable.
3. Under **Status**, select **Monitored** or **Ignored** to list this new product in one of the product views.
4. Click **Installation detection**. Note that all options are read-only.
5. Click **Usage detection**. You can add files that indicate the product is being used.
6. Click the **Add (+)** button. In the **Add files** dialog, you can select an existing filename (one that exists in the inventory database), or you can click **Define new file** and specify the name, size, and version number for the product file. Repeat this for every product file you want to use to determine when the product is being used. When you have finished, click **OK**.
7. When all information is complete, click **Save**.

Use a query to define when a product is installed

In inventory scans, most products are detected with executable files that indicate a product has been installed or is being used. In some cases you can detect that a product is being used on a device by searching for other inventory data.

To do this, create a query in the Endpoint Manager network view that is based on inventory data. You can then reference that query as the item used for installation detection when you create a custom product.

For example, if a product is licensed with a dongle key that must be connected to a device to use the product, you can create a query that identifies the dongle as a hardware inventory item. When a device has the dongle connected, the inventory scanner identifies the dongle. That data is matched to the product by the software license monitoring (SLM) console when you associate that query with the product. In SLM calculations, the existence of the dongle indicates when the product is being used.

Another example is when you have a font installed that is licensed per device. You can create a query with the font name and version, and then associate that query with the product definition for the font. The inventory scanner will find any use of the font, and that data will be reported in the SLM console.

IMPORTANT: Any query you create for product identification must contain **Computer.ID** as one of the query components; if it’s not included, no data for the query will be returned. Add the component to your query, and also select it as one of the columns to display.

To use a query for product installation detection

1. In the Endpoint Manager console, open the network view and right-click **My queries**. Select **New Query**. Define the query with items that identify the product you want to monitor and
include Computer.ID as a component. Save the query.

2. Click **Tools > Reporting/Monitoring > Software License Monitoring** to open the SLM console.

3. Click **Products > Monitored**. On the toolbar, click **New > Custom Product**.

4. Enter the product name, version, and manufacturer name.

5. Click **Installation detection** and select **Use query detection**.

6. Click **Browse**. Under **My queries**, find the query you created. Select it and click **OK**.

7. Add any other product data on the **Usage detection**, **Unit price**, **Allocations**, and **Reclamation** pages. When all information is complete, click **Save**.

### Creating a normalized product name

As you review product data, you may find that the same product is represented by multiple instances of the product and version number. You can normalize products so that one product name and version number is used in place of all variations of the product and version.

For example, computers in your organization may have multiple versions of Adobe Reader installed. If you’re not interested in tracking older version numbers separately, you can select all instances of Adobe Reader 7, 8, and 9 in the **Products>Discovered** page and normalize them as ”Adobe Reader”. If you want to track how many devices have version X installed, you can select all instances of Adobe Reader X (such as version number 10.0 and 10.1) and normalize them as ”Adobe Reader X”.

A normalized product is displayed with a plus sign (+) before the product name. Click the plus sign to expand the product and see all variations that are included.

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Installed</th>
<th>Unlicensed</th>
<th>Never Used</th>
<th>Ninety Days Since Used</th>
<th>Manufacturer</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe AIR</td>
<td>2.0</td>
<td>4</td>
<td>--</td>
<td>4</td>
<td>0</td>
<td>Adobe Systems Inc.</td>
<td>Contained</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>2.7</td>
<td>7</td>
<td>--</td>
<td>6</td>
<td>1</td>
<td>Adobe Systems Incorporated</td>
<td>Contained</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>3.0</td>
<td>2</td>
<td>--</td>
<td>2</td>
<td>0</td>
<td>Adobe Systems Incorporated</td>
<td>Contained</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>1.5</td>
<td>1</td>
<td>--</td>
<td>1</td>
<td>0</td>
<td>Adobe Systems Inc.</td>
<td>Contained</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>2.0</td>
<td>1</td>
<td>--</td>
<td>1</td>
<td>0</td>
<td>Adobe Systems Inc.</td>
<td>Contained</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>1.1</td>
<td>1</td>
<td>--</td>
<td>1</td>
<td>0</td>
<td>Adobe Systems Inc.</td>
<td>Contained</td>
</tr>
<tr>
<td>Adobe AIR</td>
<td>2.6</td>
<td>6</td>
<td>--</td>
<td>6</td>
<td>0</td>
<td>Adobe Systems Incorporated</td>
<td>Contained</td>
</tr>
</tbody>
</table>

**To create a normalized product definition**

1. Click **Products** and then click one of the product views (Monitored, Discovered, Ignored, or All installed products).

2. Find the product names you want to combine, using the **Search** box.
3. Select the product names and then click Actions > Group.
4. Edit the name you want to use as the normalized product name.
5. Select the view where you want the product listed (Monitored or Ignored).
6. Click Save.

The name you select appears in the product view you selected. A plus sign (+) next to the name indicates it is a normalized product. When you expand the name (click +), you’ll see all the names that are grouped for that normalized name.

To automatically add products to a normalized product

1. Click Products and then click one of the product views (Monitored, Ignored, or All installed products).
2. On the toolbar, click New > Normalized product. (If you want to add products to an existing normalized product, select that product and then click Edit on the toolbar.)
3. Enter the name you want to use as the normalized product name, as well as version and manufacturer information.
4. Select the view where you want the product listed (Monitored or Ignored).
5. Click Dynamic rules.
6. Type a rule in the box. Use an asterisk (*) for wildcard matching.
7. To add another rule, click the Add [+ ] button and type another rule.
8. When all rules have been added, click Save.

Product names currently in the database that match the rules are listed in the Matching products box. As new inventory data is added and other product names are added to the database, those names will automatically be included in the normalized product.

NOTE: With some normalized products you can specify a single manufacturer name on the Definition page of the product details dialog. However, other normalized names include products with different variations of the manufacturer name. If this is the case, use a partial match string with a wildcard so that all variations are included. For example, type Adobe* in the manufacturer box to include all variations of “Adobe Systems” as a manufacturer.

You can also set up license allocations or a reclamation process for a normalized product. For more information, see "Allocating licenses and chargeback costs to a computer group" (543) and "Reclaiming product licenses" (537).

Deleting a normalized product

You can delete a normalized product by selecting it and pressing the Delete key. If you do this, the individual products that were grouped together are returned to the product list as individual products.
If you delete a normalized product, any licenses you associated with that product will no longer be associated with it, and compliance reports will no longer show the normalized product as consuming licenses. When this happens, you should edit the licenses and review the product associations for each license.

**Creating a normalized manufacturer name**

As inventory data is added to the software license monitoring (SLM) console, you may find that a manufacturer is represented by multiple versions of its company name. You can create one normalized manufacturer name that is used in place of those variations.

Normalized manufacturer names are preceded by a plus sign (+) in the list. For example, in the following list, there are four variations of the manufacturer Alchemy Software:

<table>
<thead>
<tr>
<th>Manufacturers</th>
<th>1,013 items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type</td>
</tr>
<tr>
<td>Airgo Networks, Inc.</td>
<td>Normalized manufacturer</td>
</tr>
<tr>
<td>alch</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>Alchemy Software</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>Alchemy Software Development</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>Alchemy Software Development Ltd.</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>Alchemy Software Development.</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>:: Alentum Software</td>
<td>Normalized manufacturer</td>
</tr>
<tr>
<td>Alex Feinman</td>
<td>Manufacturer</td>
</tr>
</tbody>
</table>

You can select those names and group them so that one normalized name is used for all of them. That normalized name is then displayed in the list.
Manufacturers 1,010 items

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airgo Networks, Inc.</td>
<td>Normalized manufacturer</td>
</tr>
<tr>
<td>alch</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>Alchemy Software</td>
<td>Normalized manufacturer</td>
</tr>
<tr>
<td>Alchemy Software Development</td>
<td>Contained manufacturer</td>
</tr>
<tr>
<td>Alchemy Software Development Ltd.</td>
<td>Contained manufacturer</td>
</tr>
<tr>
<td>Alchemy Software Development</td>
<td>Contained manufacturer</td>
</tr>
<tr>
<td>Alentum Software</td>
<td>Normalized manufacturer</td>
</tr>
<tr>
<td>Alex Feinman</td>
<td>Manufacturer</td>
</tr>
</tbody>
</table>

Normalized manufacturers provided with SLM

The SLM console includes normalized manufacturers. The first time you open the list of manufacturers, you'll notice that the list includes commonly used manufacturer names that have been normalized.

Ivanti may provide additional normalized manufacturers. When they become available, they will be downloaded automatically as patch content. If you have already defined normalized manufacturers of your own, your content will be maintained. Any new normalized manufacturers that might conflict with your own definitions will not overwrite your custom content.

Creating a normalized manufacturer

You can create a normalized manufacturer in the following ways.

To create a normalized manufacturer

1. Click Administration > Manufacturers.
2. Find the manufacturer names you want to combine (using the Search box if needed).
3. Select the manufacturer names that you want to include in the normalized name.
4. Click Actions > Group.
5. Select one of the existing names as the normalized manufacturer name.
6. Click OK.

The name you select is added to the normalized manufacturer names in the Administration > Manufacturers page. When you expand the name (click +), you'll see all the names that are grouped for that normalized name.
To automatically add manufacturers to a normalized manufacturer

You can create rules that will automatically add manufacturer names to a normalized name. For example, you could specify that any manufacturer name that begins with "Adobe Sys*" is automatically added to the normalized "Adobe Systems Incorporated" name.

1. Click Administration > Manufacturers.
2. On the toolbar, click New > Manufacturer.
3. Type a name for the normalized manufacturer.
4. Click Dynamic rules.
5. Type a rule in the box. Use an asterisk (*) for wildcard matching.
6. To add another rule, click the Add [+] button and type another rule.
7. When you have finished, click Save.

Manufacturer names currently in the database that match the rules are listed in the Matching manufacturers box. As new inventory data is added and other similar manufacturer names are added to the database, those names will automatically be included in the normalized manufacturer name.

To add a manufacturer name to an existing normalized manufacturer

If you have created a normalized manufacturer and then find another manufacturer name that you want to include with the other names, you can add the name to the normalized name.

1. Click Administration > Manufacturers.
2. Select the manufacturer name you want to add to the normalized manufacturer name.
3. Click Actions > Move to normalized manufacturer.
4. Select a normalized manufacturer and click OK.

Creating Web products

You can monitor Web-based software products in software license monitoring (SLM) the same way that you monitor products installed on a device. To monitor a Web-based product, you must first create it in the SLM console.

When you create a Web product in SLM, you specify the URL associated with the product. This URL is added to the list of items that the inventory scanner searches for on managed devices. You only need to specify a top-level domain; no path, port number, or page name in the domain can be specified. You can add subdomains. For example, if you use Salesforce to track sales and customer service, you would define a product named "Salesforce" and associate it with the URL that is accessed for logging in.
After creating a Web product, its product detection information isn’t immediately available to the Endpoint Manager inventory scanner. You can wait for the regularly scheduled publish action (which typically happens once a day), or you can publish the data immediately by going to the **Administration>Calculations** page and clicking the **Publish** button. The inventory scanner can then track which devices access the URL and for how long. This data is then included in the SLM reports and calculations.

**To create a Web product definition**

1. Click **Products > Monitored**.
2. On the toolbar, click **New > Web product**.

![Create Web Product](image)

3. Type the name in the **Product name** box.
4. Type at least three characters in the **Manufacturer** box to show matching names. Select the manufacturer name. If there is no match, type the full manufacturer name in the box.
5. Under **Status**, select **Monitored** or **Ignored** to list this new product in one of the product views.
6. Under **Domain names to monitor**, click the **Add (+)** button.
7. Type the domain name for the Web product.
8. Click **Unit price**. Select a method for calculating the unit price:
- Select **Use automatically calculated unit price** if you have multiple licenses for the product with different unit prices. If you select this option, the unit price is an average of all unit prices from the different licenses.
- Select **Specify a unit price** if you want to use the same unit price for all calculations. For example, if you have two licenses with different unit prices for the same product and you want to use the higher price for calculations, you can specify that unit price here.

9. When all information is complete, click **Save**. You will begin to see product inventory data gathered for the Web product after its detection information is published for the first time. You can wait for the regularly scheduled publish action (which typically happens once a day), or you can publish the data immediately.

10. To immediately publish the Web product detection information that is used in inventory scans, click **Administration > Calculations**, then click the **Publish** button.

You can also set up license allocations for a Web product. For more information, see "Allocating licenses and chargeback costs to a computer group" (543).

**Creating custom products**

You can create custom products for any unidentified or misidentified software executable files. When you do this, the files in the custom product are added to the list of files that the inventory scanner looks for.

You can specify which files indicate that the product has been installed, and which usage files indicate when the product is running on a computer.

In some cases, you may want to use a Endpoint Manager query to find installed products. You would do this when a product is not identified correctly from executable files but can be identified based on inventory data that you add to a query.
To create a custom product definition

1. Click Products, and then click one of the product views (Monitored, Discovered, Ignored, or All).
2. On the toolbar, click New > Custom product.

3. Type the name in the Product name box.
4. Type a number or number with a wildcard in the Version box.
5. Type at least three characters in the Manufacturer box to show matching names. Select the manufacturer name.
6. Under Status, select Monitored or Ignored to list this new product in one of the product views. (By default, a custom product is moved to the Monitored view.)
7. Click Installation detection.
8. If you want to detect products based on a Endpoint Manager query, select Use query detection. Click Browse and select a query that you have created in the Endpoint Manager network view. All devices that match the query will be returned as having a match for this product.
9. Select Use file detection to detect products based on installed files. The filenames you add here determine how the product will be detected during inventory scans.
10. Click the **Add (+)** button. In the **Add files** dialog, you can select an existing filename (one that exists in the inventory database), or you can click **Define new file** and specify the name, size, and version number for the product file. Repeat this for every product file you want to use. When you have finished, click **OK**.

11. Select **Match any** or **Match all** to specify whether a minimum of one file must be found or all files must be found.

12. Click **Usage detection**. Use this option to include files that indicate the product is being used.

13. Click the **Add (+)** button. In the **Add file** dialog, you can select an existing filename (one that exists in the inventory database), or you can click **Define new file** and specify the name, size, and version number for the product file. Repeat this for every product file you want to use. When you have finished, click **OK**.

14. Click **Unit price**. Select a method for calculating the unit price:

   - Select **Use automatically calculated unit price** if you have multiple licenses for the product with different unit prices. If you select this option, the unit price is an average of all unit prices from the different licenses.
   - Select **Specify a unit price** if you want to use the same unit price for all calculations. For example, if you have two licenses with different unit prices for the same product and you want to use the higher price for calculations, you can specify that unit price here.

15. If you add product information that will affect license and usage calculations, such as when a product is associated with a license that you are actively monitoring, select the **Calculate compliance after save** check box to initiate a recalculation so compliance reports stay up-to-date.

16. When all information is complete, click **Save**.

You can also set up license allocations or a reclamation process for a custom product. For more information, see "Allocating licenses and chargeback costs to a computer group" (543) and "Reclaiming product licenses" (537).

---

**IMPORTANT:** The two types of detection files, installation and usage, are both necessary for gathering product data in inventory scans. Installation files indicate that a file has been installed; they’re required to determine that a product exists on a computer. Usage files indicate that the product has been run; they’re required to determine whether the installed product has been used.

![Warning](image)

If a device’s inventory shows a match for the installation files, software license monitoring (SLM) will report that the product is installed. However, if there are no usage files specified for the product, SLM will always report that the product has never been used. **When creating a custom product, you need to define at least one usage file so that SLM will accurately report whether the product has ever been used.**
Creating a Data Analytics product

If you’re using Ivanti Data Analytics, you have the ability to monitor license-rules-based products within the software license monitoring (SLM) console.

Data Analytics uses license rules to evaluate your installed software and report how many installations need a license (in contrast to other discovered products in SLM that don’t take into account license rules and show the actual number of licenses installed on devices). You may have 100 installations of a product, but the license rules that Data Analytics uses may show that you need only 50 licenses to be compliant.

For example, if you have both Microsoft Office 2012 Professional and Office 2010 Professional installed on one device:

- Using license rules, the Data Analytics products show 1 installation of Office 2012 Professional and 0 installations of Office 2010 Professional, because the license for Office 2012 Professional covers multiple versions of this edition of Office on the same device. (Note that a device with different editions of a product, such as Office Pro and Office Pro Plus, would require an installed license for each edition to be compliant.)
- Not using license rules, the other automatically discovered products show 1 installation of Office 2012 Professional and 1 installation of Office 2010 Professional on the same device.

Approximately 600 Data Analytics products can display on the Products>Monitored page when you have Data Analytics installed. These products appear in the same list as the other automatically discovered products, so you can have one product showing up as two types—as a Data Analytics product and as the usual SLM-discovered product.

The Installed column shows the number of installed licenses a Data Analytics product needs to be compliant (versus the actual number of licenses installed on devices), and the Type column identifies the product as a Data Analytics type.

![Monitored 606 items (1 selected)](image)

NOTE: You can’t add Data Analytics products to a normalized product definition.

To create a Data Analytics product definition

1. Click Products and click one of the product views (Monitored, Discovered, Ignored, or All).
2. Find the product using the Search box or Select products filter.
4. Under Status, select Monitored or Ignored to list this product in one of the product views. (By default, a Data Analytics product is moved to the Monitored view.)

5. Click Installation detection.

6. If you want to detect products based on a Endpoint Manager query, select Use query detection. Click Browse and select a query that you have created in the Endpoint Manager network view. All devices that match the query will be returned as having a match for this product.

7. Select Use file detection to detect products based on installed files. The filenames you add here determine how the product will be detected during inventory scans.

8. Click the Add (+) button. In the Add files dialog, you can select an existing filename (one that exists in the inventory database), or you can click Define new file and specify the name, version number, and size. Repeat this for every product file you want to use. When you have finished, click OK.

9. Select Match any or Match all to specify whether a minimum of one file must be found or all files must be found.

10. Click Usage detection. You can add files that indicate the product is being used.

11. Click the Add (+) button. In the Add files dialog, you can select an existing filename (one that exists in the inventory database), or you can click Define new file and specify the name, version number, and size. Repeat this for every product file you want to use to determine when the product is being used. When you have finished, click OK.

12. Click Unit price. If the options can be edited, select a method for calculating the unit price:
   
   - Select Use automatically calculated unit price if you have multiple licenses for the product with different unit prices. If you select this option, the unit price is an average of all unit prices from the different licenses.
   
   - Select Specify a unit price if you want to use the same unit price for all calculations. For example, if you have two licenses with different unit prices for the same product and you want to use the higher price for calculations, you can specify that unit price here.

13. If you add product information that will affect license and usage calculations, such as when a product is associated with a license that you are actively monitoring, select the Calculate compliance after save check box to initiate a recalculation so compliance reports stay up-to-date.

14. When all information is complete, click Save.

You can also set up license allocations or a reclamation process for a Data Analytics product. For more information, see "Allocating licenses and chargeback costs to a computer group" (543) and "Reclaiming product licenses" (537).
Reset usage calculation for a product

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 devices, you can reset product usage calculation for that product. After you do this, the new usage data (number of launches and minutes used) will reflect only usage from the time you reset it.

NOTE: Keep in mind that when you reset a product’s usage calculation, the existing product usage information for that product will be removed from the database.

To reset usage calculation for a product

1. Click Products, and then click a product view (Monitored, Discovered, or All installed products).
2. Find the product using the Search box or Select products link.
3. Right-click the product and select Reset product usage.
4. Click OK to confirm that you want to delete the information.

Defining a computer group

As you monitor product and license usage, you may want to associate groups of devices with licenses. For example, a group can represent devices in a location or in a division of your organization with its own software license accounting.

You can associate licenses with groups in two ways:

- **Static group**: a group of devices that you have selected in the Endpoint Manager network view and saved as a device group.
- **Dynamic group**: a group of devices defined with a query in the Endpoint Manager network view. As monitored devices are added or removed, the contents of the group changes to match the query parameters.

You can only create groups in the Endpoint Manager network view. When you define a group in the software license monitoring (SLM) console, you are simply choosing a name to associate with an existing device group or query.

To define a computer group

1. Click Administration > Computer groups.
2. On the toolbar, click New > Computer group.
3. Type a name for the group. This name identifies the group in the SLM console.
4. Select **Use as allocation unit** if you want to define this group as an allocation unit. You can later allocate a certain number of product licenses to this group with the intent of charging back the cost of providing IT support.

5. Expand **Devices** or **Queries** and find the device group or query that is the source for the newly created computer group.

6. When all information is complete, click **Save**.

**To delete a computer group**

1. Click **Administration > Computer groups**.
2. Select a group in the list. On the toolbar, click the **Delete** button.
3. Click **Yes** to confirm the deletion.

**NOTE:** If you delete a computer group, any associated licenses will no longer be associated with those devices, so compliance reports will not apply to the group. If you do this, you need to decide what devices to associate with the license and define another group. If there is no associated group, the license is associated with all devices.

**View installed products for a computer group**

All discovered products are initially found on the **Products > Discovered** page, which can quickly add up to too many records. You can move software to the **Monitored** or **Ignored** views for those products you want to monitor actively or for those you don’t care about right now.

To view an even smaller group of product records, you can use computer groups. Remember, you initially create computer groups in the Endpoint Manager network view. When you define a computer group in the software license monitoring console, you’re simply choosing a name to associate with an existing device group or query. For more information, see “Defining a computer group” (525).

**To view the installed products for a computer group**

1. Click **Products**, and then click a product view (Monitored, Discovered, Ignored, or All installed products).
2. In the column to the left of the product list, click **Computer group** and select a computer group.
The list of products changes to display only products that are installed on devices in the group you selected.

**Monitoring product license compliance**

Product license compliance is an important part of your overall IT asset management. Your ability to monitor compliance helps ensure that you’ll have accurate records for audits and that employees are following your organization’s policies related to product usage.

Your organization’s compliance with the terms of your product licenses is dependent on:

- **Accurate inventory scans that contain data on what products are discovered and being used**: Ivanti® Endpoint Manager powered by Landesk runs inventory scans on managed devices in your network. These scans include a software monitor scan that saves product information to the database.

- **Accurate data regarding the terms of the product licenses you have purchased**: You can add this data to the database from the license records that your organization maintains. Enter each license individually or import data from different sources by first exporting the data from an Excel spreadsheet to a CSV file and then importing the data into the software license monitoring (SLM) console.

- **Correct association of licenses with products and computer groups**: Product associations occur when you add or edit a license. If you import license data, check each license to make sure it’s associated with products that are covered by the terms of the license. Also, if licenses are limited to certain departments within your organization, you should associate the licenses with computer groups you define for those departments.
Reconciliation of license data with inventory data: SLM reconciles all required data that is available in the database. Compliance is calculated each day when regular inventory maintenance runs on the database. The success of your license monitoring depends on how accurate your product license data is and how completely your inventory scans cover the devices in your organization. Your compliance results also depend on having the correct computer groups defined and associated with licenses.

Related topics

"Maintaining accurate license data" (528)
"Create a license record" (528)
"Associating a license with products" (533)

Maintaining accurate license data

An important part of your organization’s financial management is the maintenance of product licenses. The software license monitoring (SLM) tool uses license data to help you determine how well your organization complies with the terms of your licenses. Your license data needs to be available and accurate for up-to-date compliance calculations.

You may want to begin with a small number of licenses, such as licenses that need to be monitored for audits. You can manually add or import that license data using the SLM console. The data is then used to generate statistics and reports, which help you determine whether your product licenses are in compliance based on the actual product installations.

After the license data is added, you should review the product information related to each license. Find the products for a license on the Products>Discovered page and move them to the Monitored view. If appropriate, combine different versions of a product into one normalized product so it’s easier to manage in the SLM console.

The following tasks can be used to maintain accurate license data for your organization:

- Create software license records
- Import software license data
- Create normalized products
- Associate software licenses with installed products
- View software license compliance
- Re-calculate software license compliance

Create a license record

If your license data is in a format not easily imported, you can enter the data manually on the Products>Licenses page. The data you enter is stored in the database and is used to calculate compliance.
**To create a license record**

1. Click **Products > Licenses**.
2. On the toolbar, click **New > License**.
3. Enter data on the five pages of the **Create License** dialog (Definition, Associated products, Records, Purchase, and Shipping).
4. Click **Save** when you have finished.

---

**NOTE:** If you’re using the **French-language version of SLM**, Microsoft has a bug in their regional settings that affects French-language digit groupings. For numbers of one thousand and over, Microsoft has a default setting of a space character instead of a period for the digit-grouping symbol (for example, 1 234 567,00). Because of this bug, when entering numbers in the French-language version, SLM will not allow the period character to be used.

To fix this problem, you must change the setting in the **Control Panel > Region and Language** applet. Click the **Additional settings** button, and change the **Digit grouping symbol** from a space to a period (or whatever other character you want).

---

**Click here for descriptions of the fields in the Create License dialog.**

**Definition page**

- **License name**: The name of the license, which may be the same as the product name.
- **Purchase quantity**: The original number of licenses purchased for use as part of an upgrade chain, only applicable if you’re using the B2B connectors in Data Analytics. If you’re creating licenses manually using SLM, this field can’t be edited and remains at “0.”

Data Analytics creates the original license by setting the purchase quantity and license quantity to the same number of licenses. As a license is upgraded, the license quantity is decremented by the same number, showing how many licenses remain as part of the upgrade chain.

- **License quantity**: When using Data Analytics, this field shows the number of original licenses remaining from the purchase quantity after upgrading your licenses. If you’re creating licenses manually using SLM, this field shows the number of licenses allowed in the purchase agreement.
- **Unit price**: The price paid for the purchase of the license.
- **Computer group**: If the license was purchased for a specific group of devices, select the group here. Groups that appear here exist in the **Administration > Computer groups** page, which is populated by computer groups created in the Endpoint Manager network view. Select **All** when the license can be used for any device in your organization. If the group you want isn’t listed, click **Create computer group** to create a new group from an Endpoint Manager query or device group.
• **Vendor:** The vendor from whom you purchased the license. This may be the same as the manufacturer. After you type at least three characters, any matching vendor names in the database are displayed; if a name matches the vendor, select it from the list.

• **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).

• **Consumption:** The method used to calculate license usage. Usage is counted one time for each device that has the product installed, regardless of how many additional installations there may be on that device.

• **Compliance type:** The type of license, in terms of the license compliance as specified by the manufacturer.

**Associated products page**

This page lists the products that are associated with the license. List all products that can be used under the terms of the license.

List the products in the order that you want them to consume the licenses. The first product consumes available licenses first. If there are additional licenses available, then the second product consumes available licenses. This continues down the list until no more licenses are available.

You can associate any product with a license. If the product is not currently monitored, it will appear in the **Products>Monitored** page when you associate it with a license.

**To add associated products to the list**

1. Click the **Add (+) button.**
2. In the **Add Products to License** dialog, type at least three characters in the **Product name contains** box to find the products you want. All products matching the string you type are listed in the results.
3. To filter the results list, you can type a string in the **Product name does not contain** box. Products with that string are removed from the list. You can use multiple strings, separated by a space.
4. To limit the results to products in the **Products>Monitored** page, select **Show only monitored products.**
5. Select one or more products from the results list, and then click **OK.**

The products are added to the **Associated products** list.
6. Use the up and down arrow buttons to move products up or down in the list.

**Related topics**

"Associating a license with products" (533)
Records page

This page contains data and notations that document the license in terms of your organization's purchasing or accounting practices. This information is not used in license monitoring but is useful for you to maintain accurate records for auditing purposes.

- **Manufacturer part number**: The part number issued by the product manufacturer. This is useful for tracking the product within your purchasing process.
- **Manufacturer invoice number**: The invoice number issued by the product manufacturer. This is useful for tracking the product within your purchasing process.
- **Product description**: A notation describing the product type.
- **License key**: The key provided by the manufacturer to activate the license.
- **Serial number**: The manufacturer's serial number associated with the license.
- **Location**: A notation that helps you identify where the licenses are being used in your organization.
- **Supporting documents**: A notation that describes where supporting documentation is found for your license assets. This can indicate a network location, URL, or any description you want to use.
- **Notes**: Type any additional notes related to the license. These notes are saved in the database.

Purchase page

Use this page to enter all data associated with license purchasing. This information is not used in license monitoring but is useful for you to maintain accurate records for auditing purposes.

- **Purchase order number**: Your organization's purchase order number used to purchase the product. This is useful for tracking the product within your purchasing process.
- **Purchased by**: The name of the department within your organization that purchased the product.
- **Order line number**: The line number within a purchase order that relates to the specific product.
- **Coverage begin date**: The begin date of any contract or separately purchased maintenance agreement that is associated with the license. 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).
- **Coverage end date**: The end date of any contract or separately purchased maintenance agreement that is associated with the license. 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).
- **Coverage cost per license**: The maintenance agreement cost per purchased license.
Shipping page

Use this page to enter all data associated with the product shipping destination, typically a department within your organization. This information is not used in license monitoring but is useful for you to maintain accurate records for auditing purposes.

- **Address 1 and 2**: The name and street address of the department within your organization that will receive the product.
- **City**: The city where the department is located.
- **State/province**: The state/province where the department is located.
- **Zip/postal code**: The zip/postal code where the department is located.
- **Country**: The country where the department is located.
- **Shipped**: The date that the product ships to the recipients. 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).
- **Tracking number**: Your organization’s internal tracking number used to ensure the product reaches its destination.

Importing license data from a CSV file

You can import existing license data from a previous version of Ivanti® Endpoint Manager powered by Landesk or from another data source. The data must be saved as a CSV file.

A sample CSV file (ImportLicense.csv) is included in the LDMAIN share of the core server (in the LDMAIN\LANDesk\SAM folder), for your reference. Note the following guidelines for creating a CSV file to import license data:

- The only required column in the CSV file is the Name column.
- If you don’t know what to put into a column, leave it blank. The import process will add a default value for any blank column.
- After the license property columns, there are columns for associated products. They are called “Associated Product 1” and “Product 1 Version”, “Associated Product 2” and “Product 2 Version”, and so on. Put the product name in the “Associated Product x” column and the product version in the “Product x Version” column. If there is no product version, leave the column blank. The import process will look for matching products with the supplied product name and version. If multiple products are found with the same name and version, all of the matching products will be associated with the license. Any number of products can be associated to a license.
- The import will **not** override existing licenses. If an existing license matches the name of a license being imported, a new license record will be created with the name of “<License name> [1]”. The number in brackets will be incremented with each additional match so that every license has a unique name.
To import license data

1. Prepare a CSV file with the license data you want to import, using the guidelines listed above.
2. In the software license monitoring console, click **Products > Licenses**. On the toolbar, click the **Actions > Import from CSV**.
3. Browse to the location of your CSV file, and then click **Open**. The license data is added to the database and is displayed in the **Product>Licenses** page.

To review the imported licenses and edit the data

1. Click **Product>Licenses** and select a license in the list.
2. On the toolbar, click **Edit**. Review the data on each of the five pages of the edit license dialog (Definition, Associated products, Records, Purchase, and Shipping).
3. Click **Save** when you have finished.

Associating a license with products

When you add or edit a license, you need to associate the license with one or more software products in order to calculate compliance for product usage and the license. You can select one or more products, including normalized products that represent multiple individual products. If a product is not currently monitored, software license monitoring (SLM) will move the product to the **Products>Monitored** page when you associate it with a license.

When you select associated products, list the products in the order that you want them to consume the licenses. The first product listed will consume available licenses first. If additional licenses are available, the second product will consume available licenses. This continues down the list until no more licenses are available.

The following is an example of how license calculation is applied with multiple product versions:

- You have purchased a license for Product ABC that allows 30 installations (or license seats).
- The license can be used for versions 3, 4, and 5 of that product.
- In the **Associated products** list, you have ordered the versions with the most recent version (5) first followed by version 4 and then version 3.

In this situation, the license usage is calculated as follows:

- 16 users have version 5 installed, so all 16 consume a license seat.
- 21 users have version 4 installed; 14 of them consume a license seat and 7 are not licensed.
- 8 users have version 3 installed; none of them are licensed.

Your license compliance reports for this product will show that 15 uses of the product are not covered by the license. You then need to determine whether to purchase additional licenses. You might also review the actual usage of the products in your organization. If some users with the product installed have not used the product for a long period of time, you can check with them to see if they need the software. If not, they can uninstall the product and their licenses can be applied to other users.
NOTE: Licenses are associated with products for compliance calculation. If you delete a product, the license you associated with that product will no longer be associated with it, and compliance reports will no longer show that product as consuming licenses.

Viewing license compliance data

In the software license monitoring (SLM) console, there are different ways to find out whether your product installations are in compliance with the terms of your product licenses. This topic describes how to find the data you need.

Viewing information by product

Open the Products>Monitored page for information about the products installed on your organization’s devices. A product must be moved to the Monitored view so you can find the most information about its usage and licensing.

You can view the following items:

- Product installations: Double-click the product name to view a list of devices that have the product installed.
- Whether a product is currently being used: Look at the Never Used and Ninety Days Since Used columns to see the users who aren’t using the product or are rarely using it.
- Whether a product is properly licensed: Compare the Installed and Unlicensed columns to see if there are more installed copies than valid licenses.
- Licenses associated with the product: Right-click a product and select View licenses matching selected product to see a list of the licenses that are associated with the product.
NOTE: While you’ll notice that the Discovered and Ignored product views have the same columns and appear to show compliance data, the data does not accurately represent licenses compared with actual product installations. Only products in the Monitored product view that are associated with licenses will show useful, accurate data.

Viewing compliance summary data

The dashboards contain summary data related to license compliance and optimization. These pages are designed to help you act on the most important problems related to product licensing. They don’t give you a complete picture but guide you to the issues that should be resolved first so you can reduce costs and improve efficiency in your use of software.

- **Audits dashboard**: This page includes reports that are useful when you’re preparing for an audit of your product license usage.
- **Compliance dashboard**: This page includes reports that show you products that are out of compliance with license terms and need your attention.
- **License Optimization dashboard**: This page includes reports that estimate the savings you can gain by removing unused products from devices in your organization.

Viewing license-related reports

SLM reports bring together complete reporting data for many aspects of your license compliance and usage. Use reports to find all details for a particular issue or need, and then export the data or email the report for others to act on.

- **Audit reports**: These reports are useful when you’re preparing for an audit of the your license usage. They include audit flags such as monitored products without associated licenses and licenses that don’t have supporting data, such as invoice or purchase order numbers.
- **Compliance reports**: These reports include details for all products and licenses that are out of compliance. They include an overview of license consumption for all products, total costs to bring products into compliance, and so on.
- **License optimization reports**: These reports provide details that can help you optimize your organization’s use of its products. They include lists of unused licenses, products not used or rarely used, and other related data.

Re-calculating license compliance

License compliance is calculated on a daily basis, at the time that inventory maintenance is run on your database.

In many tasks related to products and licenses, a new calculation is run when you save the data you have changed. When you see a check box labeled **Calculate compliance after save**, this indicates that when you save your work, license compliance calculation will be run again.
Calculations page

On the Calculations page, you have a check box that enables software license monitoring (SLM) to calculate product installation and usage immediately whenever you make changes to specific product data. Also, if you have added license data or made other changes and want to re-calculate compliance without waiting for the scheduled maintenance, you can initiate a new calculation of product usage and license compliance.

A related option lets you publish new product detection information to the inventory scan file that detects when products are installed or used. You should publish whenever you define a custom product with installation information based on files not currently in the database, as well as whenever you add, change, or remove a domain from a web product.

A third option lets you run a license reclamation process that looks for unused product licenses and runs a task to uninstall the product so you can reassign those licenses to other end users in your organization. If an installed product hasn't been used for a certain period of time, it can be uninstalled from one device, freeing its license for use on a different device.

To recalculate usage and compliance

1. Click Administration > Calculations.
2. To calculate installation and usage whenever you make changes, click the **Calculate product installation and usage immediately when saving a product** setting and click **Save**. To update usage and license compliance, click the **Recalculate** button.

3. To publish new product detection information that is used in client inventory scans, click the **Publish** button.

4. To run license reclamation on unused product licenses, click the **Reclaim** button. All reclamation tasks that you have defined in the SLM console will run during this process.

A status message will show if the above actions were successful or completed with an error. If an error occurs, you can find more information about it in your installation directory log files (located by default in C:\Program Files\LANDesk\ManagementSuite\log):

- For recalculation or reclamation errors—View the **SLM.Routines.exe.log** file.
- For publishing errors—View the **SAM.Services.dll.log** file.

**Reclaiming product licenses**

License reclamation is the process of taking unused software product licenses and reassigning them to devices that need a license for the same product.
Your organization may have unused product licenses that can be reclaimed and given to users who need to install the product. License reclamation is a software license monitoring (SLM) feature that finds product installations that have not been used within a certain period of time. When a product on a device meets the reclamation criteria, it's uninstalled from that device, and the license is then free for you to assign to another user.

The delivery methods and uninstall packages that you use for license reclamation must have been created in the Endpoint Manager console first. They will then be available to select in the SLM console.

**Required user rights**

Any user who will work with license reclamation must have the following software distribution rights:

- View delivery methods
- View packages
- Deploy packages

For information about assigning rights to users, see "Managing roles" (58)

**Getting started**

To reclaim product licenses, you need to do the following:

- Configure defaults for license reclamation. ("Configuring license reclamation defaults" (541).) Although these are the defaults that appear when you enable reclamation for a product, you can change any of these items for a product.
- Enable license reclamation for individual products (described below). You can reclaim licenses for single products, as well as for normalized and custom products.
- Run a reclamation manually, or set up a schedule for reclamation (described below).
- View a list of product licenses that have been reclaimed. ("Viewing license reclamation status" (544).) Use this list to determine which products can be installed on other devices.

NOTE: If you’re using the French-language version of SLM, Microsoft has a bug in their regional settings that affects French-language digit groupings. For numbers of one thousand and over, Microsoft has a default setting of a space character instead of a period for the digit-grouping symbol (for example, 1 234 567,00). Because of this bug, when entering numbers in the French-language version, SLM will not allow the period character to be used.

To fix this problem, you must change the setting in the Control Panel > Region and Language applet. Click the Additional settings button, and change the Digit grouping symbol from a space to a period (or whatever other character you want).
To enable license reclamation for a product

1. Click Products > Monitored.
2. Select a product. On the toolbar, click Edit.
3. Click Reclamation and select the Enabled check box.
4. Specify how long a product has not been used to make it eligible for license reclamation. Enter a number in the Only reclaim if the product has not been used box. The default for this item is 120 days, because many manufacturers consider a product to have been used in a quarter if the product has been run at least once in a three-month period. Software usage reporting is typically counted by the quarter.
5. If you want to reclaim licenses based on the number of days that products haven’t been used, select Reclaim from all machines that have not used the product...
6. If you want to use license reclamation to always have a certain number of available licenses, select Reclaim to maintain a set of free licenses. Specify a lower threshold for the number of available licenses that triggers reclamation. Specify a higher number that represents the number of licenses you want to make available.
7. Click Task.
8. Click Browse to select an uninstall package that is applied when a product meets the reclamation criteria. For normalized products, you can specify an uninstall package for each contained product, or you can specify a package for the normalized product and make all the contained products use the same uninstall package as the normalized product.
9. For Endpoint Manager 9.5 or earlier clients, check that the delivery method for the package is correct. To change the delivery method, click Browse and select a new one.

Because a Endpoint Manager 9.6 core server can manage both 9.5 and 9.6 clients, you should specify this setting as well as the settings for distribution/patch and reboot, which are for Endpoint Manager 9.6 clients only.
10. For Endpoint Manager 9.6 clients, check that the distribution and patch setting is correct. This setting combines delivery for both software distribution and patches.
11. For Endpoint Manager 9.6 clients, check that the reboot setting is correct. This setting controls if the device will be rebooted and how the reboot will occur.
12. Select the Start scheduled tasks immediately after creation check box to run reclamation for this product after saving your data.
13. Specify how often you want license reclamation to run. Enter a number in the Run reclamation process every ... days box. If you select 0 in this box, reclamation will run daily. By default, reclamation will run immediately after you save this task, then again at night every 14 days. Once a reclamation process has run, the run date will appear in the Last run box.
14. Specify a re-installation policy task if you want to give an end user the option of reinstalling a product after reclamation. The option to reinstall will appear on the Endpoint Manager client dashboard, where the end user can choose to reinstall the product. Click Browse and select the name of the re-installation policy you want to use. Click OK.

15. Click Advanced to include or exclude computer groups for reclamation of this product.

16. If you want to include certain computer groups, select Include and click + to add groups to the list. Only devices in the groups you list here will be included in license reclamation; all other devices will be ignored. The groups you can select are defined on the Administration>Computer Groups page.

17. If you want to exclude certain computer groups, select Exclude and click + to add groups to the list. Select groups that should be excluded from license reclamation. Reclamation will include all monitored devices except those in the groups you select.

18. If you want to send an email to any administrators informing them of a reclamation action, select Enable email notification and type one or more email addresses in the box. Separate multiple addresses with a semicolon (;) or comma (,).

19. When you’ve completed the information for reclamation of the product, click Save.

The options in this dialog are generally the same as those in the Administration>Reclamation Defaults page. For descriptions of these options, see “Configuring license reclamation defaults” (541).

NOTE: After you have set the reclamation options for a product, you’ll be listed as the reclamation owner on the Reclamation page of the product details dialog. If someone else changes the options at a later time, they will become the reclamation owner. It’s important to know who the owner is, because the reclamation owner’s scopes are used during reclamation. Only licenses on devices in the reclamation owner's scope will be reclaimed.

If an error occurs during the reclamation process, an error message will appear on the Reclamation page of the product details dialog. Use this message to troubleshoot the problem.

To run a license reclamation process

License reclamation runs on the schedule you set in the Administration>Reclamation Defaults page (usually 14 days). If you want to run a reclamation process before the next scheduled time, follow these steps.

1. Click Administration > Calculations.

2. Click Recalculate to ensure that usage and compliance calculations are up to date.

3. Click Reclaim to start a license reclamation process.
Configuring license reclamation defaults

While license reclamation is enabled for products individually, you can change the default settings for reclamation in general. The default settings you enter are listed when you enable reclamation for a product.

![Reclamation Defaults](image)

NOTE: If you’re using the French-language version of SLM, Microsoft has a bug in their regional settings that affects French-language digit groupings. For numbers of one thousand and over, Microsoft has a default setting of a space character instead of a period for the digit-grouping symbol (for example, 1 234 567,00). Because of this bug, when entering numbers in the French-language version, SLM will not allow the period character to be used.

To fix this problem, you must change the setting in the Control Panel > Region and Language applet. Click the Additional settings button, and change the Digit grouping symbol from a space to a period (or whatever other character you want).

To configure reclamation defaults

1. Click Administration > Reclamation Defaults.
2. Select a Delivery method for the uninstall package. Click Browse to view the available delivery methods from the Delivery methods tool in the Endpoint Manager console.
3. Specify how long a product has not been used to make it eligible for license reclamation. Enter a number in the **Only reclaim if the product has not been used** box. The default for this item is 120 days, because many manufacturers consider a product to have been used in a quarter if the product has been run at least once in a three-month period. Software usage reporting is typically counted by the quarter.

4. Select **Start scheduled tasks immediately after creation** to automatically start uninstalling products that meet the reclamation criteria.

5. If you want to reclaim licenses based on the number of days that products haven’t been used, select **Reclaim from all machines that have not used the product**...

6. If you want to use license reclamation to always have a certain number of available licenses, select **Reclaim to maintain a set of free licenses**. Specify a lower threshold for the number of available licenses that triggers reclamation. Specify a higher number that represents the number of licenses you want to make available.

7. Specify how often you want license reclamation to run. Enter a number in the **Run reclamation process every ... days** box. If you select 0 in this box, reclamation will run daily. By default, reclamation runs at night every 14 days.

8. If you want to include certain computer groups in license reclamation, select **Include** and click + to add computer groups to the list. Only the devices in the groups you list here will be included in license reclamation; all other devices will be ignored. The groups you can select are defined on the **Administration>Computer Groups** page.

9. If you want to exclude certain computer groups, select **Exclude** and click + to add groups to the list. Select groups that should be excluded from license reclamation. Reclamation will include all monitored devices except those in the groups you select.

10. If you want to send an email to any administrators or other users informing them of a reclamation task’s progress, select **Enable email notification** and type one or more email addresses in the box. Separate multiple addresses with a semicolon (;) or comma (,)

11. When you’ve finished configuring the license reclamation settings, click **Save**.

**NOTE:** Remember that the groups you include or exclude, and the email settings you select, will be applied by default to all reclamation settings. As you create reclamation settings for individual, custom, or normalized products, you can change any of these items.

### Configuring email setting defaults

On the **Administration> Email Settings** page, you can specify which email account will be used to send email notifications when product licenses are reclaimed. Emails are typically sent to administrators or other users who need to know when software has been reclaimed.

**To configure email settings for reclamation notification**

1. Click **Administration > Email Settings**.
2. Type the name of the **SMTP server** that will send the emails.
3. Type the **Sender email address**.
4. Click **Save** to apply the settings.

**Allocating licenses and chargeback costs to a computer group**

Use software license monitoring (SLM) to track the costs of providing IT support to groups across your organization. Track costs by allocating product licenses at the computer-group level and then defining a chargeback price per license for those groups. For more information, see “Viewing license allocation status” (545).

**Setting up allocation units**

Before you can allocate product licenses to a computer group, you need to define that group as an allocation unit. Either select an existing computer group or define a new one that represents a department, locale, or office within your organization. Remember, when you define a group in the SLM console, you’re simply choosing a name to associate with an existing device group or query previously created in the Endpoint Manager network view. For more information, see “Defining a computer group” (525).

**To select an existing computer group as an allocation unit**

1. Click **Administration > Computer Groups**.
2. Select a group in the list. On the toolbar, click **Edit**.
3. Select **Use as allocation unit**. Click **Save**.

**To define a new computer group as an allocation unit**

1. Click **Administration > Computer Groups**.
2. On the toolbar, click **New > Computer Group**.
3. In the **Name** box, give the computer group a distinctive, meaningful name.
4. Select **Use as allocation unit**.
5. In the **Source** selection box, select the defined query or devices that are included in this computer group.
6. Click **Save**.

**Allocating licenses and chargeback costs to a computer group**

After you define a computer group as an allocation unit, you can begin to allocate licenses and chargeback costs.

**NOTE:** If you’re using the **French-language version of SLM**, Microsoft has a bug in their regional settings that affects French-language digit groupings. For numbers of one thousand and over, Microsoft has a default setting of a space character instead of a period for the digit-grouping symbol (for example, 1 234
To allocate licenses and chargeback costs to a computer group

1. Click Products > Monitored.
2. In the list, select a product for which you want to allocate licenses and set chargeback costs. On the toolbar, click Edit.
3. Click Allocations. Under the Computer Group column are the groups you have defined as allocation units.
4. In the Allocated box for a group, select the number of product licenses you want to allocate to that group. This number should represent the number of licenses you plan on charging a group for IT support. Repeat this step for each computer group listed. The Installed column lists the number of devices with the product installed in that group. The Licenses column lists the number of licenses available for use as purchased by that group.
5. In the Chargeback Unit Price box, enter the price per license that you want to charge a group for the IT support of this product. This price will vary by group, depending on the extent of the support you provide.
6. Click Save.

NOTE: Before you can view an accurate printable report about this allocation data, you must save your changes. After clicking Save, return to this dialog, and click the print icon to view the changes in report form.

Viewing license reclamation status

License reclamation tasks are listed on the Products>Reclamation page. You can look on this page to see how many reclamation tasks have started and how many products have been successfully uninstalled to make licenses available.

The license reclamation process runs on the schedule you set for a specific product or in the reclamation defaults. As that process is executed, it creates reclamation tasks. The tasks will run depending on the choices you make:

- If you select the Start scheduled tasks immediately after creation option (in the product details dialog or in Administration>Reclamation Defaults), the task will run after the reclamation process creates the task.
- If you don’t select that option, you’ll need to open the Endpoint Manager Scheduled tasks tool to manually start the task or schedule when it will run.

To fix this problem, you must change the setting in the Control Panel > Region and Language applet. Click the Additional settings button, and change the Digit grouping symbol from a space to a period (or whatever other character you want).
You can view the status of reclamation and export the data to a CSV file to help keep track of the licenses that become available through reclamation. You’ll also see tasks for each product in the Scheduled tasks tool. However, it’s easiest to see the status for a reclamation task on the Products>Reclamation page, where you can also create a report in CSV format of which products have been uninstalled.

To view the status of license reclamation tasks

1. Click Products > Reclamation.
2. To find a product in the list, type at least three characters of the product name in the Search box.
3. Select a product and click Edit to change any of the product’s settings. Click Save.

To save the data in comma-separated value format or as a printable report

1. Click Products > Reclamation.
2. In the product list, select a product and right-click it. Select one of the listed options.

The license reclamation data is listed by product and includes the following columns:

- **Product**: The name of the product. This may be a normalized name that includes different variations of the product name.
- **Task Start Date**: The date the reclamation task is started. (Tasks don’t start automatically unless you select the **Start scheduled tasks immediately after creation** option.)
- **Devices Targeted**: The number of devices that meet the reclamation criteria and thus have been targeted to have products removed.
- **Successfully Uninstalled**: The number of devices from which the product was uninstalled.
- **License Value**: The total cost of licenses that have been reclaimed. This figure is based on the unit price associated with each license.
- **Task Status**: The status of the reclamation task. This status matches the status column in the Endpoint Manager task scheduler. If the status shows **Needs attention**, you’ll need to edit the reclamation task for the product to see what is wrong. The problem will appear highlighted in red.
- **Type**: The computer group type, based on whether it’s created by query or device-group parameters in the database.

Viewing license allocation status

Use the Products>Allocations page to track the costs of providing IT support to groups across your organization. Some groups require more help managing their product licenses than others. By establishing a chargeback cost for the level of support provided, you can bill back that amount to each group, justifying the work you do and controlling asset management costs along the way.
To set up license allocations, you first need to select existing computer groups or define new ones as "allocation units" that represent specific offices, departments, or locales within your organization that you want to bill for IT support. You can then allocate a number of licenses, product by product, to those groups. Allocated licenses are simply an estimate of the number of licenses you think a group will need on a regular basis, most likely based on past support you’ve provided. You can then tie chargeback costs to the allocated licenses. These costs are a monetary estimation of the time and effort you spend supporting products on devices, and they will vary by group. Use this data for reference and reporting.

The Allocations page also shows the actual number of product installations on a group’s devices, the number of licenses purchased by a group, as well as overage. Overage occurs when more products are installed on a group’s devices than the number of licenses you’ve allocated to them. Overage can be useful for seeing if a group has over-installed a product, requiring either the purchase of more licenses or an increase in the number of allocated licenses.

### Getting started

Before you can see license allocation data in the Products > Allocations page, do the following:

- Go to Administration > Computer Groups to edit an existing computer group or define a new one as an allocation unit. You’ll most likely want the group to represent a specific office, department, or locale within your organization. Remember, when you define a group in the SLM console, you’re simply choosing a name to associate with an existing device group or query previously created in the Endpoint Manager network view. For more information, see "Defining a computer group" (525).
- Go to Products > Monitored to edit the products that are associated with the group. While editing a product, you can allocate licenses and the chargeback unit prices for each group defined as an allocation unit.
Viewing license allocation status

To view the status of license allocations within a computer group

1. Click **Products > Allocations**. The groups you’ve defined as allocation units will appear in the list.
2. To find a specific product or group in the list, type at least three characters of the name in the Search box.

The license allocation data is listed by computer group. Expand the group name to see product data in the following columns:

- **Version**: The version number of the allocated product.
- **Installed**: The number of devices with the product installed within a group.
- **Allocated**: The number of product licenses you have allocated to a group; it’s your best estimate of how many licenses a group needs based on the IT support you provide. The allocated number and the chargeback unit price determine the chargeback total.
- **Overage**: The number of devices with the product installed within a group, minus the allocated number of licenses. If these numbers don’t match, the overage appears in red showing that a group has more installations than it was allocated. In this case you may need to allocate the group more licenses, which will increase their chargeback total.
- **Licenses**: The number of licenses available for use, as purchased by a group. A group may have purchased more licenses than it currently needs; the allocated number more closely reflects the true number of licenses being used.
- **Chargeback Unit Price**: The estimated cost of supporting a single license of this product for a group. This cost will vary by group, depending on the type of support you provide.
- **Chargeback Total**: The total chargeback amount for all allocated licenses of this product for a group.
- **Manufacturer**: The name of the product manufacturer.
- **Type**: The type of product installed or the type of computer group, based on whether it’s created by query or device-group parameters in the inventory database.

Creating reports

Once you’ve set up and saved license allocation data so that it appears in the **Products > Allocations** page, you can export the data to a CSV file or print reports that show allocation details for groups, individual products, or multiple ones.
To save data in comma-separated value format or as a printable report

1. Click Products > Allocations.
2. To export data or print reports at the group level, select a computer group in the list (and all of the products under that group) and right-click it. Select Export selected items to CSV or Printable report of search results.
3. To export data or print reports at the product level, expand a computer group in the list. Select one or more product names in the list and right-click. Select Export selected items to CSV, Printable report of allocations for selected product, or Printable report of search results.

Create a report of software license monitoring data

The Ivanti® Endpoint Manager powered by Landesk reporting tool is available for use with the software license monitoring (SLM) console. Use it to create a printable report of the data currently displayed in the console.

When you create a report of the current view, the report contains all currently listed items. The data is organized with the same columns that are displayed in the current view. You can save the report in six different formats.

You can also run predefined reports that are provided with the reporting feature. These reports are listed on the Reports page of the SLM console.

IMPORTANT: If you are using Internet Explorer 9 for the SLM console, you must have Compatibility View turned on to view Endpoint Manager reports. To turn on Compatibility View, open Internet Explorer 9. Press the Alt key to view the menu, and click Tools > Compatibility View settings. Select the Display all websites in Compatibility View check box and click Close.

To create a data report in the console

1. View any product or license data in the SLM console.
3. On the report viewer toolbar, select a report format.
4. To save a copy of the report, click the Export button on the toolbar.
5. Click Browse and select a location to save the file. Click Save, then click Export to save the report.

On some pages, there is a report button that you can click instead of using the toolbar in step 2.
To run a predefined report

1. In the SLM console, click Reports.
2. Click Reports > Standard reports > Software license monitoring and find the report you want.
4. On the report viewer toolbar, select a report format.
5. To save a copy of the report, click the Export button on the toolbar.
6. Click Browse and select a location to save the file. Click Save, then click Export to save the report.
Unmanaged device discovery

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 Ivanti agent**: Looks for the standard Ivanti agent (CBA) on computers. This option discovers computers that have the Ivanti 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 off, or what state the OS may be in.
- **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 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 them.

**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 Ivanti network. The XDD agent on a configured device then checks to see if the broadcasting device has the standard Ivanti agent installed. If the standard Ivanti 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.

For information on enabling XDD on clients, see "Self-electing subnet services" (119) and "Configuring devices to use extended device discovery (ARP and WAP)" on page 555

---

**NOTE:** Use extended device discovery to discover firedalled 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. 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.

---

**Related topics**

"Deploy Ivanti agents to unmanaged devices" (559)

"Discover unmanaged devices with UDD" (557)

"Work with devices found through XDD" (553)

"What happens when a device is discovered" (551)

"Use extended device discovery (with ARP and WAP)" (554)

Unmanaged device discovery help

---

**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).
- **Find results:** Contains search results.
- **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.

**NOTE: 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 Ivanti 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 Ivanti agent**: Shows whether the device has CBA on it. You can deploy other Ivanti 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.
- **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 an Ivanti 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 Ivanti 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.

If you want to delete all devices from multiple groups in one step, click the Remove items in groups toolbar button and select the groups you want all devices removed from.

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 Ivanti 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.

**Work 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.
Exporting and importing discovery exceptions

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. Select the CSV file, and click Open.

Use extended device discovery (with 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 Ivanti 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 timeout period. Even devices that generate a lot of ARP traffic are only pinged once per timeout period.
Devices with Ivanti agents on them are assumed to be managed and aren’t reported to the core server. Devices without Ivanti 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

**NOTE: Reporting the MAC address**

XDD uses the wireless detection API on devices running Windows 7 and later to obtain the device MAC address and display it in the list view.

### Configuring devices to use extended device discovery (ARP and WAP)

XDD uses self-electing subnet services (SESS) for extended device discovery. Once SESS is enabled on a subnet, devices will:

- Self-organize on the same subnet to provide services, allowing automatic fail-over and avoiding duplication of services.
• Use a smart election process that ranks available devices by configuration and ability to provide the service.
• Trust each other if they report to the same core server.
• Use signed messages for SESS security purposes (to avoid impersonation).
• Use the same client certificates used for CSA access.

For more information, see "Self-electing subnet services" (119).

You can use the Agent settings tool and the Self-electing subnet services tool to enable ARP and WAP discovery. ARP discovery is enabled by default on managed Windows devices.

Note that for SESS to function, both the deployed SESS agent setting and the desired network state in the Self-electing subnet services tool must both be enabled. If you don’t enable the SESS service you want in the deployed agent settings, enabling SESS for that service in the Self-Electing subnet services tool won’t have an effect because there won’t be electable devices on the subnet.

To deploy the extended device discovery agent for ARP and/or WAP discovery

1. Click Tools > Configuration > Agent settings.
2. In the Agent settings tree, click My agent settings > Client connectivity.
3. Click the New toolbar button.
4. Enter a configuration Name.
5. On the Self-electing subnet services page, make sure Enable self-electing subnet services is selected.
6. On the Extended device discovery page, configure the options you want.
7. Deploy the agent setting to all devices on each subnet. SESS will manage which devices do discovery.
8. Click Tools > Configuration > Self-electing subnet services.
9. Under the Self-electing subnet services tree, click Extended device discovery (ARP). Right-click the subnets you want to enable and click Enable.
10. If you want WAP discovery, repeat step 9 for Extended device discovery (WAP).

Understand IP address filtering with Extended Device Discovery (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.

**Maintain 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.

**Discover 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 options you want. The default discovery type uses a standard network scan with IP OS fingerprinting of discovered devices.

3. Enter a starting and ending IP range for the scan. You must enter a range for Standard Ivanti 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 dialog boxes.

8. Click Computers in the UDD tree to view the scan results.
Configure 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 user name 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.

Deploy Ivanti agents to unmanaged devices

After you’ve discovered unmanaged devices using the scan and discovery methods described above, you can deploy Ivanti 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 Ivanti agent. If the devices have the standard Ivanti agent, you can do a push-based deployment.
- Pull-based deployment using a login script.

For more information on deploying devices, see the Ivanti User Community at https://community.landesk.com.

When organizing devices for agent deployment, you may find it easier to sort the unmanaged device list by the standard Ivanti agent to group for standard Ivanti agent device deployments and to sort by domain for scheduled task deployments.

NOTE: 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 Ivanti 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 Ivanti 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.

### Use 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 Ivanti agent is either disabled or not working.
- **History of ARP discovered devices without the agent**: History of devices where the Ivanti 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.

### Restore 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 Ivanti 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 that 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.

**Discovering VMWare ESXi virtual hosts**

Unmanaged device discovery can discover VMWare ESXi 3, 4, and 5 virtual hosts. The discovery process is agentless and doesn’t require that you install anything on the ESXi hosts. You will have to configure a single, common set of credentials for the ESXi hosts that you want to discover. The discovery process uses these credentials to connect to the host and remotely scan it.

Here’s an overview of the configuration and scanning process:

1. Add an account to your ESXi hosts. Make sure all hosts share the same user name and password for this account.
2. Enter the shared account credentials in **Tools > Configure Services** on the **OS Virtualization** tab.
3. Run an unmanaged device discovery scan. Make sure you’ve selected **Discover virtual hosts**.
   For more information, see “Discover unmanaged devices with UDD” (557).
4. Discovered ESXi hosts appear in the UDD **Virtual hosts** tree item.
5. Select the discovered hosts, right-click them, and click **Copy to inventory database**.
6. Manage the discovered hosts by clicking **Network View > Virtual OS hosts > All virtual OS hosts**. Right-clicking one shows you the available options.

**Discovery problems with VMWare ESXi hosts using default self-signed certificates**

When installing ESXi, you have the option of using a built-in, self-signed certificate. The problem with this certificate is that the ESXi hostname defaults to “localhost” and the hostname won’t be unique on the network or to UDD. UDD treats all hosts with the same hostname as a single host, resulting in a single entry in the inventory database for all hosts sharing that hostname.

VMWare strongly recommends that you not use the self-signed certificate in a production environment. For virtual host discovery to work correctly, all ESXi installations must have a unique CA-signed SSL certificate and hostname. See the following links for more information:

- [http://kb.vmware.com/kb/2034833](http://kb.vmware.com/kb/2034833)
**Troubleshoot 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 <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 Endpoint Manager’s nmap-services document (C:\Program Files\LANDesk\Management Suite\nmap\nmap-services) and comment out the ports with a hash (#) character that consistently respond.
Provisioning

Provisioning overview

Ivanti provisioning allows you to 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 Mac; 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. Ivanti provides pre-built provisioning templates to get you started. You can combine these provisioning templates with your own master templates. You can also 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 also use provisioning to reconfigure a device from one purpose to another, changing a device's base function to handle your organization's changing demands.

Provisioning is also very useful for OS migration. You can capture a profile from a previous OS and then deploy a new OS with the same profile and previously installed software applications. You can even automatically do the same from an older computer to a newer computer, as well as upgrade application versions on the fly.

You can use alerting to let you know when provisioning events occur.

Provisioning agent

The center of provisioning is the agent ldprovision, located in the core server's ldlogo/provisioning folder. This agent consists of small applications for each action. The agent needs to reside on the target device, which you can place there through a PXE server, a virtual boot (vboot), or 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 server.

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 use provisioning in full, users are required to have the provisioning role in User management. These rights are automatically enabled for any users with Administrator rights and can be enabled for any other users.

**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; however, CD or USB drives are highly portable and guarantee that the computer running the preboot environment is the one you 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 preboot environment.

You don’t need unique boot media for each client system; you can re-use the boot media for other devices.

**The provisioning interface**

The provisioning tools are a part of the operating system deployment tool (click Tools > Provisioning > OS provisioning). A tree structure displays provisioning templates, and a toolbar opens dialog boxes for different tasks.

![Operating system provisioning](image)

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. This instance can’t be deleted, but it can be hidden.

The right pane displays the selected folder’s templates, with 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.

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 that apply specifically to this template, view and modify the list of templates included by this template, or view and modify the list of templates that include the template. You can also make a template public, view its history (when the template was executed), and view or modify the template’s XML code.

You can open multiple templates at once and use copy and paste (CTRL+C and CTRL+V) to copy actions you’ve configured between open templates. The template window is also resizeable.

**Creating and editing provisioning templates**

The **New template** toolbar dropdown is the starting point for creating a new template. Pre-configured Capture and Deploy wizard templates are available that only take a minute to configure. These preconfigured templates automatically support normal and UEFI BIOS booting and device provisioning. Default actions are automatically added to support basic image capture or deployment. If necessary, you can further customize capture and deploy templates on your own.

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 you use a template, you can’t change it directly. However, you can clone and change it. 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**

Each template has a **Condense** right-click menu option to combine multiple templates into one template. This feature is useful when you want to simplify a template for export or make one public.

If other templates are included within the current parent template, condensing will merge their XML code with the XML code of the parent template to create a single XML file—the parent will no longer have dependencies. Once a template is condensed, it’s a new template, and you can’t expand it 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: Create a template**

To provision a device, you first 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.

You can chain multiple templates together in a provisioning task so that they run in a particular sequence. You can also change the action order in a template where applicable (for example, you can’t place a post–OS task before the installation of the OS). To get you started, provisioning comes with numerous pre-configured templates for various vendors (HP, Dell, and so forth).

Templates are saved in the core database as XML documents.

For more information, see "Creating templates" (567).
**Step 2: Configure the template**

Once you create the template, you must configure it by adding actions that are ordered into five sections:

1. System migration
2. Pre-OS installation
3. OS installation
4. Post-OS installation
5. System configuration

You can only select actions in each section that apply to that section (for example, you can’t select Software distribution as an action for the Pre-OS 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 wrong order.

For more information, see "Configure a provisioning template" (571).

**Step 3: Schedule 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 core database so that the configuration history remains attached to the computer. Configuration tasks can’t be reused with different target devices, but they can be reused by specifying another device identifier.

The **Scheduled tasks** tool shows the 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 (which 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, see "Schedule a provisioning task " (577)

**Creating templates**

Use the **New template** toolbar button to create a capture image 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 can’t be changed where it does not make sense (for example, you can’t place a post-OS-specific action before the installation of the OS).

Templates that you create through the **Capture template** and **Deploy template** toolbar options are pre-populated with default actions the template needs to work. No additional customization is necessary and you can immediately use a template after you create it. Of course, you can still customize these templates for your environment and needs, if necessary.
To create a capture template

1. Click **Tools > Provisioning > OS provisioning**.
2. Under the **Provisioning templates** group, select either the **Public** or **My templates** folder.
3. On the toolbar, click **New template > Capture template**.

![Create Capture Image Template](image)

4. In the **Template name** box, type a descriptive name.
5. In the **Template description** box, type a description. The Name and Description are displayed in columns in the list of templates.
6. Select the **Image type** that you want to create.
7. Specify the UNC file path to the image file, including the name of the image file:
   \`\`\MyPreferredServer\Images\Win7Capture.tbi\`\`
   - Click **Browse**.
8. Click **Create**.

To create a deploy template

1. Click **Tools > Provisioning > OS provisioning**.
2. Under the **Provisioning templates** group, select either the **Public** or **My templates** folder.
3. On the toolbar, click **New template > Deploy template**.

![Create Deploy Image Template](image)

4. In the **Template name** box, type a descriptive name.
5. In the **Template description** box, type a description. The Name and Description are displayed in columns in the list of templates.
6. Select the **Image type** that you will use for deployment.
7. Specify the UNC path to the image file, including the name of the image file.
8. Select the **Agent configuration name** that you want installed on the destination device.
9. Select the unattended installation **Script name** you want used during the OS installation and the target path and filename for the script on the destination device.
10. If you want to use hardware-independent imaging for driver installation, select that option.
11. Click **Create**.

To change template properties, double-click the template or right-click the template and select **Properties**.

**To create a Mac deploy template**

1. Click **Tools > Provisioning > OS provisioning**.
2. Under the **Provisioning templates** group, select either the **Public** or **My templates** folder.
3. On the toolbar, click **New template > Mac deploy template**.

![Create Mac Deploy Image Template](image)

4. In the **Template name** box, type a descriptive name.
5. In the **Template description** box, type a description. The Name and Description are displayed in columns in the list of templates.
6. Enter the smb:// or afp:// path for the Mac image file. UNC paths aren't supported with Macs.
7. If you want to also include a Bootcamp Windows image file with the deployment, select **Include Windows image**.
8. If you want to include a profile, enter a **Profile** path.
Configure a provisioning template

Follow these steps to configure a template.

To configure a provisioning template

1. In the OS provisioning tree, double-click a provisioning template.
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 when migrating a device to other hardware or a virtual machine. For example, this section can include an action to capture profile information when migrating to Windows Vista.
• **Pre-OS installation:** Actions that are performed when the device boots into a pre-installation environment (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 (Windows PE) when the OS is installed.

• **Post-OS Installation:** 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 to this section.

4. Click **Add**.
5. In the **Name** field, type a specific name for the action.
6. In the **Description** field, type a detailed description of the action.
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**.

**Edit a template's XML code**

1. Click **Tools** > **Provisioning** > **OS provisioning**.
2. Select **Public** or **My templates** or one of their subgroups.
3. Double-click a template. In the Template view, click **XML**.
4. Make changes to the XML code for the template.
5. To save changes, click **Save changes**.
6. To export a copy of the template, click **Export** and specify a file location.
7. Click **OK** to close the Template view.
Provisioning templates are structured using the following general XML format.

```
<template name=
<description></description>

<section name=
<description></description>
<action></action>

</section>

<section name=
<description></description>
<action></action>

</section>

</template>
```
Delete a provisioning template

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 core database.

To delete a provisioning template

1. Click Tools > Provisioning > OS provisioning.
2. Under the Provisioning templates group, select either the Public or My templates folder.
3. Select a template, and click Delete.
4. Click Yes.

Sharing templates

Use the Import templates toolbar button to import templates in XML format. When you import a template, a copy of the template is saved in the My templates folder. You can then edit the template’s XML to make changes to it.

You can also export a template to save it as a new file and then share that template file with others.

To import a template

1. Click Tools > Provisioning > OS provisioning.
2. On the toolbar, click the Import templates button.
3. In the Import file box, type the path and filename of the XML file, or click Browse and select the file.
4. Click Import. This imports the template into the My templates folder.

The file is saved as an .xtp (XML template page) file. In the My templates folder, the imported template is listed with the original filename, followed by the date and time of import.

To export a template

1. Click Tools > Provisioning > OS provisioning.
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 where you want to save the template, and click Save.

The file is saved as an .xtp (XML template page) file. If you’re 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.
Provisioning template groups

Use provisioning template groups to organize your templates in various ways. For example, you can create groups based on specific vendors and create 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 template group

1. Click **Tools > Provisioning > OS provisioning**.
2. Select **Public** or **My templates**.
3. On the toolbar, click the **Create a template group** icon.
4. Type a group name and description.
6. Click **OK**.

To delete a group

1. Select a group, and click the toolbar’s **Delete** icon.
2. Click **Yes**, and then confirm that you want to delete the group.

**NOTE:** 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.

Using installation scripts in provisioning templates

Use the Install scripts tool (**Tools > Provisioning > OS Provisioning**) to create a template out of one or more installation scripts, which can then be used for scripted installation actions in templates. Provisioning supports batch file scripts, shell scripts, and many others.

The Deploy image, Scripted install, and Inject script actions use scripts like sysprep.inf or unattend.txt. You can use the Install scripts tool to insert variables into your scripts; for example, a device name can be inserted into a sysprep.inf file.

Using variables

Install scripts supports many key value pairs, such as:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ldHostname%</td>
<td>The host name</td>
</tr>
<tr>
<td>%ldDeviceID%</td>
<td>GUID of the device</td>
</tr>
</tbody>
</table>
If the win.inf file already has a key value pair that exists as a user-defined variable, Install scripts will replace it with the new 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\dlogon\provisioning\config folder to see the installation script with the variables replaced. Access this folder any time you need to troubleshoot after modifying a script or using a script in the Inject script or Deploy image actions.
- The temporary directory used for provisioning is %systemdrive%/ldprovisioning.

**Import and export installation scripts**

**To import an installation script**

1. Click **Tools > Provisioning > OS provisioning**.
2. On the toolbar, click **Tools > Install scripts**.
3. In the **File name** box, type the path and filename of the script or click **Browse**, navigate to the script, select it, and click **Open**.
4. In the **Script name** box, type a name for the script. This name will display in the **Install scripts** list in this dialog box. The name is also displayed in the **Installation scripts** list when you add a Scripted install action to a provisioning template.
5. In the **Description** box, type additional details about the script.
6. In the **Target operating system** list, select the target operating system.
7. Select the **Insert variables into script** check box if you want to swap out variables during the script import. When variables are replaced, public variables 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 filename and location and click **Save**.

**Schedule a provisioning task**

**To schedule a provisioning task**

1. In the **OS provisioning** tool, select a template from one of the **Provisioning templates** folders.
2. Click the **Schedule template** toolbar button.

   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 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 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 Endpoint Manager 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** (Endpoint Manager administrative users only): All tasks users have created.

**User notifications when a task is running**

When a provisioning task is running on a device and the provisioning actions include a reboot, the task continues to run after the device reboots. The user is prompted to log in after the reboot, and when the login is complete, a status message reports on the progress of the task.

If the user is not logged in when the provisioning task begins, the task runs without user input. If there is a reboot action, the task will continue to run without the user logging in.

If the user logs in to the device while the provisioning task is in process, a status message reports that a task is in process and gives the progress of the task. Note that status messages are updated only between actions. If a task is working on a long action, such as installing a large application, it may appear that the progress bar is not moving. However, when the action is completed, the status will be updated.
About the Machine Mapping tool

Use the Machine Mapping tool (Tools > Provisioning > Machine Mapping) to map one device to another. This is used for OS provisioning when migrating users from one device to another.

This tool has the following options:

- **Days Valid**: Sets the number of days the machine mapping will be assigned.

  The use case for this setting is to create a safety feature. If a machine mapping is used, the Last Used field populates with the date and time the OS Provisioning template used the machine mapping. With the field populated, the Days Valid field is put into effect. If an OS Provisioning task tries to use the mapping beyond the setting in the Days Valid field, the mapping is ignored. You likely do not want the mapping to be valid months from now when the task might run unexpectedly on a device, overwriting its hard drive.

- **Remove**: Deletes the assignment of the **Source** and **Destination** devices.

- **Reset Used**: Removes the contents of the Last Used field.

- **Refresh**: Refreshes the Machine Mapping tool view to show mappings that have been used by OS Provisioning templates being run.

- **Search**: Allows you to search for a device to place it in the **Source** and **Destination** columns.

- **Source**: The machine that is being replaced with another device. (This would be the old device.)

- **Destination**: The machine that is replacing another device. (This would be the new device.)

- **Last Used**: The date and time the machine mapping assignment was last used. (Populating this field activates the Days Valid setting, so the machine mapping assignment will be ignored if the number of days set in the Days Valid field have passed.)

Provisioning device naming templates

The Device naming tool (Tools > Provisioning > OS Provisioning) enables you to create unique device names using device-naming templates. The naming template can use truncated core database values and a multi-character incrementing numeric sequence. You can create multiple templates and use the Device Name Prompter action to select the name template you want. Name length can’t exceed 15 characters.
The **Template** field shows the template you are building. Customize a variable or number sequence and click **Insert** to add that item to the Template field. You can also type custom elements or make other adjustments directly in the **Template** field.

In the example above, the naming template uses the beginning 5 characters of the `%ldHostname%` value, with a hardcoded location of `_slc_`, followed by a 3-digit zero-padded number sequence that will increment automatically.

The core server tracks the number used in each naming template and automatically increments that number (starting at 1) each time a device is named.

**Define the image store location and tool**

The image location is specified in the template under **OS installation > Capture image** or **Deploy image**. This location must be on a Endpoint Manager preferred server and the preferred server must be configured with credentials that allow read/write access. For more information, see “Configuring preferred servers” (964).
Product to package mapping

Use the Product-to-package mapping tool (Tools > Provisioning > OS Provisioning) to map applications detected on source devices to applications found in software distribution packages you’ve created. You can then use provisioning to automatically install those detected applications onto newly provisioned destination devices.

The list of applications that can be detected comes from the Software license monitoring tool’s monitored products list. When the inventory scanner runs on a device, it gives the core server a list of applications from the list that it found on the device. Only products that you’ve added to the monitored products list are available for product-to-package mapping.

The Customize mapped software action requires a technician to customize mappings at a device while it’s being provisioned. For more information, see “Customize mapped software (all sections)” (602).

The Install mapped software action takes a snapshot of the currently installed products from inventory when the scheduled task is started. This allows the inventory to persist after the device is imaged and a new agent is installed. The snapshot of inventory is cleared once the scheduled task is deleted. The task can be restarted or rerun as long as the task is not removed. For more information, see "Install mapped software (System configuration section only)” (608).

You can map any software distribution package to an item in the monitored products list. For example, if Office 2003 is a monitored product, in smart migration, you could map it to an Office 2013 distribution package.

Products can have the following mapped states:

- **Disable**: Product will not be installed on new devices and won't be available in the Customize mapped software action.
- **Critical**: If a mapping is critical and the package fails to install for some reason, the whole provisioning job will fail and quit. If you don’t make a mapping critical, OS provisioning will try to install the application and then it will keep going even if the install fails.
- **Customizable**: During provisioning, allows a technician at the provisioned device to select whether each customizable mapping will be installed. The provisioning template must have a Customize mapped software action for this to work. This action usually goes at the beginning of the template. If a technician doesn’t make any selections, the action will eventually time out and customizable packages that were on the source device will be installed on the new device.

To map products to packages

1. Click Tools > Provisioning > OS provisioning.
2. On the toolbar, click Tools > Product to package mapping.
3. On the left side, select the monitored product that you want to map.
4. On the right side, browse the list of available distribution packages that you’ve created, and
select the one you want.

5. Click Assign.

**Provisioning bare metal devices**

Provisioning enables you to provision bare metal devices. You can begin this process before a device is physically present. To do so, enter a hardware identifier (such as the GUID, serial number, or MAC address) for each new device by accessing the Configuration > Bare Metal Devices folder in the network view. You can add several devices at once by importing a list of device IDs using a CSV file. The information required by the automated provisioning agent (ldprovision) is recorded in the core database.

**To provision bare metal devices**

1. In the network view, click Configuration > Bare metal devices.
2. Right-click in the device list and select Add devices.

3. To enter data manually 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). Select a type from the Identifier type list. Type the identifier for each device and click Add to add it to the list.

4. To import device data from a CSV file, 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.

5. Associate each device with a provisioning template.

6. Plug in the devices and provide them an ldProvision boot CD or bootable USB drive, or configure a BIOS to network/PXE boot.

7. Power up the devices.
USB-based disconnected provisioning templates

If you want to provision devices that can’t see a core server or that use slow WAN links, you can create a disconnected provisioning template on a USB thumb drive. When you do this, OS provisioning makes the thumb drive bootable and copies the necessary files, such as Windows PE, drivers, the OS image you’re deploying, and so on, to the USB drive.

When using a disconnected provisioning template, any template actions that require a core server will still fail if the device can’t see the core server. This includes software distribution and patch actions.

To create a USB-based disconnected provisioning template

1. Connect a USB drive with enough space to hold your image and the provisioning files.
2. Click Tools > Provisioning > OS Provisioning.
3. In the Provisioning templates tree, right-click the provisioning template you want and click Create disconnected template.
4. Select the drive letter your USB drive is using.
5. Click Create and wait for the file copying to finish.

Changing the Windows PE image drivers and wallpaper

Provisioning uses a Windows PE image to image devices. Endpoint Manager ships with 32-bit and 64-bit versions of this image. If necessary, you can add drivers to the base Windows PE images. Drivers you add there will be available on any device booting the image. If you want drivers for a specific device, consider adding them through hardware-independent imaging. For more information, see "Hardware-independent imaging overview" on page 624

To add drivers to the base Windows PE image

1. Click Tools > Provisioning > OS provisioning.
2. On the toolbar, click Preboot > Manage drivers in WinPE image.
3. Select the image you want to have the drivers, 32-bit WinPE, 64-bit WinPE, or a custom image you’ve provided.
4. Click Next. Wait for provisioning to process the image file you selected.
5. Click Add.
6. Give the driver a name and browse for the driver’s .inf file.
7. Click OK and then Finish.

To change the Windows PE wallpaper (visible while devices are being imaged)

1. Click Tools > Provisioning > OS provisioning.
2. On the toolbar, click Preboot > Change WinPE wallpaper.
3. Select the image types that should use the new wallpaper (32-bit and 64-bit).
4. Browse for the wallpaper file. The file's resolution should be 1024x768 for best results.

5. Click OK.

**Re-branding the provisioning client interface**

The provisioning client interface on devices being provisioned defaults to Ivanti branding. You can change that branding if you want. Re-brandable elements are:

- **Title:** Appears on the main provisioning user-interface window.
- **Banner image:** Appears at the top of all provisioning windows on provisioned devices.
- **Interface colors:** Changes the window background (background color) or the interface text color (foreground color).

This re-branding only affects provisioning dialog boxes. Other Endpoint Manager windows and dialog boxes won’t be affected.

You can re-brand the provisioning interface globally or you can re-brand it on the individual template level. Re-branding done at the template level overrides the global re-branding.

**To re-brand the provisioning UI globally**

1. Click **Tools > Provisioning > OS Provisioning**.
2. On the toolbar, click **Tools > Branding**.
3. Change the branding elements you want and click **OK**.

**To re-brand a template**

1. Double-click the template you want to re-brand.
2. On the left, click **Options**.
3. Change the branding elements you want and click **OK** or **Apply**.

**Provisioning history**

The Provisioning history option enables you to view the history of a provisioning template. You can check on the status of a particular task, determine how a particular device was provisioned, or find out which devices were provisioned with a particular template. When a system is provisioned, all the actions (successful and failed) 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 > Provisioning > OS provisioning.
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.

NOTE: 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.

NOTE: To get the current status of a template that is in the process of executing, click the Refresh button to update the history status.

Cleaning up the provisioning history

You can specify how many days of provisioning history that you want to keep. The default is to keep all of it. If you enable this option, the provisioning history database data older than the number of days you specified will be deleted. Deleted provisioning data won’t include items that are part of a task that’s visible in the Scheduled tasks window.
To clean up the provisioning history

1. Click **Tools > Provisioning > OS provisioning**.
2. Under the **Tools** toolbar menu, select **Provisioning settings**.
3. Select **Automatically cleanup provisioning history**.
4. Enter the number of days that you want to keep.
5. Click **OK**.

Operating system provisioning for Macintosh devices

Ivanti® Endpoint Manager powered by Landesk OS provisioning fully supports Mac OS X devices. For detailed information, see this document on the Ivanti community:

- Step-by-Step Process, Including Videos, for OS X Provisioning in Ivanti® Endpoint Manager powered by Landesk 2016 ([https://community.landesk.com/docs/DOC-40085](https://community.landesk.com/docs/DOC-40085)).

Provisioning template variables

Template variables allow for greater portability and customizability in templates. For example, a template may contain very specific filenames to copy, paths to install to, or an IP address to export files from. But with 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):

1. **Device**: Variables assigned to a specific device.
2. **Global**: Variables that are public (available) to all templates.
3. **Template**: Variables that only apply to a specific template.
4. **Action**: Variables that only apply to a specific action in a specific template.

Variables are case-sensitive. It's imperative that you match case when implementing variables.

Related topics

"Define a device variable" (586)
"Define a public (global) variable" (587)
"Define a template variable" (588)
"Define an action variable" (590)
"Creating unique identifiers for new devices " (591)
Define a device variable

1. In the network view’s All devices list, right-click a device and select Manage variables.

2. In the Name box, type the item you want to add as a variable (such as IPAddress). Use quotation marks around names with spaces. Names are case-sensitive.

3. In the Value box, type the replacement value. You can use most values found in the core database. Use quotation marks around values with spaces. Values are case-sensitive.

4. Select the variable type:
   - **String**: An alpha-numeric string value.
   - **Database value**: A database ID string, such as Computer.Network."NIC Address".
   - **Sensitive data**: A value to be encrypted in the core database.

5. Click Add and OK.
Define a public (global) variable

Use Public variables to view and set global variables that apply to all provisioning templates. Such variables are used to customize template filenames to copy, paths to install to, or IP addresses to export files from. User-defined variables (variables that apply to only one template) take precedence over public variables.

To create unique identifiers for new devices, see "Creating unique identifiers for new devices " (591)

1. Click Tools > Provisioning > OS provisioning.
2. On the toolbar, click Tools > Public variables.

3. To add a variable, click Add.
4. In the Search value box, type the item you want to add as a variable (for example, CoreIP). Use quotation marks around names with spaces. Names are case-sensitive.
5. In the **Replacement value** box, type the value you want as a replacement (for example, if the search value is CoreIP, type the IP address you want to replace CoreIP). You can use most values from the core database. Use quotation marks around values with spaces. Values are case-sensitive.

6. Select the variable type:
   - **String**: An alpha-numeric string value.
   - **Database value**: A database ID string, such as Computer.Network."NIC Address".
   - **Sensitive data**: A value to be encrypted in the core database.

7. Click **OK**.

Database value lookups are handled by adding a ldbnf: prefix to the Replacement value. The database table and key pair can then be used to look up a specific entry in the core database. The ldDeviceID public variable that is configured by default is an example of how to add a database value.

**Define a template variable**

1. Click **Tools > Provisioning > OS provisioning**.
2. Right-click a template and click **Edit**.
3. In the right pane, click **Template variables**.
4. Click **Add**.

5. In the **Search value** box, type the item you want to add as a variable. Use quotation marks around names with spaces. Names are case-sensitive.

6. In the **Replacement value** box, type the value you want as a replacement. You can use most values from the core database. Use quotation marks around values with spaces. Values are case-sensitive.

7. Select the variable type:
   - **String**: An alpha-numeric string value.
   - **Database value**: A database ID string, such as `Computer.Network."NIC Address"`.
   - **Sensitive data**: A value to be encrypted in the core database.

8. Click **OK**.
Define an action variable

1. Click **Tools > Provisioning > OS provisioning**.
2. Right-click a template and click **Edit**.
3. In the right pane, click **Action list** and select a section in which you’ll define the variable.
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**.

6. In the **Search value** box, type the item you want to add as a variable. Use quotation marks around names with spaces. Names are case-sensitive.
7. In the **Replacement value** box, type the value you want as a replacement. You can use most values from the core database. Use quotation marks around values with spaces. Values are case-sensitive.
8. Select the variable type:
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%
```

Related topics

"Provisioning template variables" (585)

"Define a public (global) variable" (587)

Provisioning template conditionals

Provisioning supports conditional If/Else statements that can help you control template flow. The result of an action determines whether the template branches or not. You can use any action with a conditional. Branch nesting isn't allowed. Else conditionals require an If, but you don't have to use an Else. You can add multiple actions to If and Else conditionals.

The Compare variable action is useful for conditionals. The example below shows a template that uses conditionals to support both laptops and desktops. The variable comparison to check the device type is system.chassisType=Laptop.
To add a conditional to a template

1. With a template view open, right-click the template section you want configure and click Add condition > If. The If condition will be added and selected.
2. With the If condition selected, click Add and select the action you want. The result of that action determines if child actions will be executed.
3. If you want an Else, you can add and configure it the same way by right-clicking the template section and clicking Add condition > Else.

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 include a template, its boot environment and target OS must match the template setting of the parent template.

To add a template to the current template

1. Click Tools > Provisioning > OS provisioning.
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, select the template and click Remove.

Not Applicable is treated as a wildcard.
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 > Provisioning > OS provisioning.
2. Under Provisioning templates, click Public or My templates to display templates.
3. Double-click a template.
4. Click Included by.

Adding actions to a provisioning template

You can create new actions or edit existing ones for your provisioning 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 into five sections, which are:

- System migration
- Re-OS installation
- OS installation
- Post-OS installation
- System configuration

In each section, you can only select actions that apply to that specific section (for example, you can’t select Software distribution as an action for the Pre-installation section). You can add any available action to a section, but be aware that some actions will break the template or may render your system unusable if completed in the improper steps.

For tables that show the action types and where they fit into sections by default, see "Provisioning template action types" (595).

Each template has a Condense right-click menu option that rewrites the current parent template to incorporate all actions from its included templates. Condensing merges the XML code of all included templates with the XML code of the parent template to create a single XML file—the parent no longer has dependencies.

This feature is useful when you want to simplify a template for export or make one public. Once a template is condensed, it’s a new template, and you can’t expand it into separate templates again.

To add actions to a template

1. Click Tools > Provisioning > OS provisioning.
2. Under Provisioning templates, click Public or My templates to display templates.
3. Double-click a template.

4. In the Template view, click **Action list**.

5. Click the section you want to add an action to:

   - **System migration**: Features and components that need to be saved before modifying the system or migrating a device to other hardware or a virtual machine. For example, this section can include an action to capture profile information when migrating to a newer version of Windows.

   - **Pre-OS installation**: Actions that are performed when the device boots into a pre-installation environment (Windows PE). For example, on a server you would add RAID configuration in this section.

   - **OS Installation**: Actions that are performed in the pre-installation environment (Windows PE) when the OS is installed. For example, deploying an image to the disk.
- **Post-OS Installation**: Actions that are performed in the target operating system after it has been installed, such as performing hardware-independent imaging to install a driver.

- **System configuration**: Additional application installation/execution and system configuration in the installed OS. For example, installing the Ivanti agent and other software installation tasks in this section.

6. Click **Add**.

7. In the **Name** box, type a specific name for the action.

8. In the **Description** box, type a detailed description of the action.

9. From the **Type** list, select an action type. The type determines what options you'll need to specify for the action.

10. If you want to add a variable that applies to this action only, under **Action variables** click **Add**.

11. Select **Stop processing the template if this action fails** if you want to define an action as essential to the provisioning task. If the action can be ignored, clear this check box.

12. When finished, click **OK**.

Provisioning supports conditional If/Else statements that can help you control template flow. For information about adding conditional statements to actions within templates, see "Provisioning template conditionals" (591).

### Provisioning template 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.

<table>
<thead>
<tr>
<th>Action name</th>
<th>System migration</th>
<th>Pre-OS installation</th>
<th>OS installation</th>
<th>Post-OS Installation</th>
<th>System configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture image</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Capture profile</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change agent settings</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Compare variable</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Configure agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Configure target OS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Control service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Action name</td>
<td>System migration</td>
<td>Pre-OS installation</td>
<td>OS installation</td>
<td>Post-OS Installation</td>
<td>System configuration</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>----------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Copy file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Create directory</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Customize mapped software</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Delete file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Deploy image</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy profile</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Device name prompter</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Distribute software</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Download file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Download from preferred server</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Execute file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hardware-independent imaging</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Inject script</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Install mapped software</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Install service</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Join domain</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Launch template</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Map/Unmap drive</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Map/Unmap drive to preferred server</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Partition</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Patch system</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Reboot/Shutdown</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Replace text</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Scripted install</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
### Mac OS X action types

The table below shows actions you can use with Mac OS X devices.

<table>
<thead>
<tr>
<th>Action name</th>
<th>System migration</th>
<th>Pre-OS installation</th>
<th>OS installation</th>
<th>Post-OS Installation</th>
<th>System configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture image</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capture profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Change agent settings</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Compare variable</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Configure agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Configure target OS</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Copy file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Create directory</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Customize mapped software</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Delete file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Deploy image</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Deploy profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Device name prompter</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Distribute software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Download file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Execute file</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
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.

- **Select the image type**: Select the type of image you want to capture. If you select Symantec or Other, you will also need to provide a path to the application used for imaging.
- **Specify the UNC path to the image file**: Enter a UNC path to the image that is captured, including the image file name. Configure your preferred server with valid credentials to the share for the image file path. This option is used only when you select Symantec or Other as the image type.
- **Specify the UNC path to the imaging tool**: Enter a UNC path and file name for the imaging application. This option is used when you select Symantec or Other as the image type.
- **Command-line parameters**: Enter any command-line parameters that will customize the way the image is captured.
- **Validate**: Click this button to generate a default command line for the imaging tool and path you specified. You can add other command-line parameters after you click Validate, but if you have already entered any custom parameters they will be removed when you click Validate.

**Capture Image (Mac OS X, OS installation section only)**

Use this action to capture a Mac OS X image from a target device. The capture image action uses preferred server credentials to authenticate to the shares. This is set in the Content replication / Preferred servers tool. A Mac OS X server has to be set as a preferred server for this to work. The **User name** and **Password** fields in the core server’s preferred server properties are used to access the shares. The options available for this action include:

- **Specify the path to save the image file, including the name of the image file**: To enter the location to capture and store the image file. Either smb://Server/SharePoint/ImageFile.dmg OR afp://Server/SharePoint/ImageFile.dmg format can be entered into this field.
- **Mac image**: Captures the Mac image.
- **Windows image**: Captures the Windows Bootcamp image.
- **Validate**: Click this button to populate the **Command-line parameters** field with the data provided in the other fields.

**Capture profile (System migration section only)**

This action runs the user migration assistant to capture one or more profiles. To use this action, you need to know where the user migration assistant command XML file is located on the core server and where saved profiles are to be stored.

You can use unique identifiers to name profiles when they are saved, or you can specify a full filename for the profile.

To use the user migration assistant, managed devices must have the standard Ivanti agent, which includes the inventory scanner, local scheduler, and software distribution agents. Profile migration uses the software distribution agent to distribute files.

- **Select user migration assistant command XML file**: Specify the location of the user migration assistant command file, which is an XML file saved on the core server (typically in the ldmain share, in the ldlogon\uma\commandxml folder). You can specify the path and filename in UNC or HTTP format. Click **Browse** to locate the command file you want to use. If you want to edit an existing command file or create a new one, click **Edit**. Select a file and click **Edit**, or click **New** to create a new one.
  - **UNC path for saved profiles**: Specify where to save the profile files. Type a UNC path or click **Browse** and select a path. Profiles can be saved on any available server/share, including on the core server. Profiles are saved with a .sma extension.
  - **Specify full filename instead of using variables**: Select this check box if you don’t want to name the profile using the unique identifiers.
• **File name unique identifiers**: Select any combination of the computer name, MAC address, and serial number to create the filename of each profile. (For example, if you select **Serial number** and the serial number of the machine is 123A567B, the profile name will be saved as "123A567B.sm."). These profile file names are only used to make the file names more readable. They aren’t used by automatic naming to associate profiles between computers.

**Capture Profile (Mac OS X, available only in the system migration section)**

Use this action to capture a profile on a target device. The capture profile action uses preferred server credentials to authenticate to the shares. This is set in the Content replication / Preferred servers tool. A Mac OS X server has to be set as a preferred server for this to work. The **User name** and **Password** fields in the core server’s preferred server properties are used to access the shares.

When saving profiles, you can specify a full filename, or you can use unique identifiers to create the file name to store the profile.

The Mac version of capture profile captures these items:

- Core certificate
- Device name
- How network adapter interfaces are configured
- LDMS configuration

The fields that can be selected in this action are as follows:

- **Path for saved profile**: Where to store the profile when it is captured. The format can be smb://server/sharepoint or afp://server/sharepoint.
- **Specify full filename instead of using variables**: Select this if you want to disable the filename unique identifiers options. Selecting this will require the filename to be specified in the **Path for saved profile** field.
- **File name unique identifiers**: Select any combination of the **Computer name**, **MAC address**, and **Serial number** to create the filename of each profile.

**Change agent settings (system migration and system configuration sections)**

The change agent settings action lets you select specific Ivanti agent settings for agent components. Agent settings only affect agent components that are installed on the device. Applying an agent setting to an agent component that isn’t installed won’t install that component or have any effect.

The default agent setting option is to **Keep agent’s current settings**. Use the **Edit** button to modify an existing agent setting and the **Configure** button to manage all settings for a component.

**Compare variable (all sections)**

Evaluates the variable at the client and returns success or fail based on the comparison. There is no case-sensitivity with string comparisons. This is useful for controlling the branching flow of If/Else conditions. For more information on conditions, see "Provisioning template conditionals" (591).
The variables you can compare depend on what is available from the device inventory and the template. BNF database query syntax is also supported. Note that new devices may have no or limited inventory data available.

**Configure agent (system configuration section only)**

The configure agent action lets you select an agent configuration to install on the provisioned device. 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 of valid agent configurations.
- **Reboot if required:** Select this check box to allow the device to reboot after agent configuration, if a reboot is required.

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 Agent (Mac OS X, system configuration section only)**

The configure agent action lets you select an agent configuration to install on the provisioned device. 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.

The configure agent action uses preferred server credentials to authenticate to the shares. This is set in the Content replication / Preferred servers tool. A Mac OS X server has to be set as a preferred server for this to work. The **User name** and **Password** fields in the core server’s preferred server properties are used to access the shares.

- **Configuration name:** Select which agent configuration to deploy in the action.
- **Reboot if required:** Will set a reboot to occur after the agent is installed.

**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

- **Insert unique ID:** To use the existing device ID, select this check box and enter the device ID in the box.

This action should be performed as the last action in the post-OS installation section because it 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.

- **Service name:** The display 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 device. 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 Id*.*).

- **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.

**Customize mapped software (all sections)**

This action allows the technician at the device being provisioned to select and install software that was marked "customizable" in the **Product to package mappings** dialog box. You can access this dialog box from the OS Provisioning toolbar by clicking **Tools > Product to package mapping**.
When using this action, generally add it near the template beginning. Once it’s added, you can configure a timeout for how long the customize mapped software prompt will appear on the device. The default is 300 seconds. If a technician isn’t there to customize mapped software, the action will eventually time out and whatever customizable software that was installed on the source device will be installed on the new device.

The template must include the Install mapped software action for the changes made here to take effect.

**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 Id*.*)

- **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.

- **Select the image type**: Select the type of image you want to deploy. If you select Symantec or Other, you will also need to provide a path to the application used for imaging.
- **Specify the UNC path to the image file**: Enter a UNC path to the image that is deployed, including the image file name. Configure your preferred server with valid credentials to the share for the image file path. This option is used when you select either Ivanti ImageW or ImageX as the image type.
- **Specify the mapped drive path to the image file**: Enter a path to the image, including a drive letter and the image file name. This option is used when you select Symantec or Other as the image type.
- **Specify the mapped drive path to the imaging tool**: Enter a mapped drive path and file name for the imaging application. This option is used when you select Symantec or Other as the image type.
- **Command-line parameters**: Enter any command-line parameters that will customize the way the image is deployed.
- **Validate**: Click this button to generate a default command line for the imaging tool and path you specified. You can add other command-line parameters after you click Validate, but if you have already entered any custom parameters they will be removed when you click Validate.
Deploy an Image (Mac OS X, OS installation section only)

Use this action to deploy an image from a target device. This action uses preferred server credentials to authenticate to the shares. This is set in the Content replication / Preferred servers tool. A Mac OS X server has to be set as a preferred server for this to work. The User name and Password fields in the core server’s preferred server properties are used to access the shares.

The options available for this action include:

- **Specify the path to save the image file, including the name of the image file**: This is to define the smb://Server/Share/ImageFile.dmg or afp://Server/Share/ImageFile.dmg to capture the image.
- **Mac Image**: Select this for Mac images.
- **Validate**: Click to populate the Command-line parameters field with the data provided in the other fields.

Deploy profile (System configuration section only)

This action runs the user migration assistant to deploy one or more profiles that have been captured and saved. To use this action, you need to know where saved profiles have been stored.

To use the user migration assistant, managed devices must have the standard Ivanti agent, which includes the inventory scanner, local scheduler, and software distribution agents. Profile migration uses the software distribution agent to distribute files.

- **UNC path where the profile was previously saved**: Specify where the profile files are saved. Type a UNC path or click Browse and select a path. Profiles can be saved on any available server/share, including on the core server. Profiles are saved with a .sma extension.
- **Specify full filename instead of using variables**: Select this check box if you don’t want to name the profile using the unique identifiers.
- **File name unique identifiers**: Select any combination of the computer name, MAC address, and serial number to create the filename of each profile. (For example, if you select Serial number and the serial number of the machine is 123A567B, the profile name will be saved as “123A567B.sma.”)

Device name prompter (available in the PreOS installation, OS installation, and Post-OS installation sections)

Use this action to prompt for keyboard input to name the device running the OS Provisioning Template. This is optional because without it, the name is assigned from the following two steps:

- **Variable**: Create an “IdHostname” variable to replace text in the unattend script.
- **Unattend script**: Places the “IdHostname” variable into the “ComputerName” field of the script.

These two steps assign the Hostname on the device is provisioned.
If instead, you want to allow someone to input the name, inject the Device Name Prompter action as the first step in the Pre-OS installation section. This will allow the user to start the OS Provisioning template, get the prompt right-away in the process, then leave to do something else. The name will be in memory, and will be used rather than what is in the variable “IdHostname” inserted into the “ComputerName” of the unattend script.

- **Timeout (seconds):** This sets the amount of time to allow the user at the device to input a name for the device. If the name and typed and the “Enter” key is pressed, the timeout continues without further waiting. If the name is not input before the time elapses, the action defers to the variable “IdHostname” in the “ComputerName” field of the unattend script.

**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 device.

- **Software distribution package:** Select the package you want to distribute.

**Download file (all sections)**

The Download file action downloads the selected file using an 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 disabled. 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.
  - **User name:** Enter a valid user name with authentication credentials to the proxy server.
  - **Use a 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. Enter the variable name in the Password box enclosed in percent signs (%variablename%). For more information, see "Define a template variable" (588).
• **Password:** Enter the user’s password. Confirm the password in the **Confirm password** box.

**Download from preferred server (all sections)**

This action uses content replication to download data from a preferred server to the target device. The download can be a single file or the contents of a folder (including subfolders) on the source server. To use this action, you must have configured at least one preferred server using the Content replication tool. The choice of which preferred server is used depends on the settings you made when you set up preferred servers in the Content replication tool.

• **Source:** Specify the path to the file or folder you want to download. This path must exist on all shares that are used for preferred server downloads.

• **Download directory:** Select this check box to download the entire folder specified in the Source box. If this is cleared, only the file you specify will be downloaded.

• **Destination:** Specify the path on the target device to which you want to copy the file or folder.

• **Preferred download locations:** The three check boxes let you specify which download sources you want to use. They are listed in the order of priority: if all three boxes are selected, a peer download is attempted first, followed by a preferred server, and finally a source download.

  • **Attempt peer:** Select this check box to first attempt a peer download. The replicator will first check local peers for source files that it is replicating. If the replicator can’t find the files on a peer, it will then attempt to get the file from a preferred server or the source server. This option can reduce the traffic load on preferred and source servers.

  • **Attempt preferred server:** Select this check box to download from a preferred server. If the replicator can’t find the file on a preferred server, it will then attempt to get the file from the source server.

  • **Allow source:** Select this check box to download from the file source. This is recommended only as a secondary option if a peer download or preferred server download can’t be completed.

• **Bandwidth used from core or preferred server:** 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:** 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.

**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.

• **Capture command output**: When this check box is selected, output from the executable is written to a log file. Clear the check box to avoid capturing the output.

**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 repository of device drivers that can be injected into provisioning templates or deployment scripts. 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 System configuration or 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.

You can also use HII to associate SWD packages with drivers. This works well with drivers that are only in an executable (.EXE) format.

• **Using UNC to download driver files**: select this check box to specify that only UNC is used to access the HII repository.

If you use this action, include a Reboot action after it in the Post-OS installation section.
Inject script (all sections)

This action injects a script into the target OS file system. For example, you can inject sysprep.inf into the Deploy image action or unattend.txt into a Scripted install action. The scripts that you can select are those in the Install scripts list (accessed from the Install scripts button on the Provisioning toolbar) that can be applied to the current template.

Injecting a script copies the file to the local machine and also replaces any variables within the file. This action is useful when you want to replace variables in any text file, such as a Windows Sysprep answer file.

- **Script name**: The name of the script.
- **Target file name**: The location of the script you want to inject.

Install mapped software (System configuration section only)

This action installs software detected on a target device which is monitored in the Software License Monitoring tool (for more information, see “Software license monitoring overview” (493)).

Use this action to install software using the rapid software deployment feature as configured in the Product to Package Mapping tool, which can be launched by clicking the Product to Package Mapping icon on the OS provisioning toolbar.

In the Product to Package Mappings tool, you can assign SLM Products to distribution packages. This assignment sets which software will be installed on the newly provisioned device. The ability to make these assignments enables upgrading an older version of software to a newer version, as part of an OS Provisioning task.

- **SLM Products**: Populates with all software applications in the SLM tool’s Monitored section.
- **SWD Packages**: Shows all distribution packages that are created and available to be installed.
- **Remove Assignment**: Allows removing the assignment so the software will NOT be deployed as part of the Install Mapped Software action.
• **Critical:** Selecting this checkbox is analogous to selecting the **Stop processing the template if this action fails** checkbox for a template action. When selected, if the particular software fails to install, the action fails and will NOT continue to install other software associated as a part of the Install Mapped Software action. When unchecked, even if the particular software package fails to install, the task will continue to install other distribution packages assigned to SLM products. (All software which is attempted to be installed by the action is logged in the OS Provisioning Template History.)

• **Disable:** Selecting this checkbox means that although a product may be assigned, it will NOT be installed as a part of the Install Mapped Software action. The use case scenario for selecting this is for testing purposes. While testing, do not install the software which has the **Disable** box selected, while you test other software as a part of this action, then, after all testing is complete, you can clear the **Disable** box and have the action install all assigned software.

**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)**

Use this action to have the device join a domain or workgroup. For domains, you will also need to provide credentials for an account that has rights to add devices to domains.

- **Select operation type:** Can be Join domain or Join workgroup.
- **Name:** Name of the domain or workgroup the device should join.
- **OU:** OU in the domain.
- **Username:** Type the username required to authenticate to the domain.
- **Use a 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**. Enter the variable name in the Password box enclosed in percent signs (%variablename%). For more information, see "Define a template variable" (588).
- **Password:** Enter the corresponding password to the username above. Confirm the password in the **Confirm password** box.

**Launch template (all sections)**

Use this action to launch another template as the next action, by clicking **Select New Template**. This action will start a new template targeting the device matched in the Machine Mappings tool. If no device is matched, the device will target itself, allowing templates to be chained.

The use case for this is when a user has a device that is being replaced with a new device. The OS Provisioning template can capture a profile and other information from the original device, and then the Launch Template action can deploy the desired operating system and the profile (captured from the original device) onto the new device, as well as continue installing desired software on the new device.

For more information on machine mapping, see "About the Machine Mapping tool" (578).

**Map/Unmap drive (all sections)**

Use this action to map or unmap (disconnect) a drive on Windows devices. Note that some systems do not accept drive mappings below drive H.

- **Map/Unmap a drive:** Select whether this action is to map or unmap (disconnect) a drive.
- **UNC path:** Enter the server and share you want to map to.
- **Resource path to disconnect:** When disconnecting a resource, specify the path to be disconnected.
- **Drive letter/Mount point:** Enter the drive letter you to map the path 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 on to the drive.
- **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**. Enter the variable name in the Password box enclosed in percent signs (%variablename%). For more information, see "Define a template variable" (588).
- **Password:** Enter the corresponding password to the username above. Confirm the password in the **Confirm password** box.
Map/Unmap drive to preferred server (all sections)

This action maps a drive on the target device to a path on a preferred server (or the source server). The drive mapping stays in effect until the drive is explicitly unmapped (disconnected), so you should include an Unmap action in a template after an action that downloads data from a preferred server. To use this action, you must have configured at least one preferred server using the Content replication tool. The choice of which preferred server is used depends on the settings you made when you set up preferred servers in the Content replication tool.

- **Drive letter**: Enter the drive letter you want to map the path to. If you chose to unmap a drive, type the name of the drive you want to disconnect.
- **Unmap drive**: Select this check box if the action is to unmap a drive. The action will simply unmap (disconnect) the drive you specified in Drive letter.
- **Path**: Enter the path to the drive in UNC format (\server\share\path). This path must exist on the source server and all shares that are used for preferred server downloads.
- **Attempt preferred server**: Select this check box to first attempt to map the drive to the nearest preferred server that contains the specified folder structure. If no preferred server is found with the folder structure, an attempt will then be made to map the drive to the path on the source server.
- **Require preferred server**: Select this check box to map the drive to the nearest preferred server that contains the specified folder structure. If no preferred server is found with the folder structure, the task fails (rather than map to the source server).
- **Don’t allow preferred server**: Select this check box to map the drive to the path on the source server, without mapping to a preferred server.

Mount ISO (Mac OS X, all sections)

Use this action to mount an ISO image.

- **Image name and path**: Enter the \server\share\file.iso information.
- **Mount point**: Enter the desired mount point.

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.

NOTE: 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.
  - **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.
- **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.

**Format partition**: Create a file system structure on a partition.
- **Logical disk drive letter**: The drive letter of the partition to be formatted (Windows).
- **File system**: For Windows, the file systems are FAT, FAT32, and NTFS.
- **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 ID**: The partition number to be mounted (Windows).
- **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.
- **Logical disk drive letter to remove**: The drive letter of the partition to be unmounted (Windows).

**Make bootable**: Make a partition bootable.
- **Disk**: The disk number to be made bootable. For Windows, this is the disk number.
- **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 a 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.
- **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).

**Partition (Mac OS X, available in pre-OS installation, OS installation, and post-OS installation sections)**

The Partition action lets you complete a variety of actions relating to partitions on the target server.

- **Action type**: Use this field to select a partition action. Option include: create a partition, remove all partitions, format a partition, mount a partition, unmount a partition, or resize a partition.
  
  NOTE: The Boot environment and target OS must be set prior to executing this action.
- **Disk ID**: Type the disk ID (Windows: disk number).
- **Partitions**: Use this field to select and name partitions.

You can specify a size in MB or a percentage of the disk. Be sure the amount of disk space exists. This action will overwrite anything that currently exists. If you do not specify a size on a partition, (this can only be left empty on the last partition) the remainder of the disk will be assigned the last partition.

**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.
- **Boot to managed WinPE (virtual boot)**: Boot the client machine into a managed WinPE environment. Actions will be executed as instructed by the core server. This option is for use when there is no PXE server in the network for provisioning.
- **Confirmation message timeout**: Specify the number of seconds that a confirmation message is displayed before it times out.

**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. Enter the variable name in the Password box enclosed in percent signs (%variablename%). For more information, see "Define a template variable" (588).
- **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.
- **Force reboot**: Select this check box to require a reboot after the OS has been installed.
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** 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 file**: 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.
- **Time**: Pause the template execution for a period of time.
- **Number of seconds to wait**: Type the number of seconds for which to pause the template.
- **File**: Pause the template execution until a file has been created.
- **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, the next action in the template is executed.
- **Maximum number of seconds to wait**: Type the number of seconds to wait for the file to be created. If the time passes and the file isn’t created, the template continues with the next action.

### Windows Refresh (available in the System Configuration section only)

Act upon a target device with a Windows 8 or later OS. These options call the Windows actions for Update and recovery.

- **Reset**: If you want to recycle your PC or start over completely, you can reset it to its factory settings. Select this option to remove everything and reinstall Windows. This will use the .wim file included in a default image without reformatting the drive.
  - **Fully clean the drive**: Select this checkbox to format the drive prior to overwriting the drive with the .wim file.
  - **Use default local WIM**: Select this checkbox to use the .wim file included in the default OS.
  - **UNC path including WIM filename to use**: Type the UNC path and file name of the .wim file to use. The **Use default local WIM** checkbox must be cleared to enable this option.

- **Refresh**: Select to refresh the target PC without affecting the user profile items, such as My Documents, My Music, My Pictures, and so on. This uses a .wim file to overwrite the drive without affecting the user profile items.
  - **Use default local WIM**: Select this checkbox to use the .WIM file included in the default OS.
  - **UNC path including WIM filename to use**: Type the UNC path and file name of the WIM file to use. The **Use default local WIM** checkbox must be cleared to enable this option.

- **Create and assign local WIM**: Select to refresh the image with the .wim file included in the default OS.
  - **UNC path including WIM filename to use**: Type the UNC path and file name of the .wim file to use and replace as the local .wim file for future use.

- **Assign specified image as local WIM**: Select to refresh the image with the .wim file designated in the **UNC path including WIM filename to use** field.
  - **UNC path including WIM filename to use**: Type the path and file name of the .wim to use to refresh the image.
Template properties

Use the template Properties view to display the template information from the time the template was created.

To view template properties

1. Click Tools > Provisioning > OS provisioning.
2. Under Provisioning templates, click Public or My templates or one of their subgroups.
3. Right-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).
   - Target OS: The target operating system of the template.

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.

PXE-based deployment

Provisioning supports PXE booting and image deployment. With PXE-based deployment, you can boot both new and existing PXE-enabled devices into a WinPE preboot environment where you can select and execute a provisioning script. Or scan devices into your core database and then schedule an provisioning task with the Scheduled tasks tool.

PXE-based provisioning is a useful way to image devices in a variety of situations, such as:

- Initial provisioning of new devices.
- Imaging devices in a test or training lab.
- Re-imaging corrupted devices.

Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk offers a couple of options to provision devices:

- Ivanti managed boot, which lets you pre-target devices with existing agents for imaging.
- A PXE boot menu, which lets you interactively select an option for a non-UEFI device.
- An option to always PXE boot UEFI devices.

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)
- 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 provisioning script.

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.

**Enabling PXE representatives**

Starting with Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk 2016.3, PXE representatives are part of self-electing subnet services (SESS). SESS simplifies PXE deployment. The 2016.3 and newer Ivanti agent installation process automatically uninstalls legacy PXE representatives. For more information on SESS, see "Self-electing subnet services" (119).

When the PXE service is enabled for multiple devices on a subnet, SESS will ensure that only one device per subnet is running the PXE service and SESS will automatically elect a new PXE representative if the originally elected device goes down.

PXE representatives automatically update their PXE settings and local copies of WIM files. By default they do this every 15 minutes. When you update WIM files, be aware that PXE representatives may not get the change until the polling interval completes. You can customize the polling interval in PXE subnet settings.

The PXE service components are part of the base agent configuration, but PXE is disabled by default in agent settings. Once the PXE service is enabled in the client connectivity agent settings and the setting is deployed to devices, SESS will elect a PXE service representative for each subnet where the PXE service has been activated.

It's important to note that an elected PXE representative will be available for use, but by default it won't PXE boot any devices except for those that are set to network boot.

Follow these steps to enable PXE on a subnet.
1. Enable PXE in an agent setting

1. Click **Tools > Configuration > Agent settings**.
2. In the **Agent settings** tree under **Client connectivity**, double-click an existing agent setting or right-click and create a new one.
3. In the agent setting, click **Self-electing subnet services > PXE service**.
4. Select **Enable PXE service**.
5. Click **Save**.
6. In the Agent settings toolbar, click **Create a task > Change settings**.
7. On the **Change settings** page, select the client connectivity setting you modified.
8. Click **Save**.
9. Add targets to the new change settings task and run it. You can target multiple (or all) devices on a subnet and let SESS manage which device runs the PXE service on that subnet. If you target only one device on a subnet, that device will always win the SESS PXE election.

2. Configure PXE behavior on a subnet

If you just enabled the PXE service on devices, it may take a while for the subnet to appear in the self-electing subnet services tree.

1. Click **Tools > Configuration > Self-electing subnet services**.
2. In the tree select **PXE service**.
3. Right-click the subnet you want to modify and click **Service settings**. The settings apply only to the subnet you selected.
4. If you want to limit which devices can PXE boot you can add MAC addresses to the allowed or disallowed areas. By default this list is empty and PXE will boot all devices.
5. Change other settings if necessary.
6. Click **Save**.

3. Enable PXE on a subnet

1. Click **Tools > Configuration > Self-electing subnet services**.
2. In the tree select **PXE service**.
3. Right-click the subnet you want to modify and click **Enable**.
4. It may take up to 15 minutes for the change to propagate.

Additional PXE information:

**About the PXE boot options dialog box**

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. Press the F8 function key during this countdown to access the PXE boot menu and select an OS image to deploy on the device.

**To configure PXE boot options**

1. Click **Tools > Provisioning > OS provisioning**.
2. On the toolbar, click **Preboot > PXE boot options**.
3. Change the options you want and click **Save**.

**Timeout**: Enter a value (in seconds). The default value is 4 seconds. The maximum number of seconds you can enter is 60.

**Message**: Type a message that devices will see when PXE booting. The default message is "Press F8 to view menu." The maximum number of characters you can type is 75.

**Always PXE boot UEFI devices**: When selected, allows UEFI devices to boot into WinPE without prescheduling a task

**Allow anonymous login for public templates**: When selected, allows anyone to PXE boot and select a public template for imaging, without any authentication. We recommend against using this option.

**About the PXE Settings dialog box**

Use this dialog box to configure SESS PXE settings.
1. Click **Tools > Configuration > Self-electing subnet services.**
2. In the tree select **PXE service.**
3. Right-click the subnet you want to modify and click **Service settings.** The settings apply only to the subnet you selected.
Polling frequency: How often the SESS PXE representative on the subnet should check for updated settings and imaging files. The default is 15 minutes. Be aware that if you change a setting or a WIM file, that change won’t get to affected PXE representatives until their next polling interval check.

TFTP block size: The default is 16384 for ia32 and 65464 for x64. Smaller sizes may be required in certain environments, though going smaller tends to slow down transfers, often substantially. VMWare in particular requires a block size of 1456.

Allowed and Denied: Allowed specifies that the list of provided MAC addresses are the only devices on the subnet allowed to PXE boot. Denied means all devices not on the list but on the subnet will PXE boot.

Attempt peer: Check with subnet peers for WIM images before downloading from somewhere farther away.

Attempt preferred server: Allow WIM downloads from preferred servers.

Allow source: Allow WIM downloads from core servers.

Bandwidth used (WAN and Local): Percent of available bandwidth to use when downloading images.
Hardware independent imaging

Hardware-independent imaging overview

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 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 Ivanti® Endpoint Manager and Endpoint Security, powered by LANDesk, you can avoid these types of problems and have greater control over the use of drivers in your managed devices.

You can use hardware-independent imaging with images from any imaging tool. You can define the images with the tool you prefer, then create imaging scripts in Endpoint Manager 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 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 related help topics listed at the end of this topic.

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 Ivanti agent is installed.
Setting up hardware-independent imaging

To implement hardware-independent imaging with OS provisioning scripts or templates, create a repository of drivers that will be available to the imaging tool. These drivers are used on the hardware you want to image, including audio, video, network, mass storage device, and other types of device drivers.

Store the drivers in one location on a preferred server and ensure that the path is accessible by both UNC and HTTP methods.

If HII isn't assigning the right drivers in some cases, manually assign the drivers you want in the HII Assign dialog box.

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.

Related topics

"Creating a driver repository" (625)

"Using hardware-independent imaging with provisioning templates" (627)

Creating a driver repository

As you plan and define the images you want to use for managed devices, you'll decide which drivers you want to use. To use these drivers for hardware-independent imaging, you create a repository of drivers that is saved in one location (by default, on the Endpoint Manager and Security core server). The drivers are then available for any deployment or provisioning script you want to run.

This location needs to be available as a UNC path and also as an HTTP location (URL) because HII relies on both methods to download drivers.

Your HII driver repository must be located on a preferred server, which you can define in Tools > Provisioning > Content Replication/Preferred Servers.

To create a repository, you need to save the driver files in a folder. You must include a .inf file for each driver. The HII tool scans the folder and creates a drivers.db3 file that is used to match device hardware with the appropriate drivers.

To create a driver repository

1. Click Tools > Provisioning > HII Driver Management.
2. Click the Build library toolbar button.
3. Verify that the repository location is correct as a UNC path. If driver files are stored in a different location, click Browse and select your repository folder.
4. Verify that the URL to the same repository location is correct.
5. Click **Save**. The HII tool scans the repository folder and builds a list of drivers. When it is complete, a success message indicates a repository file count (how many files were found) and the number of drivers processed (how many individual drivers were found).

6. Each time you add driver files to the repository folder, repeat steps 1-5 to update the drivers.db3 file with the new data.

### Disabling HII drivers

If there are drivers in your repository that you no longer want to use, you can find them in the repository and disable them. They will no longer be used when you use provisioning scripts that include hardware-independent imaging.

**To disable drivers in your HII library**

1. Click **Tools > Provisioning > HII Driver Management**.
2. Click the **Disable Drivers** toolbar button.
3. To search by name in the driver library, type all or part of the driver filename and click **Search**.
4. To filter your search, select items in the **OS** and **Architecture** lists.

   Items matching your search specifications are listed under **Devices**.

5. Select one or multiple items in the list, or click **Select All**.
6. Click **Update** or **Update and Close** to change the status of the drivers to disabled. If you click **Update and Close**, you’ll be returned to the HII Driver Management tool.

### Assigning HII drivers

By default, HII autodetects the correct drivers for a device by using drivers from your driver repository ("Creating a driver repository" (625)). However, HII sometimes has problems choosing the right driver because there are multiple matches for a device or the drivers don’t match well. If this happens, use the HII Assign dialog box to customize HII driver detection and assignments.

When you install Endpoint Manager agents on a computer, the agents send that computer’s HII driver detection information to the core server. That computer model is then available in the HII Driver Management dialog box, where you can preview and customize HII driver detection for that model.

When manually assigning HII drivers, you can use a mix of manually-assigned and auto-detected drivers.

There are three ways you can customize HII driver detection and installation:

- **.inf File**: Select specific driver .inf files found in your driver library.
- **Driver Package**: Select software distribution packages that can install drivers.
- **Auto Detection**: Select a device and preview HII driver detection for it. You can then assign new drivers manually from your library if necessary.

**To assign a driver to hardware for use in HII**

1. Click **Tools > Provisioning > HII Driver Management**.
2. Click the **Assign** toolbar button.
3. Select the **Make** and **Model** of the hardware.
4. Select the **OS** and **Architecture** to associate with the driver.
5. Select the driver source you want, either **.inf File**, **Driver Package**, or **Auto Detection**, and customize that source.

**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. The HII tool automatically selects the manufacturer and model of the device you are provisioning, based on the strings in the device’s BIOS.

**To include hardware-independent imaging in a provisioning template**

1. Click **Tools > Provisioning > OS provisioning**.
2. Under **Provisioning templates**, select a Windows-based template. Right-click the template and select **Edit**. Or, to create a new template: on the toolbar, click **New template > Empty template**. Name the template, select the Windows PE boot environment, and select the target OS. Click **OK**, then open the template.
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 specify that only UNC is used to access the HII repository, select the **Using UNC to download driver files** check box.
6. If you want to allow unsigned drivers, select **Force unsigned drivers to install**.
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.
LANDESK SmartVue

Welcome to Ivanti SmartVue

Use Ivanti® SmartVue to view key information about IT processes that impact user productivity, system performance, and endpoint security. SmartVue shows the value of IT within your organization and is ideal for CIOs, department heads, and IT directors who need timely information for decision-making and business conversations. By default, SmartVue is installed on each core server.

SmartVue gives you data to share about the successes, challenges, or needs of your IT department. You can also use it to track goals, service level agreements, or key performance indicators.

With SmartVue, you’ll see visual graphs and charts on your iPhone or iPad that are generated from management and security data stored in your Ivanti core server, such as:

- Devices managed
- Operating systems
- Patch processes
- Power management
- Provisioning
- Remote control
- Security
- Software
- Software distribution
- Windows upgrades

In the Dashboard, you can view SmartVue charts that display data from the core server. However, to view aggregated data from all of the servers, you must view the data in the SmartVue app.

Other key features include the following:

- Shareable information via PDF exports
- Time and location filters for all records
- Integration with iBooks to print directly from your iPhone or iPad
- Connectivity with other Ivanti products, such as Service Desk
Scheduling SmartVue data collection

The SmartVue app doesn’t display real-time data. Instead, it updates the data once a day. You can change this default frequency in the SmartVue Configuration dialog.

Each widget in the SmartVue iOS application is driven by a series of database queries. These queries need to run periodically, and the app then displays data based on the last time the queries ran. For more information, see "Modifying SmartVue widgets" (635).

When you first run SmartVue on your core server, you may want to start an immediate data collection cycle so that you have some data to see in the app.

To schedule an immediate SmartVue data collection cycle

1. In the management console, click Configure > SmartVue configuration, then click the Scheduler page.
2. Click Start now, and click OK.
3. Monitor the task progress in the scheduled tasks tool. Click Tools > Distribution > Scheduled tasks, and click All tasks > SmartVue.
Once you have some SmartVue data in the database, you can configure a periodic data collection schedule. Most widgets gather data monthly, so running data collection once a day usually works fine.

**To schedule a periodic SmartVue data collection cycle**

1. In the management console, click **Configure > SmartVue configuration**, then click the **Scheduler** page.
2. Click **Repeat**.
3. Select an **Hourly, Daily**, or **Weekly** schedule.
4. Configure the interval you selected.
5. Click **OK**.

**Configuring SmartVue data sources**

By default, SmartVue collects data from the core server where it was installed. You can add other data sources in the **SmartVue Configuration** dialog. Any server can be a point core and you can specify which servers you want to post to and pull from. By forwarding data to another core, you can create a server hierarchy.

If you’re connecting to a custom data source, you can enter your own name. Note that the case-sensitive **Data source** name you enter here also must be entered in the .XML widget configuration file that refers to it. The attribute that needs to match is `<DataDefinition datasource=""`.

**To configure data sources**

1. In the management console, click **Configure > SmartVue configuration**, then click the **Database sources and cores** page.
2. Click **Add** or select an existing data source and click **Edit**.
3. Enter the data source information and database credentials.
4. Click **OK**.

**Configuring SmartVue locations**

If you manage devices at multiple locations, you can configure SmartVue to group devices by location. Use the **Location** page (**Configure > SmartVue configuration**, then click the **Location** page) to configure how SmartVue determines device location. You have three choices:

- LDAP
- Device name
- LDMS public queries

You can only choose a single location method.
**Configuring LDAP locations**

When the inventory scanner scans a managed device that belongs to an Active Directory, the scanner returns that device's location path. You can tell SmartVue which part of that path contains the location text that you want to use.

On the SmartVue configuration dialog's Location page, select LDAP. The page shows a sample location path that the inventory scanner reported. The text box below the sample path lists elements in the path based on the delimiter you specify (/ is the default). Select the path element containing the location text that you want SmartVue to use.

**Configuring device name locations**

If your managed devices have a standardized location prefix in their device names (for example, a three-letter city prefix), you can enter it here. You will need to enter the starting character position and length. Select the characters in the sample entry and the dialog box will automatically enter the values for your selection. Note that the first character in the device name is position 1, not 0.

You can only configure a single device name location template.

**Configuring Ivanti public query locations**

If you have queries that identify computers by location, you can use the public query location option. Each query's results correspond to a location. You can add multiple queries. Once you've selected the queries you want, click the query Location name and customize it. The Location name will appear in the widget results.

**Using the SmartVue iOS app**

Before you can use the SmartVue iOS app, you need to:

1. Schedule and run the SmartVue data collection utility (LDGatherData.exe) so data from your core is available to the SmartVue iOS app.
2. Give SmartVue app users the SmartVue permission so they can log into the core from the mobile app (Tools > Administration > User management). Ivanti administrators have this permission by default.
3. (Optional) Configure additional database connections to other core servers, Ivanti Service Desk servers, or custom data sources.

Once you've completed the prerequisites above, you can log in to your core.
To connect to a SmartVue core from the iOS app

1. On your mobile device, launch SmartVue.
2. In the Settings dialog box, enter your Ivanti User name and Password.
3. The Core URL will be http://<your core's computer name or IP address>. For example, http://myIvanticore.

Once the app has connected you can browse the data that the data collection utility has gathered. Refer to the help screen if you’re wondering how to use the app:

The iOS app connects to the core to get widget data when you first show a category and when you change categories. Navigation within a category won’t trigger widget data updates.

Using the SmartVue web application

Ivanti® Endpoint Manager powered by Landesk includes a SmartVue web application that you can access from the following browsers:

- Recent IE versions with compatibility view disabled
- Chrome
Firefox
Macintosh version of Safari

Once SmartVue is configured, you can access the SmartVue web application here:

http://<corename>/smartvuweb

If you’re using an IvantiCloud Services appliance and you want to access the SmartVue web application from the Internet, use URLs with the following format.

For Chrome-based browsers:

https://<CSA_public_name>/rtc/<corename>/smartvuweb

For other browsers (note the trailing slash (/) at the end of the URL):

https://<CSA_public_name>/rtc/<corename>/smartvuweb/

**SmartVue architecture**

Core servers have three web services. The web services use the existing STS token service on the core server for authentication/security.

- **SmartVueData**: Accepts data posted by LDGatherData.exe.
- **SmartVue**: Provides data to the SmartVue mobile application.
- **Dashboard1**: Manages widget display in the SmartVue mobile application.

Setup creates these new tables in the core database:

- SmartVueData
- SmartVueLocationData
- SmartVueQueryLocations
- SmartVueWidgets
- SmartVueUserWidgets
- SmartVueConnections
- SmartVueSettings

LDGatherData.exe posts results to SmartVueData web service, which then puts the data into the SmartVueData and SmartVueLocationData tables.

With slow links, LDGatherData.exe is installed locally. You can then schedule it to run whenever you want. When it runs, it gets the latest XML files from the point core and posts its data to the point core’s SmartVueData web service.
Modifying SmartVue widgets

Each SmartVue widget category is defined in an XML file that the SmartVue installer puts on the point core. You can modify these XML files to add, change, or remove widgets that display in the SmartVue mobile application. The XML files are stored here on the point core:

- C:\Program Files\LANDesk\ManagementSuite\SmartVueDef.

NOTE: When SmartVue's LDGatherData.exe program runs, it creates a \SmartVue folder that also contains XML files. Don’t edit these files. If you modify a \SmartVueDef XML file, the corresponding file in \SmartVue will be overwritten when LDGatherData.exe runs.

Make sure you create a backup of any XML file that you plan to edit before you make any changes.

Here is the basic XML structure:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<DataDefinition name="" id="" datasource=""
  <Definitions>
    <Definition name="" id="" controlType="" dataSet=""
      <Sql>
      </Sql>
      <TotalSQL>
      </TotalSQL>
      <LocationSQL>
      </LocationSQL>
      <Controls>
        <Control title="" columns="" />
      </Controls>
    </Definition>
  </Definitions>
</DataDefinition>
```

Each widget contains a widget definition and three sets of queries.

- **<SQL>**: Collects data for the widget.
- **<TotalSQL>**: Queries the SQL data that was collected and returns it to the widget.
- **<LocationSQL>**: Joins the Total SQL query results with the location information that was configured on the point core. On the point core, configure locations in Configure > SmartVue configuration > Location. You can define locations based on an LDAP directory, a computer device name prefix string, or an LDMS public query.

The following sections give more detail on the XML element attributes.

**<DataDefinition>**

- **name**: The category name. This name is used in the <TotalSQL> section’s WHERE condition.
- **id**: The unique ID for this definition. This ID is used in the browser query string. It can’t contain spaces or characters like &.

Example: `<DataDefinition name="MyCategory" id="123" datasource=""/>

```xml
<DataDefinition name="MyCategory" id="123" datasource=""
  <Definitions>
    <Definition name="" id="" controlType="" dataSet=""
      <Sql>
      </Sql>
      <TotalSQL>
      </TotalSQL>
      <LocationSQL>
      </LocationSQL>
      <Controls>
        <Control title="" columns="" />
      </Controls>
    </Definition>
  </Definitions>
</DataDefinition>
```
• **datasource**: The database data source type. This is case-sensitive and must exactly match the Data source you specified in the Add database dialog box (Configure > SmartVue Configuration > Database, click Add or Edit).

### <Definition>
- **name**: The widget title. This name is used in the <TotalSQL> section’s WHERE condition.
- **id**: The unique ID for this widget. It can’t contain spaces.
- **controlType**: The type of widget to use for this data. It must be one of the following:
  - BarTemplate
  - BurnDownTemplate
  - ColumnTemplate
  - DonutTemplate
  - LineTemplate
  - PercentBallTemplate
  - PercentBarTemplate
  - PieTemplate
  - RadialTemplate
- **dataSet**: The returned data format, either “row” or “column”. For example, if the data set returned is in a format where count 1 is in column 1, count 2 is in column 2, and so on, the data set is “column”. If your SQL statement returns multiple rows, it must be “row.”
- **seriesData**: Specify “bymonth” if this is for time-based widget data. You can see examples of this in Remotecontrol.xml. This works well with bar-based templates.

### <SQL>
Contains the SQL queries that get data for the widget.

### <TotalSQL>
Contains the SQL queries that return data to the widget.

The order and the names of the columns matter. The name of the column must be first. If you want something other than “Data Count” or “Count”, you need to alias the first column as DataName (select a.columnname DataName, ...). The count must be the second column in the select list and it must be aliased as DataCount. If you have row data, is must be a SUM. (select a.columnname DataName, SUM (a.DataCount) DataCount, ...).

If you want your data to be displayed by a date (on the y-axis), the alias ReportDate must be the last column in the SELECT clause (select a.columnname DataName, SUM(a.DataCount) DataCount, a.ReportDate FROM ...).

The a.CountType="" condition must contain the <DataDefinition name=""> and the <Definition name=""> you specified earlier in the XML file, with no space separating the two names.
For example, if `<DataDefinition name="Power Management">` and `<Definition name="Devices under Power Management">`, `a.CountType= would be "Power ManagementDevices Under Power Management".

**Non-SQL items in the TotalSQL section queries**

#SVTABLE# is a placeholder place that is used to determine if queries are looking for location-specific data or non location-specific data. This placeholder is replaced dynamically.

The #SVWHERE# and #SVTIME# placeholders are used to determine whether the query should be based on location or time, depending on what the user selected in the application. There are two classes of widgets, time-based (often represented by bar graphs) or location-based (often represented by pie charts). Location-based data generally doesn't have a time period associated with it. Time-based widgets use monthly data counts.

**<LocationSQL>**

Joins data to location.

Set locations on the point core by clicking *Configure > SmartVue configuration > Location*. You can define locations based on an LDAP directory, a computer device name prefix string, or an LDMS public query. You can only pick one.

**<Controls>, <Control>**

Defines the row or column data and titles that the widget should display. This section is currently not used by SmartVue.

**Making widgets active**

When you add or change XML files in the C:\Program Files\LANDesk\ManagementSuite\SmartVueDef folder, the changes won’t be visible in the SmartVue mobile application until the data collection program runs:

- C:\Program Files\LANDesk\ManagementSuite\LDGatherData.exe

If you specified a data gathering schedule for SmartVue, it will run at that time. If you want it to run right away, do the following.

**To update SmartVue data**

1. Click *Configure > SmartVue Configuration > Scheduler.*
2. Click *Start now.*
3. Click *OK.*

The LDGatherData.exe process will take a few minutes to complete.
About the SmartVue configuration dialog box

The SmartVue configuration dialog box (Configure > SmartVue configuration) is only available on the core server. Use this dialog box to configure SmartVue database connections, location methods, and data collection schedules.

- "About the Database sources and cores page" (638)
- "About the Location page" (638)
- "About the Scheduler page" (639)

About the Database sources and cores page

Use the Database sources and cores page to add database data sources that SmartVue should collect data from. For more information, see "Configuring SmartVue data sources" (631).

About the Add database dialog box

- **Data source:** If you’re connecting to a Endpoint Manager or Service Desk database, make the corresponding selection, otherwise enter your custom data source name.
- **Display name:** A descriptive name for your data source. This name appears in the main SmartVue configuration database list.
- **Server:** The computer name hosting the database you’re adding a connection to.
- **Database:** The database name on the server you specified.
- **User name** and **Password:** The database credentials that grant access to the database.

When you click OK, SmartVue will use the information you provided to connect to the database. If the connection fails, you will see an error message with additional information.

About the Location page

Use the Location page to configure how SmartVue determines device location. You have three choices:

- LDAP
- Device name
- Ivanti public queries

For more information, see "Configuring SmartVue locations" (631).
About the Scheduler page

The **Scheduler** page controls when the SmartVue data collection utility, LDGatherData.exe, runs. This utility gathers data from the point core it is installed on and any other data sources that you’ve configured. This utility doesn’t run automatically or have a schedule by default. You must create a schedule for it or run it manually.

The **Scheduler** page has these options:

- **Leave unscheduled**: This is the default option. LDGatherData.exe isn’t scheduled to run.
- **Start now**: Runs LDGatherData.exe when you click **OK**. If you had previously configured a repeating schedule, that schedule will be cleared. If you want to resume a repeating schedule after using the **Start now** option, you will have to reselect **Repeat** and reconfigure it.
- **Repeat**: Runs LDGatherData.exe on the repeating schedule you specify. You can choose **Hourly**, **Daily**, or **Weekly** intervals. If you select Hourly, the schedule runs (TBD at what time?) each hour. If you select **Daily**, you can select the time you want. If you select **Weekly**, you can select the day of the week and the time you want.
Local accounts

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 Ivanti 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 devices at near real-time.

Manage local user 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 box, right-click Groups and then click Add.
4. In the New Group dialog box, 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 box, 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 box, click Groups.
4. Right-click the group you want to edit and then click Edit.
5. Make your changes to the group and then click OK.
Manage 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 box, right-click Users and then click Add.
4. In the New User dialog box, 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 box, 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 box, click Users.
4. Right-click the user you want to edit and then click Edit.
5. Make your changes to the user properties and then click OK.

Assign users to groups

There are two methods for adding and removing users to and from groups on a local client when working from the console. The first method lets you add or remove multiple users to or from a group at one time. The second method lets you 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 box, 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 box, 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 box, 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 box, 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**.

**Change a local account password**

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 box, 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.

Reset a local account password

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 box, click Users.
4. Click the Schedule icon.
5. In the Schedule task dialog box, insert the user name that you want to reset the password for. You can select an existing user name from the 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 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.

Using the local accounts tool on the core server

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 Ivanti users to the console by creating local users and adding them to the Windows LANDesk Management Suite or LANDesk Administrators group. This lets you 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 "Role-based administration overview" (52).

Local accounts management help

About the New user dialog box

Use this dialog box to create a new user. For more information, see "Manage local users" (641).

- **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 box

Use this dialog box to edit the user properties. The dialog box consists of three configuration tabs, General, Member of, and Profile.

For more information, see "Manage local users" (641).

General tab

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 whether the user to has to change their password upon logging in to the console.
- **User cannot change password**: Specifies whether the user can change their password.
- **Password never expires**: Specifies whether the password will expire.
• **Account is disabled**: Specifies whether the account is disabled.

• **Account is locked out**: If an account is locked, this option is available. Accounts generally lock when the user has unsuccessfully tried to log in to their account more than three times in one session. This option unlocks the account so the user can authenticate to the operating system.

**Member of tab**

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 box, which lets you 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 box**

Use this dialog box to configure the group. For more information, see "Manage local user groups" (640).

- **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 box, which enables you to add users to the group.
- **Remove**: Removes the selected users from the group.
Managing Macintosh devices

Macintosh device management overview

Ivanti® Endpoint Manager powered by Landesk provides system management for Apple Macintosh computers and devices. This helps you automate system management tasks throughout the enterprise. From the Ivanti Management 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.

This topic describes how to use Ivanti® Endpoint Manager powered by Landesk to manage Macintosh computers. It lists 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 help topic for each tool.

Supported OS versions

For information on supported Mac OS X versions, see this document on the Ivanti Community:

- [https://community.landesk.com/support/docs/DOC-23848](https://community.landesk.com/support/docs/DOC-23848)

Agent configuration for Macintosh devices

Ivanti® Endpoint Manager powered by Landesk uses agent configurations to gain control of devices and manage them. Macintosh agent configurations are pushed to unmanaged Macintosh devices using the same process used to push agents to Windows devices.

The Default Mac Configuration package contains the required agent for controlling Macintosh devices. In order to manage your Macintosh devices, you need to:

1. Create a Mac configuration with the Agent Configuration tool
2. Deploy the Mac agent to your Mac devices

After the agents have been installed, your Macintosh devices become managed devices. Then you can create custom configurations to have greater control of these devices. Custom agents are easily implemented once your devices are managed.
NOTE: All devices must support TCP/IP.

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 from LDLogon/Mac using a Web browser 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.

Deploying 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 then schedule the task.

Create or update 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. Select a configuration group (My configurations or Public configurations). On the toolbar, click the New agent configuration button > New Mac agent configuration.
3. Complete the options in the Agent configuration dialog box. For more information, see "Using the Macintosh agent configuration dialog" (648).
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**.

**Schedule the agent configuration**

You can push agent configurations to devices that have the standard Ivanti agent installed. Use the **Scheduled tasks** tool to deploy 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 agent deployment**.
3. From the network view, drag devices, groups, or queries onto the task to target devices for the task.
4. Select the task, click the **Properties** button on the toolbar, and schedule a time to start the task.

**Manually running agent configurations for Macintosh devices**

You can manually run agent configurations for Macintosh devices once they have been created or updated. When you create an 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 installing the agent (see "Manually running agent configurations for Macintosh devices" (648)), but insert your agent configuration file name instead of the default file name.

**Uninstalling Macintosh agents**

To uninstall Macintosh agents, run `uninstallmacagent.sh` from `\<core>\ldmain`.

**Using the Macintosh agent configuration dialog**

This section describes the agent configuration dialog for Macintosh devices. The dialog includes the following pages:

- Start
- Application policy management
- Inventory
- Remote control
- Standard Ivanti agent
- Patch and compliance scan
- Antivirus
About the Start page

- **Configuration name**: Type a unique name for the agent configuration.
- **Default configuration**: Select this check box to make this the default Macintosh agent configuration.
- **Agent components to install**: Standard Ivanti agent is selected by default. You can also select Ivanti Antivirus.
- **Do not run client status menu**: Select this check box if you don’t want end users to see the status bar menu that lets them run installs and scans.

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 12176. 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 selected, 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, and whether a user is logged. The default schedule is to run a scan every day with a random delay of up to one hour.

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, and whether a user is logged in. 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, displays a visual cue in the menu bar.

**About the Standard Ivanti agent page**

Use this page to configure agent security and management scope. For more information on agent security, see "Agent security and trusted certificates" (140). For more information on scope, see "Role-based administration overview" (52).

- **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 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, and whether a user is logged in. The default schedule is to run a scan every day with a random delay of up to one hour.
- **Use alternate update server:** Specify a different core server to use for patch and compliance updates if the main core server is not available.
- **Scan and repair settings:** Select the settings that you want to use for patch and compliance scans.
- **Configure:** View all available scan and repair settings. Edit or create new settings and select the settings that you want to use for patch and compliance scans.

**About the Antivirus page**

Use this page to specify which antivirus settings are included with the agent.

- **Ivanti Antivirus settings:** Select the settings that you want to use for antivirus scans.
- **Configure:** View all available antivirus settings. Edit or create new settings and select the settings that you want to use for antivirus scans.
- **Include Antivirus setup files:** Antivirus setup files (which are 158 MB) are included when the Macintosh agent is scheduled and downloaded to the Macintosh device.
- **Exclude Antivirus setup files:** When the Macintosh agent is deployed, the Antivirus setup files are downloaded from the core server. This makes the agent package smaller.

**About the Tenant page**

Use this page if you have the Tenant management add-on for Endpoint Manager. You can assign an agent configuration to a tenant within your organization.

- **Assign a tenant to this configuration:** Select this check box if this Macintosh agent configuration is only used with a tenant in your organization.
- **Choose a tenant:** Select a tenant from the list of available tenants that have been defined in the Ivanti Management Console.

**About the OSX profiles page**

Use this page if you want to use an OSX profile with the Macintosh agent.

- **Apply OSX profiles to this configuration:** select this check box to use an OSX profile with this Macintosh agent.
Choose which OSX profiles to apply: Select the settings to use with this Macintosh agent.

Configure: View all available OSX profile settings. Edit or create new settings and select the settings that you want to use for this Macintosh agent.

Connect to the core server through the Ivanti Cloud Services Appliance

There are two options for configuring managed Macintosh devices to connect to the core through the Ivanti Cloud Services Appliance (formerly the Ivanti 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 Ivanti Cloud Services Appliance after they are disconnected from the local network. This type of configuration enables Ivanti® Endpoint Manager powered by Landesk functionality through the appliance without the necessity of manually configuring individual managed devices.
- Manually configure each managed device to connect through the Ivanti Cloud Services Appliance. This type of configuration enables Ivanti® Endpoint Manager powered by Landesk functionality through the appliance. Manual configuration can only be done by a user with Administrator rights on the client device.

After configuring the core for connection through the Ivanti Cloud Services Appliance, rebuild any agents for Macintosh devices and push them to the devices. For more information, see “Configuring the Ivanti Cloud Services Appliance (Management Gateway)” (977).

To manually configure a managed device

1. From the Utilities folder on the managed device, launch the Ivanti Cloud Services Appliance application.
2. Specify the Domain name of the appliance.
3. Choose the best connection method to the Ivanti core.
4. Request a certificate by typing an Ivanti console user name and password, then clicking Request.
5. Click Test to test the connection from the managed device to the Ivanti Cloud Services Appliance.
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.

Enabling Mac OS X FileVault encryption

Mac OS X uses FileVault to encrypt drives. The Ivanti® Endpoint Manager powered by Landesk security scanner can detect whether devices running OS X have FileVault enabled. If you enable the FileVault vulnerability and remediate it, FileVault will be turned on if it isn’t already.
When you enable FileVault through Endpoint Manager, it creates a special encrypted core database inventory record that is saved even if you later delete the device in the Network view. This record includes the FileVault recovery key that Endpoint Manager administrators can use to disable FileVault and restore access to the device.

To enable FileVault on Mac OS X devices

1. If you haven’t already, use the Patch and compliance tool to download Apple Mac Vulnerabilities.

2. In the Patch and compliance tool, click All types > Scan. In the Find box type FileVault and press enter. You’ll see two FileVault vulnerabilities, one that only detects the FileVault state (APPLE-FileVault_DetectOnly) and another that activates it (FileVaultActivation-xx). Drag the activation vulnerability to an Autofix group or your preferred group.

3. When the vulnerability scanner runs and detects that FileVault needs to be enabled, a dialog box on the managed device pops up and lets users know that FileVault has been enabled and they need to reboot. Clicking OK closes the dialog, but the reboot isn’t forced.

4. When users reboot the standard OS X FileVault activation process begins. Users are prompted to log in. A dialog box then appears and tells users that “Your administrator requires that you enable FileVault”. Users can only click Cancel or Enable Now. Clicking Cancel returns them to the login prompt. Once they click Enable Now, the encryption process begins. This takes a while.

Viewing Client data storage

The Client data storage tool (Tools > Configuration > Client data storage) lets you view encrypted client data. Currently, this tool only shows data for Mac OS X devices that have FileVault enabled via Endpoint Manager. Use this tool if you need to retrieve a device’s FileVault recovery key.

To retrieve a FileVault recovery key

1. Click Tools > Configuration > Client data storage.

2. In the Devices tree, double-click the device you want.

3. In the Client data dialog box, select the FileVault2RecoveryKey item, and click the export toolbar button.

4. Select a location for the resulting XML file.

5. Open the XML file in an editor and find the RecoveryKey element. The associated <string> value contains the actual key.

Applying Mac configuration profiles

Apple’s OS X server Profile Manager lets you create Mac configuration profiles for your Mac devices. Each profile is an XML file with a .mobileconfig file extension that defines device settings, such as wireless network and VPN configurations. For more information on Profile Manager, see https://support.apple.com/profile-manager.
Once you use Profile Manager to create a configuration profile, you can use Endpoint Manager agent configurations or agent settings to deploy that configuration profile to other managed Mac devices.

If your Mac configuration profile uses a self-signed trust certificate, make sure you deploy that certificate before deploying other configuration profiles.

To create a configuration profile setting

1. Use Profile Manager on a Mac OS X Server to create a .mobileconfig file that contains the Mac configuration settings.
2. Copy the .mobileconfig file to a location you can access from a Endpoint Manager console.
3. Click Tools > Configuration > Agent settings.
4. In the Mac Configuration Profile group, create a new setting or double-click an existing one.
5. Click **Import** and browse for the .mobileconfig file you saved earlier. Give it a descriptive **Display name** and click **Import**. At this point the .mobileconfig file contents are imported into the LDMS database. Note that the LDMS console doesn’t currently have an XML viewer for this content, so you may want to keep a copy of the file for future reference, even though the core server and console no longer need it.

6. Move one or more **Available configurations** to the **Selected configurations** list to select them for this named setting.

7. Select whether you want to **Append** or **Replace** the configuration profile. Append preserves existing profile settings. Replace removes all existing profile settings, including settings you aren’t modifying, and replaces them with the profile settings you specified.

8. Click **Save**.

**To add a Mac configuration profile to an agent configuration**

Generally, this option is used if an Endpoint Manager agent hasn’t been installed yet on a Mac device.

1. Click **Tools > Configuration > Agent configuration**.
2. Double-click the Mac agent configuration you want to modify.
3. On the **OSX profiles** page, select **Apply OSX profiles to this configuration**.
4. Select the configuration profile setting you want from the list.
5. Deploy this agent to Mac devices.

**To apply a Mac configuration profile with an agent setting update**

This option can only be used if a Endpoint Manager agent has already been installed on targeted Mac devices.

1. Click **Tools > Configuration > Agent settings**.
2. In the toolbar, click the **Create a task** button, then click **Change settings**.
3. Assign a **Task name** and select scheduled task or policy.
4. In the list beside **Mac Configuration Profile**, change the name in the **Settings** column to match the setting you want.
5. Click **OK**.
6. If you used a scheduled task, run the job.

**Run an inventory scan on 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 Ivanti 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 idiscan (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 idiscan 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.

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.

Changing Mac scanned file extensions and searched folders

The Mac inventory scanner defaults to scanning files with .dmg and .pkg extensions, and multimedia files with the following extensions: .aac, .aiff, .gif, .m4p, .mov and .mp3. You can change these items and specify other folders to search in the Manage software list.

To edit the Manage software list

1. Click Tools > Reporting / Monitoring > Manage software list.
2. In the Inventory tree, click Settings and double-click MacMultimediaExtensions, MacScanExtensions, or MacSearchFolders in the settings list.
3. Click New and type the filename or (or folder name for MacSearchFolders) you want. Press the Enter key when you’re done.
4. 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.
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.

For information on scanning for custom data, see "Scanning for custom data on Macintosh devices" (338).

**Remote control Macintosh devices**

You can remote control a Macintosh device from the console. 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.

NOTE: Macintosh devices only support HTML 5 remote control.

For more information about using remote control in Endpoint Manager, see "HTML remote control" (448).

**Connect to a Macintosh device**

You can connect to a Macintosh device and remote control it; you can also use chat, file transfer, or remote execute features.

**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.

NOTE: Clipboard sharing and draw features are not supported on Macintosh devices.

**Macintosh keyboard emulation**

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.
Inactivity timeout

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.

Accessing a Mac device with the 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 Ivanti 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 most tasks 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 Ivanti 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 Ivanti Agent for Mac installed. This feature works even if you’re not viewing a remote device’s screen.

You can save the messages from a chat session. 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 box, type in a filename and click Save.

Sending Macintosh key sequences

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.

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 box’s **Change settings** tab (Ivanti 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.
- **Hide the remote computer screen**: Makes the remote device’s screen blank 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 box’s **Optimize performance** tab (Ivanti 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.

Deploy software packages to 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, Endpoint Manager will decompress the file before returning.

NOTE: Make sure that Stuffit Expander has its “check for new versions” option disabled; otherwise a dialog box may interrupt the software distribution execution.

Software distribution also lets you distribute shell scripts as jobs. This lets you 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.

NOTE: You must install the Ivanti 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. For successful distribution, the package must exist on either a network or Web server and the recipient devices must have the software distribution agent installed.

Distribute a software package to Macintosh devices

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 packages, Public packages*, or *All packages*, click **New** on the toolbar and select **New Macintosh package**.
4. In the **Macintosh properties** dialog box, enter the package information and set the options. For more information on each page, click **Help**.
5. Click **Save** when you’re done. Your package appears under the tree item for the package type you selected.

**To create a delivery method**

1. Click **Tools > Distribution > Delivery Methods**.
2. Expand a delivery method group, right-click the type of delivery method you want to use, and then click **New delivery method**.
3. In the **Delivery method** dialog box, enter the delivery information and change the options you want. For more information on each page, click **Help**.
4. Click **Save** when you’re done. Your method appears under the tree item for the delivery method you selected.

**NOTE:** If a package requires a reboot, it will reboot the target device regardless of the option you select on the Reboot page of the Delivery method dialog box. The **Never reboot** option is not supported for Macintosh package distribution, because the target device could become unstable or not bootable if a package doesn’t initiate a reboot as expected.

**To schedule a software distribution task**

1. Click **Tools > Distribution > Scheduled Tasks**.
2. Click the **Create software distribution task** toolbar button.
3. On the **Overview** page, enter the task name and the task schedule. Review other options and click **Change** to makes changes to any of them.
4. On the **Distribution package** page, select the package you created.
5. On the **Delivery Method** page, select the delivery method you want to use.
6. The **Target devices** page has no devices listed. Devices are targeted for distribution after you drag them from the network view to the task in the Scheduled tasks tool.
7. The **Custom message** page is not applicable to Macintosh package distribution.
8. The **Schedule task** page is set to **Leave unscheduled**, unless you have targeted devices.
9. Click **Save** when you’re done. The task is listed in the **Scheduled tasks** tool.
10. To distribute the package, drag Macintosh devices from the network view onto the task. You can drag individual devices, group, or queries onto the task.

The distribution begins immediately. View the task progress in the Scheduled tasks window.

**Macintosh software distribution commands**

Macintosh software distribution commands are download commands, as opposed to a shell command. 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 download command format:

```shell
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.

**Configure 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 Ivanti 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 Ivanti agent application on the Macintosh device, click the Delivery icon.
2. Click Check now for application policy management.

To view installed policies

- In the Endpoint Manager Preference Pane on the Macintosh device, click the APM tab.

Expose the user interface to the client

You have the option of showing or hiding the UI to the client when distributing a software package. If the Ivanti 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 and timing from the tree.
3. Select Display progress to user from the Package progress UI list.
4. Select Display full package interface.
5. Click Save.
Execute custom tasks with managed scripts

Ivanti® Endpoint Manager powered by Landesk 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 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.

Run scheduled tasks on 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 "Scheduling tasks" (415).

NOTE: Before you can schedule tasks for a device, it must have the standard Ivanti 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

Software license monitoring and reporting

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 tool 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 Ivanti agent application can be used to show applications that have been launched and how often they have been used.

**Generate reports 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 "Using reports" (381).

**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.

**Configure Macintosh devices for security scanning and remediation**

Security functionality is included as part of the standard Ivanti 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 run a compliance scan from the Ivanti Management Console**

1. Click **Tools > Security and Compliance > Patch and compliance**.
2. Click the **Create a task** button on the toolbar, and select **Compliance scan**.
3. Type a name for the task and select **Create a scheduled task** or **Create a policy**, depending on how you want to run the scan.
4. In the **Scheduled tasks** tool, select the task and click the **Properties** button on the toolbar.
5. Specify the scan options. On the **Custom script** page you'll specify the details of the compliance scan.

For details on creating a compliance scan task, see "Create a patch and compliance scan task" (736)

---

**NOTE:** When you define settings for a compliance scan, some functionality is available for managed Macintosh devices. Point to items in each page of the dialog box; a message indicates when an item is not available for Macintosh scans.
To launch the security scanner on a Macintosh client

1. Open the Mac OS X System Preferences on the target device and select the Ivanti Client panel.
2. On the Overview tab, click Check Now in the Security and Patch Manager section.

Blocking applications for Macintosh devices

You can use the Endpoint Manager 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.

You can block only .app files on managed Macintosh devices. In order to block specific applications, you must create a custom definition for each blocked application. When creating the custom definition, be sure to select Apply to Mac.

Operating system provisioning for Macintosh devices

Ivanti® Endpoint Manager powered by Landesk OS provisioning fully supports Mac OS X devices. For detailed information, see this document on the Ivanti community:

Introduction to LANDESK Security Suite

Welcome to the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk

Ivanti® Endpoint Security for Endpoint Manager provides the tools you need, in a single integrated console, to secure and protect all of the devices and critical data on your enterprise network.

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk supports heterogeneous network environments that include Windows, Macintosh, and Linux clients.

Endpoint Security for Endpoint Manager is based on the primary Ivanti® Endpoint Manager powered by Landesk functionality that lets you configure and manage network devices, and then enhances and focuses that functionality by adding specific security-related tools like Patch and Compliance, Antivirus, Endpoint Security, Application Control, Ivanti Firewall, Device Control, Agent Watcher, Data Protection, and more; offering a comprehensive and layered security solution.

Comprehensive and layered security solution

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk is a complete security management solution that lets you proactively monitor, evaluate, remediate, verify, defend, and fortify your network infrastructure and resources.

The fundamental Patch and Compliance tool enables you to scan for and remediate the most prevalent types of security exposures and risks that continually threaten the health and performance of your managed devices, including: known operating system and application vulnerabilities, spyware, viruses, system configuration errors, unauthorized or prohibited applications, and other potential security exposures.

Ivanti Antivirus lets you download the latest virus definition file updates; and configure virus scans that check managed devices for viruses and provide the end user with options for handling infected and quarantined objects. Device Control allows you to monitor and restrict access to managed devices through network connections and I/O devices.

The table below shows how the Endpoint Security for Endpoint Manager tools complement each other and provide a strong, complete network defense:

<table>
<thead>
<tr>
<th>Security concern / task</th>
<th>Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge and verification</td>
<td>Console views:</td>
</tr>
<tr>
<td></td>
<td>- Security content lists</td>
</tr>
<tr>
<td></td>
<td>- Definition (and detection rule) properties</td>
</tr>
<tr>
<td></td>
<td>- Patch and compliance scan results</td>
</tr>
<tr>
<td>Security concern / task</td>
<td>Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk solution</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Antivirus activity and status information</td>
</tr>
<tr>
<td></td>
<td>Alerts</td>
</tr>
<tr>
<td></td>
<td>Reports</td>
</tr>
<tr>
<td>Patch management</td>
<td>Patch and Compliance</td>
</tr>
<tr>
<td></td>
<td>Ivanti updates</td>
</tr>
<tr>
<td></td>
<td>Driver updates</td>
</tr>
<tr>
<td></td>
<td>Software updates</td>
</tr>
<tr>
<td>Vulnerability assessment and remediation (known industry-published definitions, custom security definitions)</td>
<td>Patch and Compliance</td>
</tr>
<tr>
<td></td>
<td>Definition and patch file downloads</td>
</tr>
<tr>
<td></td>
<td>Security scans</td>
</tr>
<tr>
<td></td>
<td>Compliance scans</td>
</tr>
<tr>
<td></td>
<td>Patch deployment and installation</td>
</tr>
<tr>
<td></td>
<td>Autofix</td>
</tr>
<tr>
<td>Malware detection and repair</td>
<td>Antivirus</td>
</tr>
<tr>
<td></td>
<td>• Ivanti Antivirus pattern file updates and scans</td>
</tr>
<tr>
<td></td>
<td>• Third-party antivirus content updates</td>
</tr>
<tr>
<td></td>
<td>Spyware scans</td>
</tr>
<tr>
<td></td>
<td>Riskware scans</td>
</tr>
<tr>
<td></td>
<td>Real-time scans</td>
</tr>
<tr>
<td></td>
<td>Application blocker</td>
</tr>
<tr>
<td>Device configuration, zero-day attack protection, and lockdown</td>
<td>Endpoint Security</td>
</tr>
<tr>
<td></td>
<td>• Location awareness (network connection control)</td>
</tr>
<tr>
<td></td>
<td>• Application Control</td>
</tr>
<tr>
<td></td>
<td>• Ivanti Firewall</td>
</tr>
<tr>
<td></td>
<td>• Device Control</td>
</tr>
<tr>
<td></td>
<td>• Trusted File Lists</td>
</tr>
<tr>
<td></td>
<td>Security threats (system configuration exposures)</td>
</tr>
<tr>
<td></td>
<td>Windows Firewall configuration</td>
</tr>
<tr>
<td></td>
<td>Agent Watcher</td>
</tr>
<tr>
<td>Unmanaged device scan and discovery</td>
<td>Unmanaged Device Discovery</td>
</tr>
<tr>
<td></td>
<td>Extended Device Discovery (ARP and WAP)</td>
</tr>
</tbody>
</table>
Once you’ve installed Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk and activated your core server with a Endpoint Security for Endpoint Manager license, you can refer to specific help topics for information on starting the console and using the available tools, including the security-specific tools and features listed below.

Navigate the Ivanti® Endpoint Manager powered by Landesk and Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk help topics in the Ivanti Help Center or perform a search using a specific key word or phrase to find the information you want.

**IMPORTANT:** **Endpoint Security for Endpoint Manager doesn’t include all Endpoint Manager components**

Keep in mind that some Endpoint Manager components do not apply to a Endpoint Security for Endpoint Manager implementation, such as OS provisioning and rollup cores.

---

**Install and activate Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk**

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk and Ivanti® Endpoint Manager powered by Landesk both use the same setup program to install the necessary components on your core server. As with other Ivanti software products, such as Endpoint Manager and Inventory Manager, it’s when you actually activate the core server with your Ivanti account information that the applicable Endpoint Security for Endpoint Manager functionality is made available in the console.

If your account is licensed for Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk, you’ll see the tools and features described in the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk help topics when you log into the console.

**Ivanti User Community resources**

Installing and deploying enterprise applications like Ivanti systems and security solutions software to a heterogeneous network requires a deliberate methodology and significant planning before you run the setup program.

Because the network infrastructure and database scalability requirements and considerations are similar between Endpoint Manager and Endpoint Security for Endpoint Manager, and because these Ivanti products use the same setup program, you should refer to the *Installation and Deployment BKM* (best known method) documents located at the Ivanti Support User Community.

**NOTE:** **The Ivanti User Community**

The Ivanti User Community has user forums and best known methods for all Ivanti products and technologies. To access this valuable resource, go to: [Ivanti User Community Home Page](#)
The User Community hosts several useful documents that provide detailed information on deployment strategies and step-by-step instructions for each phase of your Ivanti software deployment, such as:

- Design your management domain
- Prepare your database
- Install or upgrade the Ivanti core server
- Understand port usage
- Configure managed device agents

**Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content subscriptions**

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk offers scanning and remediation support for several different types of security risks, including known OS and application vulnerabilities for supported device platforms, spyware, viruses, system configuration threats, unauthorized applications, and more. Each security risk, of any type, is characterized by definition files. A definition file is typically comprised of an ID, specific attributes, detection rule details, and patch file information if applicable.

Ivanti maintains a database of validated security definition files, referred to as Endpoint Security for Endpoint Manager content or security and patch content, that are continuously updated, verified, and made available via web download. In order to download security and patch content you must have an associated Endpoint Security for Endpoint Manager content subscription.

For information about Endpoint Security for Endpoint Manager content subscriptions, contact your Ivanti reseller, or visit the Ivanti website:

[IVANTI HOME PAGE](#)

**Download security updates from Ivanti**

The Patch and Compliance section in the help describes how to download the security and patch content for which you have subscriptions. For more information, see "Download security content" (724).

**Related topics**

"Endpoint Security for Endpoint Manager tools and features" (672)
Endpoint Security for Endpoint Manager tools and features

The underlying tool of Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk is called Patch and Compliance. For information about security content and supported device platforms, and how to use the Patch and Compliance tool to perform security and compliance scanning and remediation, view scan results, generate security reports, and configure ongoing system security, see "Patch and Compliance" (679).

This help topic includes brief overviews of the following security management tools provided by the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk, with links to the tool's overview topic:

- "Patch and Compliance" (672)
- "CVE naming standard compliance" (673)
- "Federal Desktop Core Configuration (FDCC) standards compliance" (673)
- "Security Activity" (674)
- "Agent Settings" (674)
- "Endpoint Security" (674)
  - "Application control overview" (793)
  - "Agent settings: Ivanti Firewall" (270)
  - "Device Control overview" (805)
- "Ivanti Antivirus" (675)
- "Common Ivanti tools included with Endpoint Security for Endpoint Manager" (676)
- "Other Ivanti® Endpoint Manager powered by Landesk features included with Endpoint Security for Endpoint Manager" (678)
- "Where to go for more information" (678)

Patch and Compliance

Use Patch and Compliance to download the latest known vulnerability definitions (and other security content type definitions) and their associated patches. Scan managed devices, as well as core servers and consoles, for Ivanti software updates. Configure and run customized security assessment scans for known platform-specific vulnerabilities, spyware, system configuration security threats, antivirus scanners, and blocked or unauthorized applications.

With the Patch and Compliance tool, you can also:

- Create your own custom security definitions to scan devices for specific, potentially threatening conditions.
- Research, prioritize, download, and deploy and install patches.
- Create and run scheduled tasks and policies that remediate detected security risks.
• Configure whether the security scanner displays on end user devices during scan and repair processes, device reboot options, and the level of user interaction.
• View comprehensive security and patch information for scanned devices.
• Enable security alerting.
• Generate security reports.

For more information, see "Patch and Compliance" (679).

NOTE: Patch and Compliance scans in a Ivanti® Endpoint Manager powered by Landesk implementation

The Patch and Compliance tool is included by default in a Ivanti® Endpoint Manager powered by Landesk installation (core server activation). However, initially you can scan only for Ivanti software updates and your own custom security definitions. To scan for and remediate additional security types, you must have the corresponding Endpoint Security for Endpoint Manager content subscription.

CVE naming standard compliance

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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, Ivanti compatibility with the CVE standard, and how to use CVE identification to find individual vulnerabilities in Patch and Compliance, see "Search for vulnerabilities by CVE name" (730).

Federal Desktop Core Configuration (FDCC) standards compliance

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk now provides extended support for the Federal Desktop Core Configuration (FDCC) Initiative. Ivanti software products have been certified by the National Institute of Standards and Technology (NIST) as conforming to the Security Content Automation Protocol (SCAP) standards, and are listed as validated products at the National Vulnerability Database website.

In order to perform FDCC security scanning and remediation tasks, you must have a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content subscription that allows you to download the FDCC-specific content, which includes: FDCC scanner detection and installation; FDCC compliance scanning and status reporting; and FDCC-certified vulnerability scanning and remediation by component.

With the FDCC-certified scanner and security content, you can scan your managed devices to ensure they comply with the Federal Desktop Core Configuration standards and requirements.

For more information about how to use the FDCC scanner and security content, see "Secure Content Automation Protocol (SCAP)" (740).
**Security Activity**

The Security Activity tool lets you view critical activity and status information for several security components and services. Security Activity provides a single tool window where you can easily see Ivanti Antivirus scan results, HIPS preventions, Ivanti Firewall preventions, Device Control blocked devices, and more.

For more information, see "Security Activity overview" (781).

**Agent Settings**

The Agent Settings tool let you create and manage settings files for several security components and services. Configurations (i.e., settings files) control how security services operate on managed devices.

With the Agent Settings tool, you can deploy security agent/services and their associated settings to your managed devices as part of the initial agent configuration, separate install or update tasks, and change settings tasks.

For more information, see "Agent Settings overview" (317).

**Endpoint Security**

The Endpoint Security tool protects your managed devices from zero-day attacks, firewall intrusions, prohibited application and process actions and behaviors, and unauthorized network and device connections.

Endpoint Security is comprised of customized settings files (saved feature and option configurations) that can be deployed to target devices for the following security components:

- Location awareness (network connection control via trusted locations)
- Host Intrusion Prevention System (HIPS)
- Ivanti Firewall
- Device Control
- Trusted File Lists

**Application Control**

Ivanti Application Control provides an additional layer of protection that proactively secures systems and applications from zero-day attacks (i.e., malicious unauthorized behavior). Using customized rules and file certifications, HIPS continuously monitors specified processes, files, applications, and registry keys, and blocks prohibited actions and behaviors. With Application Control, you can control which applications run on devices and how they are allowed to execute. Application Control lets you protect the file system, registry, system startup, and even detect stealth rootkits.
Because Application Control is a rule-based system, instead of a definition-based (i.e., signature-based) system such as known vulnerability, spyware, and antivirus scanning, it doesn’t require ongoing file updates. You configure and deploy your own customized level of system security.

For more information, see "Application control overview" (793).

**Ivanti Firewall**

Ivanti Firewall lets you create and configure proprietary firewall settings to prevent unauthorized application behavior on your managed devices.

**IMPORTANT: Ivanti Firewall and Windows Firewall compatibility**

The Ivanti Firewall complements the Windows Firewall, and both can be enabled and running at the same time on managed devices.

For more information, see "Agent settings: Ivanti Firewall" (270).

**Device Control**

Device Control adds another level of security to your Ivanti network by allowing you to monitor and restrict access to managed devices through 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, USB devices, and wireless connections.

For more information, see "Device Control overview" (805).

**Ivanti Antivirus**

Ivanti Antivirus lets you protect all of your managed devices from the latest known viruses as well as suspected infections. Antivirus scans can also check for riskware (via an extended database). Ivanti Antivirus is a configurable virus protection tool that is fully integrated with both Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk and Ivanti® Endpoint Manager powered by Landesk.

Ivanti Antivirus provides a wide range of antivirus features, including: scheduled antivirus scans, on-demand scans, red-button scans, real-time file and email protection, automated downloading of virus definition file updates (the Ivanti virus signature database contains the very latest known virus definitions and is renewed several times a day), configuration of antivirus scan behavior and end user options, scan exclusions, as well as antivirus alerts and reports.

Additionally, you can view real-time antivirus information for scanned devices in both the main console and the web console's executive dashboard to quickly identify virus outbreaks and see virus control over a specified period of time.

For more information, see "Ivanti Antivirus overview" (815).
Common Ivanti tools included with Endpoint Security for Endpoint Manager

Common Ivanti tools provide the underlying device configuration and management capabilities in both Endpoint Manager and Endpoint Security for Endpoint Manager. The following tools are available in a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk implementation, appearing in the Tools menu in the console.

IMPORTANT: Be aware that some of these common tools have certain restrictions in a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk license activation.

Agent Configuration

Use Agent Configuration to create custom agent configurations to deploy and install the necessary Ivanti agents required to manage and protect your network devices. These agents are the standard Ivanti agent (that includes the inventory scanner, local scheduler, bandwidth detection, and security scanner), the software distribution agent, and the software license monitoring agent (used for application blocking).

NOTE: Agents not applicable to Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk
The following Ivanti agents (components) are NOT applicable in a Endpoint Security for Endpoint Manager installation:

- Custom data forms
- Remote control
- OS provisioning

Reports

Use the Reports tool to generate and publish a wide variety of specialized reports that provide useful information about your managed devices, including several predefined Patch and Compliance, Antivirus, and Compliance reports.

NOTE: Reports not applicable to Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk
The following report categories are NOT applicable to the Endpoint Security for Endpoint Manager: All Asset Reports, All SLM Reports, and All Remote Control Reports.

Scheduled Tasks

Use Scheduled Tasks to create recurring tasks specifically related to security and patch management, remediation, compliance security enforcement, antivirus scans, and more. You can configure the task’s targeted devices and scheduling options.
Unmanaged Device Discovery

Use Unmanaged Device Discover (UDD) to locate devices on your network that haven’t submitted an inventory scan to the core database.

Extended device discovery (XDD) works outside the normal scan-based discovery methods used by UDD. Managed devices with the extended device discovery agent on them 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. Extended device discovery can also detect WAP (wireless access point) devices.

Role-based administration

The User Management tool let you add users to Endpoint Security for Endpoint Manager management roles, and configure their access to specific tools and managed devices based on their administrative role.

With role-based administration, you assign roles (with their associated rights) to determine the tasks users can perform, and scopes (based on device groups, queries, LDAP directories, or custom directories) to determine the devices a user can view and manage. Roles that are available with Endpoint Security for Endpoint Manager include: Patch and Compliance, Network Access Control, Agent Settings, Software Distribution, Public Query Management, and Unmanaged Device Discovery.

Local accounts

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.
Other Ivanti® Endpoint Manager powered by Landesk features included with Endpoint Security for Endpoint Manager

In addition to the tools listed above that appear in the console Tools menu, Endpoint Security for Endpoint Manager provides the following common Ivanti features:

- Windows console, additional consoles, web console
- Custom console layouts
- Network view for managed devices and queries
- Shortcut menus for managed devices and queries
- Service configuration
- Inventory
- Database queries
- Software distribution
- Software license monitoring
- Alerting
- Content replication and preferred servers

**IMPORTANT:** Custom data forms are not supported in Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk

The Custom data forms tool is not available with a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk only license. You must have a full Ivanti® Endpoint Manager powered by Landesk license in order to use custom data forms.

Where to go for more information

Following the security tool help topics, the remainder of the linked help topics are found in the Ivanti® Endpoint Manager powered by Landesk help sections that cover the common Ivanti tools mentioned above (including information about understanding and using the console and network view).

**NOTE:** The Ivanti User Community

The Ivanti User Community has user forums and best known methods for all Ivanti products and technologies. To access this valuable resource, go to: [Ivanti User Community Home Page](#)

Related topics

"Welcome to the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk" (668)
Patch and Compliance

Patch and Compliance

Patch and Compliance is a complete, integrated security management tool that helps you protect your Ivanti managed devices from a variety of prevalent security exposures and risks. Ivanti Patch Manager is sold as an add-on product to Endpoint Manager and is included in Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk.

Use security scan tasks and policies to assess managed devices for known platform-specific vulnerabilities. Download and organize patch executable files, and then remediate detected vulnerabilities by deploying and installing the necessary patch files. You can also create your own custom definitions to scan for and remediate specific, potentially harmful conditions on devices. Additionally, at any time you can view detailed security information for scanned devices, and generate specialized patch and compliance reports.

In addition to patch management, use the Patch and Compliance tool to perform the following tasks:

- Verify that the latest Ivanti software is installed and up to date on your managed devices, as well as core servers and console machines.
- Use a blocked application definition to deny unauthorized or prohibited applications on devices.
- 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.

Supported device platforms

Patch and Compliance supports most of the standard Ivanti managed device platforms. For details about supported platforms, see Support Platforms and Compatibility Matrix for Ivanti Endpoint Manager in the Ivanti Community.

IMPORTANT: Scanning core servers and consoles for Ivanti software updates is supported

You can also scan Ivanti core servers and consoles for Ivanti software updates, but those machines must first have the standard Ivanti agent deployed, which includes the security scanner agent required for security scanning tasks.

Role-based administration with Patch and Compliance

A user with the Patch and Compliance right can perform most of the tasks associated with the Patch
and Compliance tool. The Patch and Compliance right appears under the Security rights group in the Roles dialog box. However, there are some tasks that require additional rights:

- To use Autofix to automatically remEDIATE these detected security types—vulnerabilities, spyware, Ivanti software updates, and custom definitions—you must be a Ivanti Administrator.
- To purge unused security type definitions, you must be a Ivanti Administrator.
- To generate a variety of security-specific reports, you must also have Reporting roles.

Administrators assign these roles to other users with the Users tool in the console.

Choose from one of the following topics for more information about Patch and Compliance:

- "Getting started with Patch and Compliance" (680)
- "How Patch and Compliance scans and remediates" on the next page
- "Open and understand the Patch and Compliance tool" on page 683

**Getting started with Patch and Compliance**

The list below outlines the main tasks involved in configuring, implementing, and using Patch and Compliance.

1. Configure the Ivanti agent with patch settings. For information on agent settings for patch and compliance, see "Configure devices for security scanning and remediation" on page 689.
2. Download vulnerability definitions from a Ivanti security content server (updated from industry and vendor data sources). For information about downloading definitions, see "Download security content" (724).
3. Create a scan task and scan your devices. For information about scanning devices, see "Scanning devices for vulnerabilities" (734).
4. Use the scan results to decide what and how you are going to patch. Organize the security content accordingly. For more information, see "Managing security content" (723). For instructions on viewing the vulnerabilities that have been detected in your environment, see "View detected vulnerabilities" (738).
5. Download patches (used to remEDIATE detected vulnerabilities). For information about downloading patches, see "Download security content" (724).
6. Repair detected vulnerabilities by deploying and installing patches to affected devices. For information about patching, see "Patching devices with vulnerabilities" (745).
7. View reports that provide patch status and repair history information. For information about patch reporting, see "Generate Patch and Compliance reports" (766).

If you’re new to Patch and Compliance, the following related topics may help you understand how Patch works in your environment:
• "Patch and Compliance" (679)
• "How Patch and Compliance scans and remediates" below
• "Open and understand the Patch and Compliance tool" on page 683
• "Scanning devices for vulnerabilities" (734)

How Patch and Compliance scans and remediates

The table below describes how the Patch and Compliance security scanner searches for each type of security risk and the steps taken during remediation:

<table>
<thead>
<tr>
<th>When scanning for...</th>
<th>Patch and Compliance scans by...</th>
<th>and remediates by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ivanti software updates</td>
<td>Using software update definitions published by Ivanti to check for the latest Ivanti software versions.</td>
<td>Installing the appropriate Ivanti software update.</td>
</tr>
<tr>
<td>Windows and Mac vulnerabilities</td>
<td>Using vulnerability definitions published by Ivanti (based on official security bulletins) to check for known operating system and/or application vulnerabilities.</td>
<td>Using a scheduled task or an autofix to deploy and install the required patch files. Patch files must already be downloaded to the local patch repository.</td>
</tr>
<tr>
<td>Mac vulnerabilities</td>
<td>Using vulnerability definitions published by Ivanti (based on official security bulletins) to check for known vulnerabilities.</td>
<td>Using a scheduled task or an autofix to deploy and install the required patch files. Patch files must already be downloaded to the local patch repository.</td>
</tr>
<tr>
<td>Linux/UNIX vulnerabilities</td>
<td>Using vulnerability definitions published by Ivanti (based on official security bulletins) to check for known vulnerabilities.</td>
<td>Using a scheduled task or an autofix to deploy and install the required patch files. Patch files must already be downloaded to the local patch repository.</td>
</tr>
<tr>
<td>Custom definitions</td>
<td>Using custom vulnerability definitions created by an Ivanti Administrator to check for a user-defined platform, application, file, or registry setting conditions.</td>
<td>Deploying a custom patch or script that addresses the situation. You may have the remediation as part of the initial definition, or as a separate patch.</td>
</tr>
<tr>
<td>Security threats</td>
<td>Using security threat definitions published by Ivanti 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.</td>
<td>Applying the configuration settings specified by the security threat definition. 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.</td>
</tr>
<tr>
<td>When scanning for...</td>
<td>Patch and Compliance scans by...</td>
<td>and remediates by...</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Spyware</td>
<td>Using spyware detection definitions that check for instances of spyware programs on scanned devices. Patch and Compliance uses the Ivanti 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.</td>
<td>Removing the violating spyware application (as a repair task) or blocking the application when it tries to run. To enable real time blocking, enable autofix and spyware blocking in the agent settings and set the spyware definitions to autofix.</td>
</tr>
<tr>
<td>Driver updates</td>
<td>Using third-party driver update definitions that check for driver versions.</td>
<td>Deploying and installing the appropriate third-party driver update.</td>
</tr>
<tr>
<td>Software updates</td>
<td>Using third-party software update definitions that check for software versions.</td>
<td>Deploying and installing the appropriate third-party software update.</td>
</tr>
<tr>
<td>Antivirus updates</td>
<td>Using antivirus scanner detection definitions (NOT actual virus definition/pattern files) that check for: - Installation of common antivirus scanner engines (including the Ivanti 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)</td>
<td>For Ivanti Antivirus, use Ivanti software updates to update the antivirus engine. For other antivirus engines, you must manually remediate.</td>
</tr>
<tr>
<td>Blocked applications</td>
<td>Using application definitions published by Ivanti (or user-defined application definitions) to immediately deny end user access to the application by editing the local registry. Patch and Compliance uses the Ivanti 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.</td>
<td>Blocking the application when it tries to run, 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 &quot;Legal disclaimer for the blocked applications type&quot; (734).)</td>
</tr>
</tbody>
</table>

For information about how to get started downloading patch definitions and scanning for vulnerabilities, see "Getting started with Patch and Compliance" (680).
Open and understand the Patch and Compliance tool

The Patch and Compliance tool, like all other Ivanti tools, is opened from either the Tools menu or the Toolbox and can be docked, floated, and tabbed with other open tool windows.

To open the Patch and Compliance tool, click **Tools > Security and Compliance > Patch and Compliance**.

The pane on the left shows a tree view of security type definition and detection rule groups.

The pane on the right displays information associated with what is selected in the tree view. When you have Patch and Compliance selected, you can view a dashboard of reports. When other items are selected, it displays a list of the selected group's definition details and a Find feature for searching in long item lists.

In the **Find** box, the following extended characters are not supported: < > ' " !

**IMPORTANT: Patch and Compliance right**

In order to access the Patch and Compliance tool, users must either be an Ivanti Administrator, or have the Patch and Compliance right. For more information about user roles and rights, see "Role-based administration overview" (52).

**Toolbar buttons**

The Patch and Compliance tool window contains a toolbar with the following buttons:

- **All types**: Displays the type of content you want to view. When you select Antivirus, it lists downloaded scanner detection definitions only. It does not list specific Ivanti Antivirus virus definition files.

- **Global (all devices)**: Limits the items displayed to a specific scope.
• **All items:** Filters the displayed items based on a custom filter. For information on creating and using a custom filter, see “Customize item lists with filters” (732).

• **Download updates:** Opens a dialog box where you can specify the security content you want to download. This includes selecting the platforms and languages, 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 security scanner display options, 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 by the contents of the Compliance group.

  • **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. 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 and select scan and repair settings that determine display and interaction behavior. Note that only the options on the reboot page of the dialog box 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 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:

  • **Agent settings:** Lets you create, edit, copy, and delete agent settings. Agent settings determine whether the security scanner displays on devices while running, reboot options, user interaction, and the content types scanned.
• **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.

• **Core settings**: Lets you manage scan results, autofix retry preferences, and rollup core configuration.

• **Permissions**: Lets you view the current user’s Patch and Compliance console permissions. You can also adjust how the console interprets “edit” and “edit public” permissions.

• **Manage tags**: Lets you create, edit, and delete tags to organize patch content.

• **Display dashboard in a separate window**: Opens the Patch and compliance dashboard, allowing you to view and organize charts that display patch information.

• **Import definitions**: Allows you to import an XML file containing custom definitions.

• **Export 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.

• **Add**: Depending on what is selected in the tree, creates a new chart, custom definition, or tag. If the selected item in the tree is allowed to create a custom definition, it adds a custom definition. If Patch and Compliance is selected, it adds a new chart. If Tags is selected, a new tag is created.

• **Properties**: Displays the properties of the selected chart, group, or definition.

• **Delete selected items**: Removes the selected items 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. Only an Ivanti Administrator can perform this operation.

• **Disable replaced rules**: Lets you select how you want replaced rules to be handled. Replaced rules are rules that are superceded by other definitions in your environment.

• **Help**: Opens the help to the Patch and Compliance section.
All items (definitions in the 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.

The All types object contains the following subgroups:

- **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**: Blocked applications are added to the Unassigned group by default.

Scan is one of the three possible states for a security definition, along with Do not 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, Do not scan, or Unassigned and is identified by a unique icon for each state (question mark [?] icon for Unassigned, red X icon for Do not 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 (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: Moving definitions from the Scan group**

When you move definitions from the Scan to the Don’t Scan group, the information about which devices detected those definitions is removed from the core database and is no longer available in either the definition Properties dialog boxes or in the device Security and Patch Information dialog boxes.

- **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 Do not scan groups.

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 indicates whether the patch associated with that rule has been downloaded.

- **Do not scan**: (For Blocked Applications, this group is called **Do not 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 Do not 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, drag one or more from the Unassigned group into either the Scan or Do not scan groups.

New definitions can also be automatically added to the Unassigned group during a content update by selecting the **Put new definitions in the Unassigned group** option on the Download updates dialog box.

- **View by product**: Lists all of the definitions organized into specific product subgroups. These subgroups help you identify definitions by their relevant product category.

- **View by vendor**: Lists all of the definitions organized into specific product subgroups. These subgroups help you identify definitions by their relevant vendor.

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, Do not scan, or Unassigned group, or any of the user-defined custom groups. They can reside in platform, product, and multiple custom groups simultaneously.

**Groups**

A group allows you to perform actions (such as a targeted scan, repair task, or a query) for a specific set of definitions. For example, you may choose to set up a Ready for Repair group that contains patches that have been tested and are ready to be applied.

A definition can belong to more than one group at a time. Adding a definition to a group does not change its status in a Scan or Do not scan folder. However, you can perform tasks for that group that will move the definition.
The **Groups** object contains the following default subgroups:

- **Custom Groups**: Lists the groups you've created and the definitions they contain. **My custom groups** provide a way for you to organize security definitions however you want.

  To create a custom group, right-click **My custom groups** (or a subgroup) and then click **New Group**.

  To add definitions to a custom group, 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 groups**: Lists any predefined vulnerability definition groups as determined by the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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.

- **Alert**: Lists all of the definitions that will generate an alert message the next time the security scanner runs on devices.

- **Compliance**: Lists all of the definitions that are used to determine whether a device is Healthy or Unhealthy. 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. When you run a Compliance scan using the **Create a task** button, it uses the definitions in this group.

### Tags

Tags are a way to organize definitions. A definition can have multiple tags associated with it. Create a filter or query to view the details of definitions that have been tagged.

No actions are taken based on tags. If you want to organize definitions and then take actions based on the groupings, use a group instead of a tag. A rollout project may edit the tags associated with a definition, but it does not take action based on the tag state.

Manage tags by clicking **Configure settings > Manage tags**.

### Detection rules

The **Detection rules** object only appears in the tree when you have selected **Vulnerability** or **Custom definition** as the type. This object displays the detection rules associated with definitions.

---

**IMPORTANT: Security definition types that use 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 and custom definitions. Spyware and blocked applications do not
The Detection rules group contains the following subgroups:

- **Scan**: Lists all of the detection rules that are enabled for security scanning on devices. Detection rules are automatically added to this list when you update patch content.
- **Do not 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. This can 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.

NOTE: For more information on the Dashboard, see Dashboard editor.

**Configure devices for security scanning and remediation**

Use Distribution and Patch settings in the agent settings to determine what gets scanned, what the end user sees for a scan, 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 a scan or patch application.

A device's default scan and repair settings are deployed as part of the initial agent configuration. When a task has 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 them when you create a task.

**Configure Windows devices for security scanning**

The standard Ivanti agent for Windows devices includes the vulnerability scanner, which can perform patch and compliance scanning and remediation. Configure settings for how scanning and remediation are performed in the agent settings.

**To create scan and repair settings**

1. Click **Tools > Configuration > Agent Settings**.
2. In the **Agent settings** window, select Distribution and Patch in the tree and click the **Create new settings** toolbar button. Or you can click **Edit** or **Configure** on any of the task dialog boxes that let you apply scan and repair settings.
3. Enter a name for the distribution and patch settings.
4. Specify the various settings on each page as desired for the particular task. For information about the Distribution and Patch settings, see "Agent settings: Distribution and patch" (251).
5. Once configured, you can use the settings for security scan tasks, repair tasks, uninstall tasks, reboot tasks, and change settings tasks.

To change a device’s default scan and repair settings

1. In the Patch and Compliance tool window, click the Create a task toolbar button, and then click Change settings.
2. Provide a name for the task, specify whether it is a scheduled task or policy, and either select an existing scan and repair setting as the default or use the Edit button to create a new scan and repair setting as the default for target devices.
3. Select the targets for the task and either schedule it or start the task now.

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 "Agent settings: Distribution and patch" (251).

NOTE: WinSock2 is required on Windows 9x devices in order for the security scanner to run.

After the agent is configured, a program icon for the security scanner is added to the Ivanti 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 file lists
- Windows Firewall
- Endpoint Security which includes the security components: Endpoint security, Ivanti Firewall, and Device Control

Configure Linux and UNIX devices for security scanning

Patch and Compliance supports vulnerability scanning on supported Linux and UNIX platforms.
Content downloads, scheduling scans, and scan results are all available using the Ivanti management console. You can perform remediation for vulnerabilities on Linux platforms, but Linux does not currently support the Autofix feature. Remediation is a manual process for UNIX.

For additional Linux and UNIX information, see this page on the Ivanti community: https://community.landesk.com/support/community/systems/nix.

**Configure Mac OS X devices for security scanning**

Patch and Compliance supports vulnerability scanning on Mac OS X platforms.

Additionally, you can create and configure agent configuration for your Macintosh devices with the Agent configuration tool. Configuring the agent for patch management, content downloads, scheduling scans, and scan results are available using the Ivanti management console. However, remediation is a manual process.

For more information about creating and deploying a Macintosh agent configuration with security scanner support, see "Macintosh device management overview" (646).

**To launch the security scanner manually on Mac devices**

1. Open the Mac OS X System Preferences and select the Ivanti Client page.
2. On the Overview tab, click Check Now in the Security section.

**Patch and Compliance help**

The Patch and Compliance tool window (Tools > Security and Compliance > 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" (679) introduces this security management tool. In that section, you’ll find overview and security content subscription information and 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 "Open and understand the Patch and Compliance tool" (683)). For information on Patch settings, see "Agent settings: Distribution and patch" (251).

This section contains help topics that describe the Patch and Compliance dialog boxes. From the console interface, these help topics are accessed by clicking the Help button on each dialog box.

- "Patch and Compliance tool window help" (692)
- "Download security content updates help" (693)
- "Definition properties help" (697)
- "Detection rule properties help" (701)
• "Patch and Compliance tasks help" (710)
• "Patch and Compliance toolbar help" (721)

**Patch and Compliance tool window help**

**About the Select columns dialog box**

Use this dialog box to configure data columns for item lists in the Patch and Compliance tool window. You decide which data columns to display, so that you can quickly sort through long lists of downloaded security definitions to find the information needed for a specific task or situation.

*NOTE: Using the CVE ID data column*

Ivanti® Endpoint Security for Endpoint Manager, powered by 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, Ivanti compatibility with the CVE standard, and how to use CVE identification to find individual vulnerabilities in Patch and Compliance, see "Search for vulnerabilities by their CVE name" (731).

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 box**

Use this dialog box 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 box where you can configure a new filter's settings.

• **Edit:** Opens the Filter properties dialog box 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 box

Use this dialog box 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 item lists. Only those items whose severity matches the ones you select are displayed.

Download security content updates help

About the Download updates dialog box

Use this dialog box 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 box:

- To perform an immediate download, click **Download Now**. If you click **Apply**, the settings you specify will be saved and will appear the next time you open this dialog box. If you click **Close**, you’ll be prompted to save the settings.

- To schedule a download security content task, click **Schedule download**. Enter a name for the task, verify the information, and then click **OK** to add the task to Scheduled tasks.

- You can click **View log** to open the log file.

To save your changes on any page of this dialog box, click **Apply**.

The **Download updates** dialog box contains the following pages:

- "About the Updates page" (694)
- "About the Proxy settings page" (696)
- "About the Patch location page" (696)
- "About the Ivanti Antivirus page" (697)
- "About the Content page" (697)
- "About the Import/Export page" (697)
IMPORTANT: Special considerations regarding security content downloading

Endpoint Security for Endpoint Manager content subscriptions

A basic Endpoint Manager installation enables you to download and scan for Ivanti software updates and create and use your own custom definitions. For all other security content types, such as platform-specific vulnerabilities, spyware, and so on, you must have an Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content subscription to download the associated definitions.

For information about Endpoint Security for Endpoint Manager content subscriptions, contact your Ivanti reseller, or visit the Ivanti website: Ivanti Home

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 box 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 setting, it is effective for all security content download tasks from that point on.

About the Updates page

- **Select update source site:** Specifies the Ivanti 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 All types drop-down list in the main Patch and Compliance tool window to determine which definition types are displayed in a list.

- **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 Ivanti 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 Ivanti software updates currently residing in the Scan group.
  
  - **Enable automatic patch deployment using Process Manager**: Lets you configure the Ivanti Process Manager database that is required for using the integrated automatic patch deployment feature.
  
  - **Ivanti Process Manager**: Opens the Automating patch deployment dialog box describing the integrated capability between Ivanti Process Manager and the Patch and Compliance tool. From here, you can 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, as well as help topics.
  
  - **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 move content manually in and out of the Scan group to customize the security scan.

**NOTE**: Definitions that have a 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 you’ve already placed in the Alert group (in the Configure alerts dialog box) 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 box where you can create, manage, and select definition groups. You can use definition group settings to automate scan status, download location, and how security definitions (content) that match specified type and severity criteria are downloaded.

**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 downloading patch files from the 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:** Identifies the IP address and port number for 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.

**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 URL.

• **Reset to default:** Restores both the UNC path and the URL to the default location, which is the core server’s \LDLogon\Patch folder.
About the Ivanti Antivirus page

Use this page to configure download options for Ivanti Antivirus virus definition files. Keep in mind this page applies only to actual virus definition files that are used by Ivanti 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 Ivanti Antivirus page on the Download Updates dialog box" (221).

About the Content page

Use this page to specify whether to require verification before downloading definitions. Requiring verification makes the download more secure.

- **Verify definition signatures hashes before downloading:** Check to exclude any definitions that do not have a valid SHA256 hash. The signatures that are excluded from the download will appear as failures.

About the Import/Export page

Use this page to import or export a group of download settings that you previously specified on all of the pages of the Download updates dialog box. If you have multiple cores, this allows you to save time by copying the settings to each core so that you don’t have to select the individual settings on each machine.

- **Import settings from file...** Click to open the Select File to Import dialog, then browse to the *.ldms files you wish to import and click Open.
- **Export settings to file...** Click to open the Select export filename dialog, then browse to the settings you wish to export and click Save.
- **Copy settings to another core**. Click to open the Copy content to cores dialog, then select one or more servers and click Copy content.

Definition properties help

About the Definition properties dialog box

Use this dialog box 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 box are editable. You can enter identification, attribute, and detection rule details information for a custom definition by using the available fields on this dialog box and on the detection rule properties dialog box.

Use the left and right arrow buttons (<, >) to view the previous or next definition's property information in the order they're currently listed in the main window.

The Definition properties dialog box contains the following pages:

- "About the Definition: General page" (698)
- "About the Definition: Description page" (699)
- "About the Definition: Dependencies page" (699)
- "About the Definition: Custom Variables page" (699)

**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 "Open and understand the Patch and Compliance tool" (683).
- **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.

**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 "Search for vulnerabilities by their CVE name" (731).

**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 the values of one or more setting so that the scanner checks for conditions you define, and then determines a device to be vulnerable only if that condition is met.

**IMPORTANT: Edit Custom Variables right required**

To edit custom variable settings, a 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.
- **Add variable**: Opens a dialog box where you can create your own custom variable. (NOTE: Before you can create a custom variable for a custom vulnerability definition, the definition must first contain at least one detection rule.)
- **Edit variable**: Lets you edit the selected custom variable.
- **Remove variable**: Deletes the selected custom variable.
- **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.

**NOTE: Custom variable override settings**

In some situations, you may want the scanner to ignore custom variable settings by using a feature called Custom variable override settings. You can specify that the scanner ignore certain custom variables when scanning devices so that the variables aren't detected as vulnerable and aren't remediated, even if they meet the actual conditions of a definition's detection rules. A user must have the Edit Custom Variables right to create or edit these override settings. You can create as many settings as you like, and apply them to devices using a **Change settings** task. For more information, see “Agent settings: Custom variables to override” (248).
About the Add/edit custom variable dialog box

Use this dialog to create and edit your own custom variables for your custom vulnerability definitions. 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).

**IMPORTANT:** Before you can create a custom variable for a custom vulnerability definition, the definition must first contain at least one detection rule.

This dialog contains the following options:

- **Name:** Identifies the custom variable.
- **Description:** Lets you provide additional useful information about the custom variable.
- **Type:** Identifies the type of resource used to define the custom variable (types include: string, encrypted string, multi-value string, integer, enumeration, boolean).
- **Possible values:** Enter all of the possible values that can be considered valid for the custom variable you’re creating (based on the type specified above).
- **Default value:** Enter the default value for the custom variable.

Detection rule properties help

About the Detection rule properties dialog box

Use this dialog box to view detection rule properties for downloaded security content and to create and edit custom detection rules.

This information is read-only for detection rules belonging to downloaded definitions. For custom definitions, the fields of this dialog box are editable. Specify detection rule settings and configure the options on each page 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 box contains the following pages:

- "About the Detection rule: General information page" (702)
- "About the Detection logic: Affected platforms page" (702)
- "About the Detection logic: Affected products page" (703)
- "About the Detection logic: Files used for detection page" (703)
• "About the Detection logic: Registry settings used for detection page" (704)
• "About the Detection logic: Custom script page" (705)
• "About the Patch information page" (706)
• "About the Detecting the patch: Files used for installed patch detection page" (707)
• "About the Detecting the patch: Registry settings used for installed patch detection page" (707)
• "About the Patch install commands page" (707)
• "About the Patch uninstall commands page" (709)

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. 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 box 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk web 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 will fail. 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 configure a new registry key condition and its 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 dialog boxes 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 dialog boxes are similar to the properties dialog boxes 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 box 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 dialog boxes are similar to the detection logic dialog boxes 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 should check just 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 filename of the patch file required to remediate the selected definition if detected. This is the 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 an automatic patch download if a firewall is blocking 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.
  - **Unique filename:** Identifies the unique executable filename of the patch file.

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 box 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 filename, 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 filename 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 box where the button you want clicked is located).
• **ReplaceInFile**: Edits a text-based file on target devices. Use this command 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 to uninstall it from scanned devices.

For information on the commands, see "About the Patch install commands page" (707).
**Patch and Compliance tasks help**

*About the Create security scan task dialog box*

Use this dialog box to create and configure a scheduled task that runs the security scanner on target devices.

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**. A compliance scan checks target devices specifically for compliance with your security policy based on the contents of the Compliance group.

This dialog box contains the following options:

- **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.

*About the Change settings task dialog box*

Use this dialog box 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**: 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.
• **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. For more information, see “About the Configure scan and repair (and compliance) settings dialog box” (715).

• **Compliance settings:** Specifies compliance settings used for compliance scan tasks. Compliance settings determine when and how a compliance scan takes place, whether remediation occurs automatically, and/or what to do when Ivanti 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. For more information, see “Agent settings: Custom variables to override” (248).

**About the Create reboot task dialog box**

Use this dialog box 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.

**About the Create repair task dialog box**

Use this dialog box to create and configure a repair (remediation) task for the following definition types: vulnerabilities, spyware, Ivanti software updates, custom definitions, and security threats with an associated patch. The schedule repair option is not applicable to blocked applications.

This dialog box includes the following pages:
• "About the Create repair task: General page" (712)
• "About the Create repair task: Patches page" (712)

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) Creates two 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 box from within a device Security and Patch Information dialog box).

• **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 box" (713).

• **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.

About the Create repair task: Patches page

Use this page to show either required patches only or all associated patches for the selected vulnerability.
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 box**

Use this dialog box to configure the following Targeted Multicast options for a scheduled security repair task:

- **Multicast Domain Discovery:**
  - **Use multicast domain discovery:** Enables 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:** Enables 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:** Enables Targeted Multicast to do a domain discovery from the saved results of the last discovery.

- **Have domain representative wake up computers:** Enables devices that support Wake On LAN technology to turn on to receive the multicast.

- **Number of seconds to wait after Wake on LAN:** Sets 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 devices 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.

- **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 website 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 box would process no more than 20 devices at a time that failed the multicast. The Custom job dialog box 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 box won’t perform the distribution portion of the task for any device 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 device. 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 device 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.

**About the Uninstall patch dialog box**

Use this dialog box 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 box from within a device Security and Patch Information dialog box).

• **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 box" (713).

  • **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, and so on.
About the Gather historical information dialog box

Use this dialog box 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 box contains the following options:

- **Task name**: Identifies the 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 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 box

Use this dialog box to manage your scan and repair (and compliance) settings. Once configured, you can apply the settings to tasks for security and compliance scans, repairs, uninstalls, and reboots.

This dialog box contains the following options:

- **New**: Opens the settings dialog box where you can configure the options pertaining to the specified settings type.
- **Edit**: Opens the settings dialog box 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 delete a setting, devices with that setting will still have it and continue to use it until a new change settings task is deployed. Scheduled tasks and local scheduler tasks with that setting will still run on target devices.
devices until a new configuration is deployed.

- **Close**: Closes the dialog box without applying any settings to the task.

## Install or update security components help

### About the Install or update security components task dialog box

Use this dialog box to 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.

- **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, Ivanti Firewall, and Device Control.

- **Antivirus**: Specifies antivirus settings used for antivirus scan tasks. Antivirus settings determine whether the Ivanti 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. For more information, see "About the Ivanti Antivirus settings dialog box" (226).

- **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 custom variable override settings dialog box

Use this dialog box 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 variable override settings enable you to configure exceptions to custom variable values. Use them to ignore or bypass a specific custom variable condition so that a scanned device is not determined to be vulnerable.

This dialog box contains the following options:

- **New**: Opens the Custom variable override settings dialog box where you can configure the options.
- **Edit**: Opens the Custom variable override settings dialog box 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 delete the settings, devices with those settings will still have it and continue to use it until a new change settings task is deployed. Scheduled tasks and local scheduler tasks with those settings will still run on target devices until a new configuration is deployed.

- **Close**: Closes the dialog box, without applying any settings to the task.

You can view custom variable override settings information in the device's Inventory view.

About the Definition group settings dialog box

Use this dialog box to create, edit, and select settings that control how and where security definitions are downloaded based on their type and/or severity.

This dialog box 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 box**

Use this dialog box to define definition group settings. These settings control how and where security definitions are downloaded based on their type and/or severity.

This dialog box contains the following options:

• **Filter:** Defines which security content (definitions) will be placed in the group(s) 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 setting.

• **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 custom groups you’ve created, the Alert group, the Compliant group, and several of the available security industry groups.

**About the Alert settings dialog box**

Use this dialog box to configure security-related alerting for scanned devices, including both vulnerability and antivirus alerting.

The Alert settings dialog box 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 setting 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 setting 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 Core settings dialog box**

Use this dialog box 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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.

This dialog box contains the following options:

• **Scan results:**
  
  • **Keep scan results in vulscan results folder after processing:** Saves the security scan results files in the default vulscan folder.
  
  • **Decompress files if necessary:** Enables automatic decompression of scan results files if they are compressed.

• **Autofix retry count:**
  
  • **Attempt autofix times before giving up:** Specifies the number of times the core server will try to remediate via autofix before it times out.
  
  • **Attempt autofix indefinitely:** Indicates that the core server will try to remediate via autofix until it is successful or until you stop the process.

• **Rollup core:**
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: Enables 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 check box, or you can manually edit the field by clearing the check box and entering the URL you want.

About the Permissions dialog box
Use this dialog box to view the effective permissions for the Patch and Compliance tool for the currently logged-in administrator. These permissions settings are configured with the User Management tool. Also, an Ivanti Administrator can change role-based permissions required to edit and import custom vulnerability definitions.

IMPORTANT: ONLY an Ivanti Administrator can change role-based permission.

This dialog box contains the following options:

User:
  • View: Indicates the user has the ability to view patch security content.
  • Edit: Indicates the user has the ability to edit patch security content.
  • Deploy: Indicates the user has the ability to deploy patch security content.
  • Edit Public: Indicates the user has the ability to edit custom vulnerability content.

How to interpret role-based permissions:
  • Require Edit Public permission to edit custom definitions: Specifies that the Edit Public permission is required for a user to be able to edit custom vulnerability definitions.
  • Require Edit Public permission to import definitions: Specifies that the Edit Public permission is required for a user to be able to import security definitions.
Patch and Compliance toolbar help

About the Purge patch and compliance definitions dialog box

Use this dialog box to completely remove definitions (and their associated detection rules) from the core database.

IMPORTANT: Requires the Ivanti Administrator right
A user must have the Ivanti 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 box 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 box without saving changes and without removing definition information.

About the Security scan information view

Use this dialog box to view detailed patch deployment activity and status for scanned devices on your network.

You can view scan results for:

- Devices not recently reporting
- Devices with no results
- Devices needing patches by selected severity type
About the Threshold settings dialog box

Use this dialog box to define time periods for security scan (patch deployment) results that appear in the Security scan information dialog box.

- **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 box

Use this dialog box 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 filename 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 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, which is necessary to attempt to deploy and install the patch again.

**Managing security content**

When you install Endpoint Manager, the Patch and Compliance tool is included by default. However, without a Endpoint Security for Endpoint Manager content subscription, you can only scan for Ivanti software updates and custom definitions. A Endpoint Security for Endpoint Manager content subscription enables you to take full advantage of the Patch and Compliance tool by providing access to additional security content.

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content types include:

• Antivirus updates: For third-party scanners, includes antivirus scanner detection content only. For Ivanti Antivirus, includes both scanner detection content AND virus definition files.

• Blocked applications (see the "Legal disclaimer for the blocked applications type" (734))

• Custom vulnerability definitions

• Driver updates

• Ivanti software updates

• Security threats (system configuration exposures, including firewall detection and configuration)

• Software updates

• Spyware

• Vulnerabilities
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 the different types of detected security risks on managed devices, see the appropriate sections in "How Patch and Compliance scans and remediates" (681).

For information about Endpoint Security for Endpoint Manager content subscriptions, contact your Ivanti reseller, or visit the Ivanti website.

For other questions, the Ivanti User Community has user forums and best known methods for all Ivanti products.

**Related topics**

"Download security content" below
"View and organize security content" (728)
"Search for vulnerabilities by CVE name" on page 730
"Customize item lists with filters" on page 732
"Purge security content definitions" on page 732
"Uninstall patches (patch rollback)" on page 733

**Download security content**

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 Ivanti-hosted database. Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk services consolidate known definitions and patches from trusted, industry sources and sends reliable information directly to you.

Use the Download updates dialog box to configure and perform security content updates at once or to create a scheduled task. Download the definitions and patches separately, or using the same task. For example, you may want to download definitions and run a scan at least once before downloading patches, and then only download the patches for vulnerabilities that were detected during the scan.

---

**CAUTION:** Only one Ivanti 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.

---

Before you can deploy security patches to affected devices, you must first download the patch executable file to a local patch repository on your network.

**To download security content**

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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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 are language-independent, meaning they are compatible with any language version of the OS or application. In other words, you don't need a unique language-specific patch to remediate those vulnerabilities because the patch covers all supported languages.

When downloading content for any platform, 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 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 to be placed automatically in the Unassigned group instead of the default Scan group, select the Put new definitions in the Unassigned group check box.

7. If you want to automatically download associated patch executable files, select 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 box.)

   - For detected definitions only: Downloads only the patches associated with vulnerabilities, security threats, or Ivanti 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 Ivanti updates currently residing in the Scan group.

8. If you have a proxy server on your network that is used for external Internet access, 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. To download the content now, click Update Now. The Updating Definitions dialog box displays the current operation and status. If you click Cancel or close the console before the update is finished, only the security content that has been processed to that point is downloaded to the core database.
To create a scheduled task, click **Schedule Update.** The **Scheduled update information** dialog box 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.

**IMPORTANT: 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 box 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 global settings, they are effective for all security content download tasks from that point on.
To download patches from a downloaded definition

Use this option if you have already downloaded definitions but want to selectively download patches.

1. Right-click the definition, and then click **Download associated patches.**
2. Select whether to download all associated patches or only current patches. If you choose all associated patches, this includes patches that have been superseded.
3. Click **Download.**

**NOTE:** You can also download patches from a definition's properties dialog box. On the General page, click **Properties > Patch Information > Download.**

For more information on patch file download status, see “Open and understand the Patch and Compliance tool” (683).

To configure the patch download location

1. On the **Download updates** dialog box, 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 URL where devices can access the downloaded patches for deployment. This URL should match the UNC path above.
5. You can click **Test Settings** to check if a connection can be made to the web address specified above.
6. If you want to restore the UNC path and URL to their default locations, click **Restore to Default.** Again, the default storage location is the core server's \LDLogon\Patch directory.

View and organize security content

After security content has been updated, 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.
Once security content has been downloaded, you can move items into different status groups, or copy them into your own custom groups.

You can also view property details for each of the updated definitions and detection rules by right-clicking an item and selecting **Properties**. Use this information to 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.

### Using tags and groups

Groups and tags enable you to organize content. Use groups to perform actions based on group membership. Use tags for filtering a view or creating a query, but not for defining the target for actions.

For information on how to use the different groups, see “Open and understand the Patch and Compliance tool” (683).

### View patch content for specific devices

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 box lets you view detection, installation, and repair history, and perform patch management tasks.
Search for vulnerabilities by CVE name

Patch and Compliance supports the Common Vulnerabilities and Exposures (CVE) naming standard. You can search for a downloaded vulnerability by its CVE name. You can also view the CVE names associated with an individual vulnerability.

What is CVE?

Common Vulnerabilities and Exposures (CVE) is a collaborative initiative by several leading security technology organizations. They maintain a list of standardized names for vulnerabilities and other information security exposures. The CVE naming standard makes it easier to search for, access, and share data across vulnerability databases and security tools.

Ivanti compatibility with the CVE naming standard

Ivanti products—including Endpoint Manager, Endpoint Security for Endpoint Manager, and Patch Manager—fully support the CVE standard.

When you download vulnerability definition updates, they include CVE names. Additionally, the vulnerability definition includes a hyperlink to the CVE dictionary web site where you can find the most recent CVE version information.
Search for vulnerabilities by their CVE name

Patch and Compliance lets you search for vulnerabilities by their CVE names or view the CVE details for a specific vulnerability.

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.

2. Enter the CVE name (CVE ID) in the **Find** field, select **Any** or **CVE ID** from the **In Column** 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** 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 box.

3. Click the **Description** page.

4. If the selected vulnerability has a CVE name, it displays in the **CVE ID** list. Some vulnerabilities might have more than one CVE name, which you can access by scrolling through the 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).

**Customize item lists with filters**

The **Filter** list enables 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.

You can use the **Filter** control 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, select the **Operating System** check box, and then select the operating systems you want to display.
5. If you want to filter by the severity of the definition, select the **Severity** 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.

**Purge security content definitions**

You can purge unused definitions from the Patch and Compliance tool window and the core database if you determine that they aren’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.

Only users with Ivanti administrator rights can purge content.

**To purge unused definitions**

1. Click **Tools > Security > Patch and Compliance**.
2. Click the **Purge patch and compliance definitions** toolbar button.
3. Select the platforms whose definitions you want to remove. You can select one or more platforms in the list.

4. Select the languages whose definition you want to remove (associated with the platform selected above). If you select a Windows or Macintosh platform, you should specify the languages whose definition you want to remove. If you select a UNIX or Linux platform, you must select the **Language neutral** option in order to remove their language independent definitions.

5. Select the types of definitions that you want to remove.

6. Click **Purge**.

### Uninstall patches (patch rollback)

You can uninstall (i.e., roll back) 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 roll back a patch**

1. View the properties for the definition associated with the patch. Right-click the definition and click **Properties**.

2. In the Detection Rules list, right-click one or more rules and then click **Uninstall**.

3. Enter a name for the uninstall task.

4. Specify whether the uninstall is a scheduled task, a policy-based scan, or both.

5. If you selected scheduled task, specify the devices from which you want to uninstall the patch.

6. If the patch can’t be uninstalled without accessing its original executable file (i.e., using command-line parameters), and you want to deploy the executable using Targeted Multicast, select the **Use multicast** check box. To configure Multicast options, click the **Multicast Options** button. For more information, see "About the Multicast options dialog box" (713).

7. 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.

8. Select scan and repair settings from the available list (or create custom settings for this scan), to determine how the scanner operates on end-user devices.

9. 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 box. You can also clear the patch install status by vulnerability.

**Remove 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.

**Legal disclaimer for the blocked applications type**

IMPORTANT: As a convenience to its end users, Ivanti 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk. 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, Ivanti 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."

**Scanning devices for vulnerabilities**

In order to scan for vulnerabilities, the device must have the agent with the vulnerability scanner installed. Before you scan, make sure you have configured the Distribution and Patch agent settings for to the devices. For more information about the Patch agent settings, see "Configure devices for security scanning and remediation" (689).

After you’ve downloaded definitions, make sure that the agents are configured with correct scan settings and then create a scheduled task to scan for the vulnerabilities.

**Related topics**

"Configuring what to scan for" (735)
"Create a patch and compliance scan task" (736)
"Use custom variables and custom variable override settings" on page 737
"View detected vulnerabilities" (738)
"Secure Content Automation Protocol (SCAP)" on page 740
"Forward security scan results to a rollup core" on page 744

**Configuring what to scan for**

There are two primary factors that affect which definitions are scanned for:

- The group the definition is in.
- The agent settings.

**Vulnerability groups**

When you download new definitions, they are automatically added to the Scan group. (The only exception is blocked application definitions—they're added to the Unassigned group.) When a security scan task runs, it scans for the definitions in the Scan group.

The Scan group has several sub-groups to help you organize the definitions that are scanned for. Some of these sub-groups, like the Detected group, are automatically populated when a vulnerability is detected. Other groups like the Autofix (global) group are populated when you move definitions into them.

For more information about the default groups for vulnerabilities, see "Open and understand the Patch and Compliance tool" (683).

---

**CAUTION: Moving definitions from the Scan group**

When you move definitions from the Scan to the Don’t Scan group, the information about which devices detected those definitions is removed from the core database and is no longer available in either the definition Properties dialog boxes or in the device Security and Patch Information dialog boxes.

---

**Agent settings**

When you create Distribution and Patch agent settings, the Scan options page allows you to configure the type of definitions to scan for. By default, the agent setting is configured to scan for vulnerabilities, Ivanti updates, and custom definitions.

For more information about the agent settings, see "Agent settings: Distribution and patch" on page 251.

After you have downloaded security definitions and configured what to scan for, create a scan task. For more information, see "Create a patch and compliance scan task" on the next page.
Create a patch and compliance scan task

The security scanner is generally run as a scheduled task from the core server. The scheduled task can be a push, policy, or policy-supported push task.

For testing or specific needs, you can also run the security scanner immediately from the console or from the device that needs to be scanned.

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 box displays.

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 one of the scan and repair settings from the available list (or create 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.

**NOTE: 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 Ivanti Antivirus when a virus is detected that can’t be removed or quarantined.

To run an on-demand scan from the console

1. Right-click the selected device (or up to 20 multi-selected devices) and click Patch and compliance scan now.
2. Select a scan and repair setting, choose the type of scan, and then click OK. The scan runs immediately.

Use custom variables and custom variable override settings

With custom variables, you can fine-tune security threat scanning by modifying one or more settings’ values so that the scanner checks for conditions you define. The scanner then determines a device to be vulnerable only if that condition is met, meaning that the value you specified 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.

IMPORTANT: Edit Custom Variables right required

To edit custom variable settings, a Ivanti 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 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 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).
NOTE: Custom variable override settings
In some situations, you may want the scanner to ignore custom variable settings by using a feature called Custom variable override settings. You can specify that the scanner ignore certain custom variables when scanning devices so that the variables aren’t detected as vulnerable and aren’t remediated, even if they meet the actual conditions of a definition’s detection rules. A user must have the Edit Custom Variables right to create or edit these override settings. You can create as many settings as you like, and apply them to devices using a Change settings task. For more information, see "Agent settings: Custom variables to override" (248).

View detected vulnerabilities
If the security scanner discovers any of the selected definitions on target devices, this information is reported to the core server. To delete the latest scan results from the core for a device, use the instructions below for viewing vulnerabilities by device and then click Clear scan/repair status.

Use one of the following methods to view detected vulnerabilities after running a scan:

**By the Detected group**
In the Patch and Compliance tool window, select the Scan > Detected folder 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.

You can also view compliance information by group after a Compliance scan by selecting the group and clicking the Computers out of compliance button on the toolbar.

**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 a device**
Right-click a specific device in the network view, and then click Security and Patch Information to view the results of the latest scan and the patch deployment status for the device.
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 box**

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 devices not recently reporting, devices with no results, and devices needing patches by selected severity type.
By a chart or dashboard

You can use the dashboard editor to customize the charts displayed on the main Patch and Compliance page or in the dashboard. Some of the charts available by default show detected definitions by severity, the definitions that have been detected most often, and successfully installed patches.

NOTE: For more information on the Dashboard, see Dashboard editor.

By the security scan log file

The security scanner writes a log file for the most recent scan on the device called vulscan.log. These log files record useful information about the time of the scan, language, platform, and the processes run by the scan.

Secure Content Automation Protocol (SCAP)

The Secure Content Automation Protocol (SCAP) was developed by the U.S. government’s NIST organization to create a security-oriented operating system configuration checklist. For more information, see http://web.nvd.nist.gov/view/ncp/repository.
Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk can import SCAP data from many sources, including NIST, and then use that data to scan managed devices.

This SCAP support is licensed separately. Contact Ivanti sales for details.

**Importing SCAP checklists**

SCAP checklists consist of XML files stored within a ZIP or CAB file. You can download SCAP-validated checklist policies from [http://web.nvd.nist.gov/view/ncp/repository](http://web.nvd.nist.gov/view/ncp/repository). When you import a SCAP checklist, the SCAP filename becomes the vulnerability group name in Patch Manager. Each SCAP checklist ZIP or CAB should contain these files:

- *
  - cpe-dictionary.xml
- *
  - cpe-oval.xml
- *
  - oval.xml
- *
  - xccdf.xml

When importing SCAP checklists for the first time, make sure you’ve selected the **Download SCAP scanner** check box. You only need to do this once. The core server will reuse that scanner for other checklist scans.
To import SCAP data

1. Click **Tools > Security and compliance > Patch and compliance**.
2. Select **Download SCAP scanner** if this option hasn’t been selected by someone doing an earlier import. If you aren’t sure, you can go ahead and select this option.
3. Click the **Import SCAP content** toolbar button.
4. Browse for the SCAP data package ZIP or CAB file and select the platform the SCAP data package supports. There's no error checking for platform support, so make sure you select the right platform(s).

5. A successful import shows a green progress bar. A red progress bar indicates there was an error. You can view a log file from your most recent import here: %AppData%\Local\LANDesk\SCAPContent.log.

6. Once the import finishes, close the SCAP content import dialog box and in the tree, click Patch and compliance > Groups > Predefined groups > Security Content Automation Protocol. You will see a group that matches the filename you imported.

**Scanning clients for SCAP vulnerabilities**

When you import SCAP checklist data, the console creates a group for each checklist and adds these three items to that group:

- 1 Install SCAP scanner, benchmark files, and scan
- 2 View results
- 3 Overall score

The numbers that appear before each vulnerability indicate the order in which to execute them.

The **1 Install SCAP scanner, benchmark files, and scan group** vulnerability contains three items:

- **Install SCAP scanner**: Installs the SCAP scanner on the client.
- **Install <SCAP benchmark name> benchmark**: Installs the SCAP data source XML files on the client.
- **Scan for <SCAP benchmark name> compliance**: Runs the SCAP scanner and generates the SCAP results for the client, including scanning all the SCAP content definitions included in the View results group.

When you scan clients for SCAP checklist vulnerabilities, the SCAP scanner and relevant SCAP checklist data are copied to the client. The scanner runs, checking each SCAP vulnerability and logging the results to results.xml. Vulscan parses the results.xml file and reports vulnerability data back to the core server. The information is stored in inventory as vulnerability data.

You can run all three **1 Install SCAP scanner, benchmark files, and scan group** steps at once by right-clicking that tree item in the left window pane and clicking Repair. If you've already run all three steps, and you're rechecking to see if the vulnerability is fixed, you can directly run the SCAP scan step in the vulnerability check by selecting **1 Install SCAP scanner, benchmark files, and scan group**, and in the right pane right-clicking the scan step and clicking Repair. You can do this because the SCAP scanner and SCAP vulnerability checklist were installed by the original SCAP task for that vulnerability checklist.
To scan clients for SCAP vulnerabilities
1. Click Tools > Security and compliance > Patch and compliance.
2. In the Patch and compliance tree, click Groups > Predefined groups > Security Content Automation Protocol and the imported SCAP checklist you want.
3. Under the SCAP checklist, right-click Install SCAP scanner, benchmark files, and scan group and click Repair.
4. Modify the task name if you want to and select Repair as a scheduled task. Click OK.
5. In the Scheduled tasks window, add targets to the task and run it.

Viewing SCAP vulnerability results
When the Install SCAP scanner, benchmark files, and scan task finishes running on managed devices, you can view the SCAP vulnerability data, which has two parts—the individual vulnerability results and the overall score.

To view SCAP vulnerability results
1. Run the Install SCAP scanner, benchmark files, and scan task on managed devices.
2. Click Tools > Security and compliance > Patch and compliance.
3. In the Patch and compliance tree, click Patch and compliance > Groups > Predefined groups > Security Content Automation Protocol, the imported SCAP vulnerability group that you want, and then click either View results or Overall score.
4. Filter the results by using the filter tools at the top of the results pane.

You can also check device results individually by right-clicking a device in the network view, clicking Inventory, and expanding the Detected Patch and Compliance Definitions tree item.

Forward 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. Doing so can facilitate access to real-time vulnerability information for all of your managed devices. You can enable automatic forwarding of security scan results 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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 Core settings.
2. Enable the Send scan results to rollup core immediately check box.
3. If you want to use the default URL location on the rollup core where the scan results file is written, select the Use default rollup URL check box. Otherwise, provide the URL for the destination rollup core.

Patching devices with vulnerabilities

After you have performed a scan and know what vulnerabilities exist in your environment, use a repair task to patch devices. A repair task can be a push, a policy, or a policy-supported push.

Patch and Compliance only installs the patches for detected vulnerabilities on each device. If the vulnerability is not detected, the patch is not installed even if it is included in the repair task.

Generally, vulnerabilities, custom definitions, Ivanti software updates, and blocked applications are remediated from the console using a repair task. To remediate at the time of discovery instead of using a separate repair task, use the Autofix feature.

For information about what happens on a device during patching, see "What happens on a device during remediation" on page 748.

To create a repair task

2. To remediate one definition at a time, right-click the definition and then click Repair.
   -Or-
   To remediate a set of definitions together, create a group that contains the definitions, right-click the group and click Repair. You can also select the definitions and click Create a task > Repair.
3. Configure the task type, targets, start time, and other task options. For information about the general scheduled task options, see "Schedule a task" on page 415.

4. To view or edit which definitions are included in the task, click Definitions.
   
   • To remove a definition from the task, right-click it and select Delete.
   
   • If definitions in the list have prerequisites, meaning that other patches must be installed first, you can add the prerequisite definitions to the task by clicking Add prerequisites.
• If definitions in the list have dependents, meaning that the patches currently in the task must be installed before other patches can be installed, you can add the dependent definitions to the task by clicking **Add dependents**.

5. To view or download the patches associated with the task, click **Patch list**. To change a patch so that it uses multicast, select the patch and click the **Multicast** button. Remove multicast by selecting the patch and clicking **Don’t multicast**.

6. Click **Save**.

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 Autofix**

Autofix enables you to remediate during the detection scan, when the vulnerability is detected. There is no need to create a separate task for remediation. If a patch requires a reboot, the target device always automatically reboots. By default, if the agent attempts to autofix a patch but it fails, the agent does not retry.

Autofix is generally used after a patch has been thoroughly tested and the administrator is confident that it won’t negatively affect users. The feature is available for vulnerabilities, spyware, Ivanti software updates, and custom definitions.

Autofix has to be enabled in agent settings, and then configured for each definition. When you create a task for downloading definitions, you can use a filter to enable Autofix when a definition is downloaded.

**IMPORTANT: Requirements for using Autofix**

Only Administrators or users with the Patch Manager **right and** the default All Devices scope can enable the Autofix feature.

The Windows agent, Windows Server agent, and Windows Embedded Standard agent all have an option in agent configuration that overrides what is in the agent settings. By default, Windows Server agents are set to **Never autofix**. If autofix isn’t working when you expect it to, investigate whether the **Never autofix** option is enabled in Agent Configuration > Standard Ivanti agent.

**To enable Autofix in the agent settings**

1. Click **Tools > Configuration > Agent settings**.
2. Select an existing Distribution and Patch agent setting or right-click **Distribution and Patch** in the tree and select **New**.
3. Select **Patch-only settings > Scan options**.
4. Enable the **Enable autofix** option at the bottom of the page.
5. Save your changes.
To enable Autofix for a definition

2. Drag a downloaded definition to one of the Scan > Autofix folders in the tree view, or right-click and select Autofix.

To automatically enable Autofix for definitions when they are downloaded

2. In the toolbar, click Download updates.
3. Select the definitions that you want to use autofix for.
4. Click the Definition download settings button (on the Updates tab).
5. In the Definition download settings dialog, click New.
6. In the Definition filter properties dialog, click the Autofix tab.
7. Enable the Assign Autofix option.
8. Configure the other download settings and save your changes.

To configure the number of retries for Autofix

2. In the toolbar, click Configure settings > Core settings.
3. In the Autofix retry count section, specify the number of times to attempt an Autofix, or allow the agent to retry indefinitely.
4. Click OK.

What happens on a device during remediation

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 remediate.

Almost all patch files install silently, requiring no user interaction at the end-user device itself. Some non-English patches do not install silently. You can tell whether a patch installs silently or not by checking the Silent Install column in the definition details.

However, whether a patch file can install silently or not, you can 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.

If a patch file installation requires a reboot and the settings for the task allow a reboot, Patch and Compliance first installs all of the patches for the task on the device, and then reboots the device once.

Other patch and compliance tasks

See the following topics for more information about patch and compliance reports and alerts.
• "View patch and compliance information for scanned devices" (756)
• "Using file reputation to restrict applications" (757)
• "Create a scheduled reboot task" (761)
• "Use the security scanner command line" (761)
• "Configure Patch and Compliance alerts" (765)
• "Generate Patch and Compliance reports" (766)

Custom security definitions overview

In addition to the known vulnerabilities that you can update via the Patch and Compliance tool, you can further ensure successful remediation by creating custom, user-defined definitions—complete with custom detection rules, associated patch files, and special additional commands.

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 to detect a vulnerability (or practically any system condition or status) on scanned devices.

You can use custom vulnerability definitions to implement an additional, proprietary level of patch security on your Ivanti system. In addition to enhancing patch security, custom vulnerability definitions can assess system configurations, check for specific file and registry settings, and deploy application updates to take advantage of the scanning capabilities of the vulnerability scanner.

NOTE: 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. Click the New Blocked Application button in the toolbar. Enter an executable filename and a descriptive title for the definition, and then click OK.

Custom definitions don't necessarily have to perform the remediation actions of 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 targeted 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 items such as the following:

• Application existence
• File existence
• File version
• File location
• File date
• Registry setting

For information about creating or importing and exporting security definitions, see the following sections:

• "Create custom security definitions" below
• "Import and export custom definitions" on page 755

Create custom security definitions

If you no longer need a custom definition, you can delete it. Deleting a custom definition removes its information and associated detection rules from both the core database and 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, and then click the Delete selected custom definitions button in the toolbar.

To create custom definitions

2. From the Type 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 box opens, allowing you to configure vulnerability settings.
4. Enter a unique ID and Title for the vulnerability. (The system-generated ID code can be edited.)

5. The Type is a Custom Definition and can't be modified.

6. Specify a Publish date.

7. Enter a descriptive title for the vulnerability. This title displays in vulnerability lists.

8. Specify the Published severity level. Available options include: Unknown, Service Pack, Critical, High, Medium, Low, and Not Applicable. You can also override the published severity level if your risk assessment is different.

9. Specify the Status for the vulnerability. When you specify a status, the vulnerability is placed in the corresponding group in the tree view (see “All items (definitions in the tree view)” (686)).

10. The language settings for user-defined vulnerabilities are 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’re creating a new custom vulnerability, 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 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.

13. If you want to include prerequisites for this custom vulnerability definition (and see any other definitions that are dependent on this vulnerability), click Dependencies and configure the prerequisite definitions.

14. If you want to create or edit your own custom variables for this custom vulnerability definition, click the Custom Variables tab and configure the custom variables.

15. When you’re done specifying attributes for the custom vulnerability, click OK.

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.

You can do the same things with a custom vulnerability definition 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 Autofix, create a repair job, or clear scan/repair status. To choose an option, right-click a custom vulnerability definition to access its shortcut menu.

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 box opens at the dialog box's General Information page, allowing you to configure a detection rule.
3. At the **Rule general information** page, enter a unique name for the rule. The rule’s status can’t 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 can’t be modified here either. However, you can enter any information you want in the Comments box.

4. Use the various pages of the rule properties dialog box 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 **Configure** to open the **Selected affected products** dialog box where you can add and remove products in the **Affected products** list (this list can be shortened if you like, by selecting the check box at the bottom of the dialog box). The list of available products is determined by the content you’ve updated. You don’t 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 **Query filter** page, you can optionally specify a query that includes only the devices that you want the custom detection rule to return results for.
9. 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” (703).

10. 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” (704).

11. At the **Custom script** page, you can create a custom Virtual Basic script to assist with detection for this detection rule. A script can access the security scanner’s following runtime properties to report results: Detected, Reason, Expected, and Found.

   **NOTE:** Use the **Use editor** button to open your default script editing tool associated with this file type. Upon closing the tool, you’ll be prompted to save changes in the Custom Script page. If you want to use a different tool, change the file type association.

12. At the **Patch information** page, specify whether the vulnerability associated with this detection rule can be repaired or just detected on your managed devices. If you select the repair option, the **Patch download information** and **Repair information** fields become editable.

13. 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.)

14. 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 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” (702).)

15. For a rule that allows remediation, you can configure additional commands that are run during the remediation process on affected devices. To configure additional 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. 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” (707).

**To create a blocked application definition**

1. Click **Tools > Security > Patch and Compliance**.
2. From the **Type** list, select **Blocked applications**.
3. Click the **Create custom definition** toolbar button. An editable version of the properties dialog box opens, allowing you to configure the settings.

4. Provide the **Filename** for the application that you’re blocking. The security scanner will check the file header, so even if the filename has been changed on the managed device, the application is blocked.

5. Type a **Title** and **Summary** information for the definition. These are for your convenience in organizing the definitions.

6. To put the definition in a **Category**, select an existing category from the drop-down list or type a new category in the field.

7. If desired, specify a specific version or range of versions of the application that you want to block. This option is only available for devices using a Windows operating system. It is disregarded when the definition is applied on a Mac.

8. Select the **Affected platforms** to limit the number of devices scanning for the definition.

9. Click the **Block status** tab to set the status for the definition. By default, the definition is **Block (global)**.

**NOTE:** To change the status after the definition has been created, drag the definition from the current folder to the new folder in the Blocked applications tree.

10. Click **OK**.

**Import and export custom definitions**

The Patch and Compliance tool provides a way for you to import and export custom definitions and their detection rules. 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.

Custom definitions are exported and imported as XML-formatted files. You can’t import and export known industry vulnerability definitions.

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.

**NOTE:** **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.

**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. Click Save.

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 to confirm whether you want to overwrite it. Check the status window to see whether the definition is successfully imported.

View patch and compliance information for scanned devices
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 or 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.

View 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.

Verify 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 **Clean/Repair History** object in the left-hand pane.

The **Succeeded** field indicates whether the installation was successful. Possible states include: Succeeded, Failed, and Failed to Download.

**Clear 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 box. 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 with the **Clear scan/repair status** dialog box. 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 box to remove vulnerability scan information from the database for one or more vulnerabilities.

**To clear vulnerability scan and repair status**

1. Right-click the vulnerability, and then select **Clear scan/repair status**.
2. Select the desired options.
3. Click **Clear**.

**Using file reputation to restrict applications**

The file reputation feature in security and compliance helps ensure that the files on a device’s file system aren’t malware and that no one has tampered with them. While application control behavior protection can help secure managed devices, false positives can still trigger on legitimate applications, depending on what those applications are trying to do. If you use file reputation, you have the option of creating a separate application control behavior profile for files with a known “good” reputation that bypasses the normal behavior-based application control.

File reputation isn’t enabled by default. If you enable file reputation, anonymous file reputation information from files on managed devices will be securely sent to the Ivanti file reputation cloud server, which improves file reputation accuracy and coverage for all users of this feature.

If you enable file reputation, each time the device executes an application, the agent first checks a local database to see if the application files match known good hashes. If there isn’t a match, the agent sends a request with data about the files to the core server. The core server checks its database to see if information about that file’s reputation already exists. If it doesn’t exist, the core sends a request to the Ivanti cloud reputation server. If the file hashes match results in the cloud, the cloud server returns reputation information about the files to the core and client.
The file reputation system uses a Ivanti cloud-hosted database of file information, including names, sizes, metadata, and SHA1 hashes. Much of the file reputation database is from the National Software Reference Library (NSRL). You can visit their web site for more information: http://www.nsrl.nist.gov/new.html.

A file can have one of these three reputations:

- **Good**: The file matches an entry in the NSRL database or Ivanti has gathered enough information to believe that the file is safe.
- **Bad**: The file doesn’t match any NSRL database entries or Ivanti has gathered enough information to believe that the file isn’t safe.
- **Undecided**: There aren’t any matches on this file or there aren’t enough matches to help decide whether the file is good or bad.

Among other factors, the file reputation algorithm considers how often matching files occur, how old the matches are, who signed the files, and how often those occurrences are whitelisted or blocked in Endpoint Manager.

To use file reputation monitoring on managed devices, you need to complete the following steps:

1. Download the file reputation Ivanti updates
2. Create an application control agent setting that uses file reputation
   - Or-
   Include the reputation definitions as part of the application file list
3. Deploy the setting to managed devices

**To download file reputation Ivanti updates**

1. Click Tools > Security and compliance > Patch and compliance.
2. Click the Download updates toolbar button.
3. In the Definition types list, click Ivanti File Reputation Updates.
4. In the confirmation dialog box, read the terms of use for file reputation. If you agree to the terms, click I agree. Clicking I disagree will clear the Ivanti File Reputation Updates check box.
5. Click the Download now or Apply button.

**To use file reputation with Application Control**

1. Click Tools > Security and compliance > Agent settings.
2. In the tree under Agent settings > My agent settings > Security > Endpoint Security, right-click Application control and click New, or double-click an existing setting.
3. On the General settings page, select Treat "good reputation" files as if they are in the associated trusted files list.
4. Click the "Good reputation" application behavior button.
5. Configure the **Application control** and **Ivanti firewall** behaviors that you want for files with a good reputation.

6. Click **OK** and then click **Save**.

**To use file reputation with an Application File List**

1. Click **Tools > Security and compliance > Agent settings**.
2. In the tree under **Agent settings > My agent settings > Security > Endpoint Security**, right-click **Application file lists** and click **New**, or double-click an existing list.
3. Enable the options at the top of the dialog box to **Automatically include "good reputation" files when sending list to clients** or **Automatically include "bad reputation" files when sending list to clients**.
4. If you include good reputation files, click the **Allowed application behavior** button to configure the **Application control** and **Ivanti firewall** behaviors that you want for files with a good reputation.
5. Click **OK**.

**To add files to an application file list**

1. Click **Tools > Security and compliance > Agent settings**.
2. Click the **Configure settings** toolbar button, and click **File reputations**.
3. Double-click the application file list you want to modify or create a new one.
4. On the **Application file list** toolbar, click and click **Add file by browsing** or **Add block file by inputting name**.
5. Depending on the option you chose, browse for the file you want and click **Save**, or enter the file details manually and click **OK**.

**To deploy file reputation agent settings to managed devices**

1. In the **Agent settings** window, click the **Create a task** toolbar button and click **Change settings**.
2. Depending on your preference, select a scheduled task or policy for the settings change task type.
3. Next to **Endpoint security** in the settings list, select the endpoint security setting that uses the application control setting you configured.
4. Click **OK** and finish configuring the task in the **Scheduled tasks** window.

**To override existing file reputations**

1. Click **Tools > Security and compliance > Agent settings**.
2. Click the **Configure settings** toolbar button, and click **File reputations**. To sort the list of files, use the checkboxes at the top of the page and click **Apply filter**.
3. Select the files whose reputations you want to change and click the **Override reputation** button.
4. Make sure that **Override Ivanti reputation setting** is checked, and select the **Desired reputation**.
5. Click **OK**.

**To import from other application file lists**

1. Click **Tools > Security and compliance > Agent settings**.
2. In the tree under **Agent settings > My agent settings > Security > Endpoint Security**, right-click **Application file lists** and click **New**, or double-click an existing list.
3. On the **Application file list** toolbar, click ![Import from other application file lists](image) and click **Import from other application file lists**.
4. Apply filters if necessary and select the files you want to import. Click **Next**.
5. Configure the application behaviors you want for the files you selected and click **OK**.
6. Click **OK** again to save your changes to the application file list.

**To import file lists from a .csv file**

1. Click **Tools > Security and compliance > Agent settings**.
2. In the tree under **Agent settings > My agent settings > Security > Endpoint Security**, right-click **Application file lists** and click **New**, or double-click an existing list.
3. On the **Application file list** toolbar, click ![Import from .csv file](image) and click **Import from .csv file**.
4. Browse for the .csv file containing the application file list information and click **Open**.
5. Configure the imported files if necessary and click **OK**.

Note: The .csv file format is as follows: "File name", "File size", "Version", "Manufacturer name", "Product name", "MD5 hash base64 string", "SHA1 string", "SHA256 string", "Permissions"

**To import file lists from trusted devices**

1. Click **Tools > Security and compliance > Agent settings**.
2. In the tree under **Agent settings > My agent settings > Security > Endpoint Security**, right-click **Application file lists** and click **New**, or double-click an existing list.
3. On the **Application file list** toolbar, click ![Import from trusted devices](image) and click **Import from trusted devices**.
4. Select the devices you want and click **Import files from specified devices**.
5. If you want to do an exhaustive scan for .exe files from those devices, click **Yes**.
6. Configure the imported files if necessary and click **OK**.

**To merge application file lists**

1. Click **Tools > Security and compliance > Agent settings**.
2. In the tree under Agent settings > My agent settings > Security > Endpoint Security, right-click Application file lists and click Merge application files.
3. Select the application file list that you want to be the Source list.
4. Select whether you want to merge differences or replace application files.
5. Select the target lists for the merge operation.
6. Click OK.

Create a scheduled reboot task

Patch and Compliance provides a tool that enables you to 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

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 setting from the available list (or create a custom setting just for this scan task) to specify 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) or dynamic targets (query results) and configure the policy’s type and frequency.

Use the security scanner command line

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk includes 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 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" (679) and "Patch and Compliance help" (691).

This section provides supplemental information about using the Patch and Compliance security scanner.
Security scanner command-line parameters

The security scanner is called vulscan.exe. The scanner supports the following command-line parameters:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General parameters</strong></td>
<td></td>
</tr>
<tr>
<td>/AgentBehavior=ScanRepairSettingsID</td>
<td>Overwrites the default behavior of the security scanner (scan and repair settings) for only the current scan job. The ScanRepairSettings ID is a number value.</td>
</tr>
<tr>
<td>/ChangeBehaviors</td>
<td>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. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>/ShowUI</td>
<td>Shows the scanner UI on the end-user device.</td>
</tr>
<tr>
<td>/AllowUserCancelScan</td>
<td>Shows a Cancel button on the scanner UI that lets the end user cancel the scan.</td>
</tr>
<tr>
<td>/AutoCloseTimeout=Number</td>
<td>Timeout value in seconds. <strong>NOTE:</strong> If the value is set to -1, then the scanner UI waits for the end user to manually close it.</td>
</tr>
<tr>
<td>/Scan=Number Code (0-8)</td>
<td>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 - Ivanti updates 4 - custom definition 5 - blocked application 6 - software updates 7 - driver updates 8 - antivirus 100 - all types</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>/Group=GroupID</td>
<td>Specifies the custom group that should be scanned. Find the custom group ID by selecting the group, right-clicking and selecting <strong>Info</strong>, and finding the <strong>Unique ID</strong>.</td>
</tr>
<tr>
<td>/AutoFix=True or False</td>
<td>Enables or disables the autofix feature.</td>
</tr>
</tbody>
</table>

**Repair parameters**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Repair (Group=GroupID, or Vulnerability=VulnerabilityID, or Vulnerability=All)</td>
<td>Tells the scanner which group or vulnerability to repair (remediate). You can specify All to repair all detected vulnerabilities instead of a single vulnerability by its ID.</td>
</tr>
<tr>
<td>/RemovePatch=PatchName</td>
<td>Removes the specified patch from the patch repository.</td>
</tr>
<tr>
<td>/RepairPrompt=MessageText</td>
<td>Lets you display a text message that prompts the end user.</td>
</tr>
<tr>
<td>/AllowUserCancelRepair</td>
<td>A string that allows the end user to cancel repair if using a repair prompt.</td>
</tr>
<tr>
<td>/AutoRepairTimeout=Number</td>
<td>A timeout value for the repair prompt in seconds. If it's set to -1, then the prompt waits for the end user to close it manually.</td>
</tr>
<tr>
<td>/DefaultRepairTimeoutAction</td>
<td>A string for the default action for vulscan to take if timeout expires for repair prompt. Acceptable values include start and close.</td>
</tr>
<tr>
<td>/StageOnly</td>
<td>A string to retrieve the patch or patches needed for repair, without installing them.</td>
</tr>
<tr>
<td>/Local (get files from peer)</td>
<td>Forces peer only download.</td>
</tr>
<tr>
<td>/PeerDownload</td>
<td>Same as /local.</td>
</tr>
<tr>
<td>/SadBandwidth=Number</td>
<td>Maximum percentage of bandwidth to use when downloading.</td>
</tr>
</tbody>
</table>

**Reboot parameters**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/RebootIfNeeded</td>
<td>Use this parameter to reboot a device if needed.</td>
</tr>
<tr>
<td>/RebootAction</td>
<td>A string that determines vulscan's reboot behavior when repairing. Possible values: always, never</td>
</tr>
<tr>
<td>/RebootMessage</td>
<td>A string that displays a text message to the end user in a reboot prompt.</td>
</tr>
<tr>
<td>/AllowUserCancelReboot</td>
<td>A string that allows the end user to cancel reboot if using a reboot prompt.</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/AutoRebootTimeout=Number</td>
<td>Timeout value of reboot prompt in seconds. If set to -1, then the UI waits for the user to close it manually.</td>
</tr>
<tr>
<td>/DefaultRebootTimeoutAction</td>
<td>A string that determines the action for vulscan to take if timeout value expires for reboot prompt. Acceptable values: reboot, close, snooze.</td>
</tr>
<tr>
<td>/SnoozeCount=Number</td>
<td>Number of snoozes. Vulscan decrements each time the user clicks <strong>Snooze</strong> on the reboot prompt.</td>
</tr>
<tr>
<td>/SnoozeInterval=Number</td>
<td>Number of seconds for vulscan to sleep between snoozes.</td>
</tr>
<tr>
<td><strong>MSI parameters</strong></td>
<td></td>
</tr>
<tr>
<td>/OriginalMSILocation=path</td>
<td>Path to original MSI location.</td>
</tr>
<tr>
<td>/Username=username</td>
<td>Username for MSI directory.</td>
</tr>
<tr>
<td>/Password=password</td>
<td>Password for MSI directory.</td>
</tr>
<tr>
<td><strong>Disable parameters</strong></td>
<td></td>
</tr>
<tr>
<td>/NoElevate</td>
<td>Runs vulscan with the permissions of the user who is currently logged in.</td>
</tr>
<tr>
<td>/NoSleep</td>
<td>Prevents sleeping during a vulnerability scan.</td>
</tr>
<tr>
<td>/NoSync</td>
<td>Doesn't get mutex, scans multiple instances.</td>
</tr>
<tr>
<td>/NoUpdate</td>
<td>Don't get a new version of vulscan.</td>
</tr>
<tr>
<td>/NoXML</td>
<td>Don't look for msxml.</td>
</tr>
<tr>
<td>/NoRepair</td>
<td>Same as autofix=false. Overrides autofix settings if present.</td>
</tr>
<tr>
<td><strong>Data files parameters</strong></td>
<td></td>
</tr>
<tr>
<td>/Dump</td>
<td>Dumps vulnerability data directly from the web service.</td>
</tr>
<tr>
<td>/Data</td>
<td>Pulls in vulnerability data (from /dump).</td>
</tr>
<tr>
<td>/O=Path\Filename</td>
<td>Outputs scan results to the specified file instead of to the core server.</td>
</tr>
<tr>
<td>/I=Path\Filename</td>
<td>Input scan results.</td>
</tr>
</tbody>
</table>
Configure Patch and Compliance alerts

The following section describes other tasks you can perform with the Patch and Compliance tool.

Configure patch and compliance alerts

You can configure patch and compliance security alerting so that you’re notified when specific vulnerabilities are detected on your managed devices. Patch and Compliance’s vulnerability alerting uses the standard Ivanti alerting tool.

For a vulnerability definition to generate an alert when detected, you must first copy the definition into the Alert group. 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 be placed automatically during downloads), you can configure the alert interval in the Configure alerts dialog box.

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 place automatically 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.
Generate 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 and for each of the various security risk content types.

To access the Reports tool and generate and view reports, a user must have the Ivanti Administrator right (implying full rights) and the specific Reporting roles.

For more information about using the Reports tool, see "Using reports" (381).
Rollout projects

Overview of rollout projects

Rollout projects are a simplified method for managing vulnerability patching or software distribution. A rollout project is a set of steps to automate deployment. For each step, you can perform actions (such as a scheduled task), set criteria for when the content should move to the next step (such as an 80% success rate), and send notification emails.

When the patches or software packages have completed the actions in a step and pass the exit criteria, they are moved to the next step in the project. A project can be completely automatic, or you can require administrator intervention to make sure content doesn’t progress until you approve it. And since you can set up email notices when a step succeeds or fails, you may not need to monitor the project as closely.

Use a rollout project for a distribution task that has multiple steps that can be automated. For example, applying patches in phases, or distributing new software to a pilot group before general distribution. Rollout projects are especially useful in situations where the task is frequently repeated or requires minimal oversight.

To use a rollout project, complete the following steps:

- **Create a scheduled task for the project processor.** The rollout project processor applies the actions on the content in the project, evaluates if the content meets exit criteria, and moves content from step to step. For more information about how the project processor works, see "How a rollout project works" (769).

- **Create the rollout project.** Choose whether you want the project to be for software packages or patch definitions. For information about the options when creating a rollout project, see "Creating and editing a rollout project" (771).

- **Add steps to the project.** Steps contain the information about the actions that you want performed. For more information, see "Adding steps to a rollout project" (773).

- **Add content to the project.** Once you have the project created, add the definitions or software packages to the project. You can copy and paste the content, or automatically add definitions using a download definitions filter. For more information, see "Adding content to a rollout project" (779).

Once the project is created and has content, make sure it is in the Play state. When the scheduled task runs, the project processor applies the actions.
Example software package rollout project

To perform a staged rollout for new software, you can set up a rollout project to deliver the software to a small group first, and then after it has been installed on 80% or more of those devices, wait for a week to make sure things are working as designed. If the software fails to install on a significant percentage of devices within 2 weeks, set up the rollout project to send an email warning and don’t push the software to a larger group. However, if everything works as planned, push the software to a larger group.

This example has two steps:

- **Step One**
  - Action: A scheduled task that distributes the software package to a small group.
  - Exit criteria: An 80% success rate, meaning that the package cannot move to Step Two until the success rate has been matched or exceeded.
  - Email: You get an email if the package is still in Step One after 2 weeks.

- **Step Two**
  - Action: A scheduled task that distributes the software package to a larger group.

Example patch rollout project

To create a rollout project to automate deploying Ivanti patches, set up the definition download settings to always add Ivanti patches to the rollout project. Apply the patches to your pilot group, send an email that the patches have been downloaded and applied, then wait until an administrator confirms that the patches are working successfully. Deploy the patches to a larger group, and then when the patches are installed on 85% of the devices, set the patches to Autofix and tag them with an Autofix tag to make them easy to identify.

In this example, you change the definition download settings to add content automatically to a rollout project. When you use this feature, the downloaded content is added to the project and automatically begins to move through the project steps the next time the project processor runs. Since this feature requires no administrative oversight after it is set up, you’ll probably choose to do this only in situations where you trust the content or you have an approval built into the project.

This example has three steps:

- **Step One**
  - Action: A scheduled task that applies the patch to your pilot group.
  - Exit criteria: An 85% success rate, meaning that the patch must be installed on 85% of devices.
  - Exit criteria: Administrator approval.
• Email: After the success rate has been met, you get an email saying that the content is waiting for approval.

• Step Two
  • Action: A policy-supported push task that applies the patch to a larger group.
  • Exit criteria: An 85% success rate, meaning that the patch must be installed on 85% of devices.

• Step Three
  • Action: Set the patch to Autofix.
  • Action: Tag the patch as Autofix.

How a rollout project works

A rollout project is a set of steps to automate deployment. For each step, you can perform actions, set criteria for when the content should move to the next step, and send notification emails. When the patches or software packages have completed the actions in a step and pass the exit criteria, they are moved to the next step in the project. A project can be completely automatic, or you can require administrator intervention to make sure content doesn’t progress until you approve it. And since you can set up email notices when a step succeeds or fails, you may not need to monitor the project as closely.

The rollout project processor applies the actions on the content in the project, evaluates if the content meets exit criteria, and moves content from step to step. Schedule the project processor to run as frequently as you think content needs to move from step to step.

If you have actions in the project that are scheduled tasks, such as a software deployment, the project processor uses a template to create the task. It creates a new task each time the action is applied to content. The template it uses to create the scheduled task is specified when you create the step. For more information about the options available when you’re creating steps, see “Adding steps to a rollout project” (773).

The action for a step is only applied to content once. After the action has been applied, the content either moves to the next step or stays in the step until the exit criteria are met. If content stays in a step, the project processor does not reapply the actions the next time it runs; it only re-evaluates if the exit criteria have been met and if an email needs to be sent.

IMPORTANT: Content does not move to the next step as soon as it meets the exit criteria. It moves to the next step after it has met the exit criteria AND the project processor runs as a scheduled task.
The steps in a rollout project must be linear. You cannot create branches or force content to skip steps. If a step is paused, content may move into the paused step, but the actions for that step are not applied to the content. Content does not skip a paused step.

If there are no exit criteria set for a step, the action for the step is applied and the content is immediately moved to the next step. Content can progress through multiple steps each time the project processor runs.

**Creating a scheduled task for the project processor**

Schedule the rollout project processor to run as a scheduled task. Each time it runs, it processes every rollout project that is active. For information about how the project processor handles content that is paused, see "Creating and editing a rollout project" (771).

**To create a scheduled task for the project processor**

1. From the management console, click **Tools > Security and Compliance > Rollout projects** or **Tools > Distribution > Rollout projects**. Both paths open the same Rollout projects tool.
2. In the Rollout projects toolbar, click **Create a task > Scheduled project processing**.
3. Create a name for the task, and if you choose to, select the owner for the task. The scope used is based on the owner for the task.
4. Click the **Schedule task** page on the left, and configure the options for when the task runs and how frequently it runs.
5. Click **Save**.

**Run the project processor on demand**

For troubleshooting or testing a rollout project, you may want to run the processor immediately, process just one project or one step, or apply an action to content more than once.

**To run the project processor on demand**

1. From the Rollout projects tool, right-click a project or step and select **Process now**.

   **IMPORTANT:** If you try to process an item and the **Process now** option isn't available, make sure that the step and the project are both set to **Play** and are not paused.

2. A prompt asks if you want to **Re-apply actions even if they are already applied**. When you re-apply actions, the project processor runs just for that step and applies the actions to all content currently in the step, even if they have already met the success criteria for the step. Whether or not you choose re-apply actions, click **OK** to run the project processor.

   The project processor runs for the selected step or project.
• If actions are re-applied, the Applied actions timestamp is changed, the minimum duration and post duration timers are reset, and if there are scheduled tasks in the project or step, they are created again.

• If actions are not re-applied, content is evaluated to see if exit criteria have been met or if emails need to be sent. Only content that is new to a step has actions applied.

NOTE: Emails associated with a project step are not considered an action and may be sent regardless of whether or not actions are re-applied.

**Pause and play a project, step, or content**

Rollout projects, steps, and content in a project all have a state assigned: either play or pause. The state affects whether or not it is processed when the project processor runs. The icons in the Rollout projects tool have a play or pause overlay to indicate the current state of the item.

To change the state of a project, step, or content, right-click it and select either **Play** or **Pause**.

NOTE: You must pause a rollout project or a step before you can edit it.

• **When a project is paused**: The project processor excludes the project. No actions for the project are applied, no notifications are sent, no content moves from step to step.

• **When a step is paused**: The project processor does not process the content in the step. Content can be moved into the step (either manually or by advancing from the previous step) but actions are not applied. Content in a paused step does not advance to the following step even if it meets all of the exit criteria. If the step is paused after an action is applied, timers continue to run even while the step is paused. For content that does not have actions applied, any minimum duration or other timers do not start until the actions are applied.

• **When content is paused**: No actions are applied to the content, no notifications are sent regarding the content, and the project processor does not move it from the step it is currently in. If an action has been applied and a timer is associated with the current step, the timer continues to run.

**Creating and editing a rollout project**

A rollout project can be created for either a software distribution or patch management task. You must choose which type of project it is before you can begin adding steps, because some steps are specific to the project type.

NOTE: You can use rollout projects if you have either the Software Distribution role or the Patch Management role.
You must pause a rollout project or a step before you can edit it. When a project is first created, it defaults to a paused state. If the project has already been created, right-click it and select **Pause (exclude project from processing)**. For more information on what happens when a project is paused, see "How a rollout project works" (769).

When you create a rollout project, it has the following project options:

### General

- **Project type**: Select the project type. You must select the project type and save the project before you can add steps to it.

- **State**: Determine whether the content in the project is processed by the project processor. If the project is set to **Pause**, the project processor ignores the project and content stays in the step it is assigned to. When the project is set to **Active**, the project processor evaluates the content in each step and determines which content needs to move to the next step.

- **User scope when creating tasks**: When you create tasks associated with the project, the tasks are limited to the scope set for the project. Rollout projects use the same scopes that are used in the rest of Endpoint Manager.

### Email defaults

To edit the sender's address, email server address, username and password, click the **Email send options** link at the bottom of the page.

**NOTE**: These email settings are independent of other SMTP server settings that may be configured in other places in the Endpoint Manager console.

- **Sender's address**: The address that appears in the **From** field. Generally, people use this field to either indicate the purpose of the email, or an email address that the recipient can respond to if there are questions about the email.

- **SMTP server**: The address of the SMTP server.

- **User name**: A username to access the SMTP server.

- **Password**: A password to access the SMTP server.

- **Addresses**: The email recipients for the emails sent out for rollout projects. This list is for all rollout projects. Every time an email is sent for any rollout project, it is sent to the addresses in this list. If you want to send emails to a recipient only for a specific rollout project, use the Recipients page instead.

- **Step duration exceeded**: Configure the expected duration of the step, and send an email if content stays in the step longer than expected.
• **Exit criteria met**: Send an email when content has met the exit criteria for the step.

• **Approval**: Send an email when content has met all the other criteria for the step, but needs to be approved by an administrator before it can move to the next step.

• **Recipients**: The email recipients for the emails sent out for the selected rollout project. This list is only for the rollout project that you are currently editing. When an email is sent out for the project, it goes to the addresses on this list and the addresses on the global list (configured on the Addresses page of the project properties).

### Action history

The Action history page allows you to view what actions have been performed by the rollout project, and what content was involved. Each time content enters a step, has actions applied, or is evaluated against exit criteria, that information is tracked in the action history.

Use the Action history page to search actions, or sort actions based on date, success or failure, or if they were performed for the entire project, a step, or content.

**To create a rollout project**

1. From the management console, click **Tools > Security and Compliance > Rollout projects** or **Tools > Distribution > Rollout projects**. Both paths open the same Rollout projects tool.

2. Click the **New project or project step** button in the Rollout projects toolbar.

3. Provide a name for the project, select the project type, and click **Apply**. The project defaults to a **Pause** state, and is not processed by the project processor until you change the state.

   **NOTE**: You must select the project type and save the project before you can add steps to the project. This is because there are different steps available depending on the project type.

   After you have selected the project type and saved the project, you can edit the project settings, add steps, and change the state to **Play**. For information about adding steps to a rollout project, see “Adding steps to a rollout project” (773).

### Adding steps to a rollout project

A rollout project is a set of automated steps for a software distribution or patch management task. When content is added to a rollout project, it progresses through the steps. For each step, you can perform actions, set criteria for when the content should move to the next step, and send notification emails. The project processor is a scheduled task that applies the actions, moves content from step to step, and sends the emails. For information about how the project processor works, see “How a rollout project works” (769).

You must select the project type and save the project before you can add steps to the project. This is because there are different steps available depending on the project type.
The following options are available, depending on the type of rollout project you have created.

**Patch management**

**Actions**

- **Autofix settings**: Changes the Autofix setting for the definition. This can enable or disable either global or scoped autofix.
- **Group membership**: Changes the group membership for the definition.
- **Scan settings**: Changes the scan status for the definitions. This may include changing that status to scan, do not scan, unassigned, or approved for scoped scan, or it may change the scopes that scan for the definitions.
- **Tags**: Adds or removes tags from the content.
- **Patch task template**: Selects the task template to use when creating tasks associated with this step. Tasks created for a rollout project can be viewed in the task scheduler, located in the **Auto-generated rollout project tasks** folder. The tasks are created when the step has content in it and the project processor runs.

NOTE: This option refers to a scheduled patch task created by the project processor when the project runs. It is not the same as the project processor scheduled task.

- **Targets**: Selects the targets for the patch task.

**Exit criteria**

All of the exit criteria for the step must be met AND the project processor (a scheduled task) must run in order for content to move to the next step in the project. Content does not move to the next step as soon as criteria are met; it remains in the current step until the project processor runs. For information about how the project processor works, see "How a rollout project works" (769).

To see if a definition has met the exit criteria for the step it is currently in, find the definition in the Rollout projects tool, right-click the definition, and select **Properties**.
• **Keep content together**: On the Exit criteria page, the *Keep content together when advancing to next step* option forces all content that enters the step simultaneously to leave the step simultaneously. This option allows an administrator to keep similar or associated content all in the same step, making it easier to track. When the *Keep content together* option is set for a step, content cannot progress to the next step unless all of the content with the same Applied actions timestamp is ready to move to the next step. If you want to keep content together through the entire project, enable the *Keep content together* option for each step of the project.

• **Minimum duration**: Determine the minimum length of time that content must remain in the step.

• **Success rate**: Determine the percentage of target devices that must either have the patch successfully installed, or are not vulnerable. To check the success rate, the project processor examines the scan results for target devices. For tasks that are targeting large groups, we recommend limiting the number of devices that are checked, and using the success rate of the limited sample rather than trying to determine the success rate for all of the targeted devices.

• **Additional duration**: Requires the content to remain in the step for the specified time after the success rate has been met.

NOTE: If you configure both *Minimum duration* and *Additional duration*, the two timers can run simultaneously. For example, if a step has a minimum duration of four weeks, but the definition meets the success rate after one week, the Additional duration timer begins as soon as the success rate is met, even though the Minimum duration timer is still running.
• **Approval**: Blocks the content from advancing to the next step until an Ivanti administrator approves the content for advancement. To approve content, find the content in the rollout projects tool, right-click it, and select **Approve**.

• **Date time window**: Restricts the date or time that content can leave this step and move to the next step. Content does not automatically move to the next step during the date time window. When you use a date time window, the content must meet all of the exit criteria and the project processor must run during the date time window for content to advance to the next step. Make sure that the project processor runs during the date time window that you create, or else the content will never leave the step.

**Email**

There are two lists for email recipients: one for all rollout projects and one for individual projects. When you add recipients to the address list from the step properties, you’re adding them to the project recipient list. You cannot create an email recipient list for a specific step.

When content is in a step that has email options set, the project processor sends an email when the expected duration has been exceeded, the exit criteria have been met, or the content needs approval.

• **Duration exceeded**: Sends an email to the addresses on the project email list when the content has been in the step for longer than expected. Configure the amount of time you expect the content to stay in the step. If content stays in the step past that time, recipients receive an email each time the project processor runs and the content is still in the step. You can restrict how frequently emails are sent by setting a minimum interval, but that interval only applies to the current step.

• **Exit criteria met**: Sends an email to the addresses on the project email list when the content has met the exit criteria for the step. The content progresses to the next step without administrator action.

• **Approval**: For this option, you must enable the Approval exit criterion. When all other exit criteria have been met but approval is still required, the project sends an email requesting approval. If content stays in the step, recipients receive an email each time the project processor runs and the content is still in the step. You can restrict how frequently emails are sent by setting a minimum interval, but that interval only applies to the current step.

**Action history**

The action history displays the actions associated with the step and the content in it. You do not configure anything on the Action history page.
Software distribution

Actions

- **Schedule distribution task template**: Selects the task template to use when creating tasks associated with this step. Tasks created for a rollout project can be viewed in the task scheduler, located in the **Auto-generated rollout project tasks** folder. The tasks are created when the step has content in it and the project processor runs.

NOTE: This option refers to a scheduled software distribution task created by the project processor when the project runs. It is not the same as the project processor scheduled task.

- **Targets**: Selects the targets for the distribution task.

Exit criteria

All of the exit criteria for the step must be met AND the project processor (a scheduled task) must run in order for content to move to the next step in the project. Content does not move to the next step as soon as criteria are met; it remains in the current step until the project processor runs. For information about how the project processor works, see "How a rollout project works" (769).

To see if a definition has met the exit criteria for the step it is currently in, find the definition in the Rollout projects tool, right-click the definition, and select **Properties**.

- **Keep content together**: On the Exit criteria page, the **Keep content together when advancing to next step** option forces all content that enters the step simultaneously to leave the step simultaneously. This option allows an administrator to keep similar or associated content all in the same step, making it easier to track. When the **Keep content together** option is set for a step, content cannot progress to the next step unless all of the content with the same Applied actions timestamp is ready to move to the next step. If you want to keep content together through the entire project, enable the **Keep content together** option for each step of the project.

- **Minimum duration**: Determine the minimum length of time that content must remain in the step.

- **Success rate**: Determine the percentage of target devices that must have the software successfully installed.

- **Additional duration**: Requires the content to remain in the step for the specified time after the success rate has been met.

NOTE: If you configure both **Minimum duration** and **Additional duration**, the two timers can run
simultaneously. For example, if a step has a minimum duration of four weeks, but the definition meets the success rate after one week, the Additional duration timer begins as soon as the success rate is met, even though the Minimum duration timer is still running.

- **Approval**: Blocks the content from advancing to the next step until an Ivanti administrator approves the content for advancement. To approve content, find the content in the rollout projects tool, right-click it, and select **Approve**.

- **Date time window**: Restricts the date or time that content can leave this step and move to the next step. Content does not automatically move to the next step during the date time window. When you use a date time window, the content must meet all of the exit criteria and the project processor must run during the date time window for content to advance to the next step. Make sure that the project processor runs during the date time window that you create, or else the content will never leave the step.

**Email**

- **Duration exceeded**: Sends an email to the addresses on the project email list when the content has been in the step for longer than expected. Configure the expected duration and how often the email recipients receive emails for the rollout project. This reduces email traffic when several definitions complete steps at the same time.

- **Exit criteria met**: Sends an email to the addresses on the project email list when the content has met the exit criteria for the step.

- **Approval**: For this option, you must enable the Approval exit criterion. When all other exit criteria have been met but approval is still required, the project sends an email requesting approval. If content stays in the step, recipients receive an email each time the project processor runs and the content is still in the step. You can restrict how frequently emails are sent by setting a minimum interval, but that interval only applies to the current step.

**Action history**

The action history displays the actions associated with the step and the content in it. You do not configure anything on the Action history page.

**To create a new step in a rollout project**

1. Select the rollout project, and make sure that the project is paused. You cannot add steps to a project while it is active.
2. Click the **New project or project step** button in the toolbar.
3. In the Project step properties dialog, provide a name for the new step and configure the options. On some pages, you must enable the checkbox in the upper left corner before you can edit the options on the page.
4. Click **OK** to save the step.

5. Change the state of the project back to **Play**. If the project is paused, content will not be processed the next time the project processor runs.

### Adding content to a rollout project

Add definitions or software packages to a rollout project by either dragging and dropping the content, or copying and pasting it. If you add content to a specific step, the content will start processing at the step where you put it. If you add content to the project, it will start processing in the first step in the project.

Content can be in more than one rollout project at a time, and it can be in more than one step of a project at a time. For example, if an administrator doesn’t notice that a definition has already progressed to step 6 and he adds it to step 1, the actions for both step 6 and step 1 are applied to the definition.

However, if you try to add a definition or package to a step where it already exists, the project detects it and ignores the duplicate. If you want to reapply the actions in a step to content (usually for testing purposes), right-click the step and select **Process now**. In the dialog box that appears, enable the **Re-apply actions even if they are already applied** option and click **OK**. The project processor will process just that step of the project and apply the actions to all the content in the step.

To see a summary of the current state or action history for a definition or package, find the content in the Rollout projects tool, right-click it, and select **Properties**. The Gantt chart page displays any differences between the expected duration (how long content spent in a step) and the actual duration. To configure the expected duration for a step, select the step, click **Properties**, and edit the **Expected step duration** on the Exit criteria page.

### Adding patch definitions automatically

For Patch and Compliance, you can also add content to a rollout project automatically using a definition filter. When definitions are downloaded, the content matching the definition filter is automatically added to the specified rollout projects.

#### To automatically add downloaded definitions to a rollout project

1. Make sure you have already created a Patch rollout project.

2. From the Patch and Compliance tool, click the **Download updates** button in the toolbar. If you haven’t already, select the definitions that you want to download, and configure other download settings as desired.

3. On the Updates tab, click the **Definition download settings** button.
4. In the Definition download settings dialog, click New.

5. Configure the rule to match the content that you want added to the rollout project.

6. On the Rollout projects tab, enable the Add definition to projects check box and click the Add button. Select the rollout project you want to add the content to.

When content is downloaded, all content that matches the filter is added to the rollout project. If the rollout project is in an active state, the next time the project processor runs, the content will have the actions for the first step applied.

**Deferring content**

When you copy or drag content into a project, you have an option to wait before processing the content. A dialog asks if you want to defer the actions until a specified date and time. When actions are deferred, the content does not progress through the project steps and no actions are applied to the content until after the deferral time has passed. The deferral is only applied to the content you just added. It is not a project setting.

If you decide you do not want the deferral prompt each time you add content, make sure the Prompt to defer actions when dropping/pasting vulnerabilities or packages into a rollout project option is not selected when you click OK. You will still be able to defer content or enable the option again.

To defer content after it has been added to a project, find the definition in the Rollout projects tool, right-click it, and select Defer start.
Security activity

Security Activity overview

The new Security Activity tool provides a convenient single window where you can view status and activity information for several Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk services running on your managed devices.

Security Activity lets you view status and activity information for:

- Ivanti Antivirus
- Host Intrusion Prevention (HIPS)
- Ivanti Firewall
- Device Control

You can also perform these tasks:

- Configure security activity threshold settings
- Purge security activity information

View security status and activity

The Security Activity tool lets you view information about Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk services.
The security tools you can view are described in the following sections.

**View Ivanti Antivirus activity and status information**

If the Ivanti 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**, and in the **Type** drop-down list select **Antivirus**. You can view:
- Missing antivirus updates
- Not detected
- Antivirus updates not scanned
- Installed antivirus updates
- Clean/Repair history

**About the Antivirus activity and status information dialog box**

Use this dialog box to view detailed antivirus activity and status information for all of your managed devices with the Ivanti Antivirus agent. This scan result data is used to generate the Ivanti 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 box contains the following options:

- **Refresh**: Updates the fields in the dialog box with the latest antivirus scan information from the database.
- **Thresholds**: Opens the Threshold settings dialog box, 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 Ivanti Antivirus agent that have not been scanned for viruses within the time period specified on the Threshold settings dialog box. If you want to run an immediate antivirus scan, right-click the device, click Ivanti Antivirus scan now, select an antivirus setting, and then click OK.
- **Computers with recent antivirus activity**: Lists all of the devices with the Ivanti Antivirus agent that have been scanned and have returned antivirus activity within the time period specified on the Threshold settings dialog box. Select a device to see its specific antivirus activities, including virus detection, removal, infected object quarantine, backup, and restoration.
View 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 box

Use this dialog box to view detailed HIPS activity for all of your managed devices with the Ivanti HIPS agent. This data is used to generate the Ivanti 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 box contains the following options:

- **Refresh**: Updates the fields in the dialog box with the latest HIPS information from the database.
- **Thresholds**: Opens the **Threshold settings** dialog box, 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.

**View Ivanti Firewall activity**

The window displays Firewall activity by the following categories:

- Preventions by computer
- Preventions by application
- Preventions by action

**Views 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

**Configure security activity threshold settings**

Security activity information for your managed devices can build up quickly and adversely impact the performance of the core database.

Use this dialog box to define data collection time periods and control the amount of security-related data that is stored in the core database for the Ivanti Antivirus, Application Control, and Firewall tools. This information appears in the corresponding Security Activity views.

**About the Threshold Settings dialog box**

- **Common Thresholds**:
  - **Threshold for recent activity views**: Specifies the time period (in days) to collect security activity for devices that have been scanned and have returned antivirus activity.
  - **When displaying results, truncate lists to**: Indicates the maximum number of entries to display in the lists in the activity dialogs. You can specify 1 item to 999,999 items.
• Ivanti Antivirus:
  • Pattern files out of date if older than:
  • Threshold for license expiration warning:
  • 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.

• Automatic purge (Application Control / Ivanti Firewall only):
  • Automatically delete activity older than: Indicates the maximum number of days to keep reported Application Control and Ivanti Firewall activity for protected devices in the core database. You can specify 1 day to 999 days. (IMPORTANT: Ivanti recommends that you carefully watch the amount of data being sent to the core and find an optimal number of days so that Application Control data doesn’t use too much space or hinder core database performance.)

**Purge 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.

*Security activity purging is a one-time task, not a scheduled task or policy.*
About the Purge security activity dialog box

Use this dialog box to completely remove activity records from the console and core database.

This dialog box contains the following options:

- **Select activity type**: Specifies which security component activity information you want to purge.
- **Select computers**: Specifies which managed devices’ security activity is purged. (Note: You must be an administrator user 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 selected security activities.

Configure security 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 Ivanti alerting tool.

The alert settings dialog contains options for both vulnerability alerting and antivirus alerting.

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 avoid receiving 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 box. Right-click a device, select Security and Patch Information, select the Antivirus type in the Type list, and then select the Antivirus History object.

**Vulnerability alerting**

For information on vulnerability alerting, see "Configure Patch and Compliance alerts" (765).

**Application information view**

The application information view is a Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk feature that shows information about the applications used on a specific endpoint. It helps admins detect and troubleshoot suspicious and malicious applications.

For example, if a user calls support complaining that his computer isn’t working correctly, an IT admin can open the Application information view for that device. The admin then uses it to determine which applications were running on the device and view detailed information about those applications.

For each detected application, this view shows:

- File name/path
- Date discovered
- Last executed
- Reputation and Ivanti reputation
- The number of devices the file has been detected on
- File version, company name, and product name
- SHA256 hash

Additionally, if the endpoint has the endpoint security agent installed, the following information is available for each application:

- Amount of network traffic sent/recieved
- The URL or IP the application connected to
- Memory and CPU usage

The application information comes from the last inventory scan. If you need more recent information, a Data sync button lets you remotely trigger an immediate inventory scan. It can take a few minutes for the remote scan to complete and for the Application information view to refresh.

The Application view toolbar provides quick access to the following tools:

- Diagnostics window
- Full device inventory
- Security and patch information
- Remote control
- Virus scan
- Remote reboot
- Virus Total (requires file hashes from the inventory scanner, this isn’t enabled by default)
- IOCBucket searches
- Community and Google searches
Endpoint security

Endpoint Security overview

The Endpoint Security tool is a set of complementary features and settings that enables you to configure and implement strong system security for the managed devices on your network. You can restrict network connections for managed devices, restrict access to those machines by other types of devices, and use the Host Intrusion Prevention System (HIPS) and Ivanti Firewall tools to prevent unauthorized application operations.

Endpoint Security provides an impenetrable defense for all the protected devices within your Ivanti network and the perimeter of that network, as well as mobile users—providing complete control over access to and from those devices and what is allowed to occur on them. You can define trusted locations (network connections) for managed devices, create settings for each of the Endpoint Security components listed below, and deploy those settings based on whether the device is inside or outside the trusted network location.

Endpoint Security components

The Endpoint Security components are:

- **Location Awareness**: Provides network connection control with location awareness and trusted location features. For information, see Endpoint Security help.
- **Application Control**: Prevents unauthorized intrusions. For information, see "Application control overview" (793).
- **Ivanti Firewall**: Prevents unauthorized application operations and connections. For information, see "Agent settings: Ivanti Firewall" (270).
- **Device Control**: Restrictions access for storage volumes, devices, interfaces, and so on. For information, see "Device Control overview" (805).
- **Whitelist and the trusted file list**: Provides lists of files configured with a specific set of rights (privileges or authorizations) that allow and deny certain actions that can be performed on that file by an application.

Although Endpoint Security is a single agent that is deployed to target devices, it is fully configurable and is meant to consolidate the security component services. You can configure these components independently or in a combined deployment. For example, you can deploy application control only, or application control and device control (via their respective settings), or any other combination of security components.

Enable and deploy Endpoint Security

Endpoint Security is enabled on managed devices by deploying custom 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. Click Tools > Configuration > Agent Settings. In the Agent Settings tool window, right-click Endpoint Security, and then click New.

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. At the Digital signatures page, configure how signed applications are handled.

4. At the Default policy page, select which Endpoint Security components you want to deploy to target devices with the Endpoint Security settings.

5. At the Location policies page, configure location-aware policies that you want to use.

6. At the Trusted folders page, specify any folders whose contents you want to trust automatically.

7. Click Save.
Once configured, you can deploy settings to target devices with an installation or update task, or a change settings task.

**What happens on a device with Endpoint Security**

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 user interface**

Once Endpoint Security has been deployed to managed devices, the client can be accessed through either the Start menu or the system tray icon.

**IMPORTANT: 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.

**End user actions**

The client is displayed in a window that includes the following elements, where the end user can:

- View Protection status for Endpoint Security components (home view)
- View program activity (reports view, **Program activity**)
- View startup applications (reports view, **Startup applications**)
- View the Ivanti trusted file list (reports view, **Trusted file list**)
- View the detailed Endpoint Security activity log for your computer (reports view, **Detailed activity**)
- Request that the Ivanti administrator grant an exception for a blocked file (reports view, **Detailed activity**, right-click the blocked file notification and click **Request exception**)

**Administrator notifications on Endpoint Security activity**

Use the Security activity tool's **Application control** section (**Tools** > **Security and Compliance** > **Security activity**) to view Endpoint Security notifications. If there are endpoint security actions that may need your attention, you will also see a notification when you log in to the Endpoint Security for Endpoint Manager console.

**Additional endpoint security information from the Ivanti community**

The Ivanti endpoint security agent (EPS) provides two main ways to protect applications running on the endpoint: application behavior protection and whitelisting protection. Application behavior protects applications against malicious change to the application itself (for example protect against in-memory attacks), and whitelisting prevents untrusted applications from running.
The EPS agent also protects itself and other Ivanti agents from tampering. The EPS agent will prevent deleting/modifying files protected by it. This protection is always active and does not require any configuration.

For detailed information on these EPS features, see [The Definitive Guide to Ivanti Endpoint Security](https://community.ivanti.com/doc/47588) on the Ivanti community (document 47588):

- Application behavior
- Application blocking
- Whitelisting
- Application firewall
- Malicious activity detection
- 3rd party integration, such as SIEM
- Browser isolation for unpatched browsers
- Device network isolation

## Application control overview

Application control provides another layer of protection — on top of patch management, antivirus, anti-spyware, and firewall configuration — to prevent the intrusion of malicious activity on your managed devices. Application control 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 (i.e., signature-based) system, application control is more effective at protecting systems against zero-day attacks (malicious exploitation of vulnerable code before exposures are discovered, defined, and patches made available).

Unlike vulnerability detection and remediation, spyware detection and removal, or antivirus scanning and quarantine; application control protection does not require ongoing file updates, such as patch files, definition/pattern files, or signature database files.

Application control 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 Application control settings are accessed from the main console (Tools > Security and Compliance > Agent Settings). The Application control agent setting lets you create application control agent installation, update, and removal tasks; configure application control settings that can be deployed to targeted devices you want to protect; and customize application control display/interaction settings that determine how application control appears and operates on managed devices, and which interactive options are available to end users. You can also view endpoint security activity and status information for protected devices in the Security activity tool (Tools > Security and Compliance > Security activity).

Component of Endpoint Security

Application control is one of the components of the comprehensive Endpoint Security solution, along with the Location Awareness (network connection control), Ivanti Firewall, and Device Control tools.

Proactive security

Application control 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

Application control 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
**Application control console features**

Application control provides administrators with the ability to define and manage separate profiles for different user groups with application control settings. Endpoint security settings accommodate the needs of any and all user groups by allowing administrators to create multiple, highly flexible configurations for different user profiles.

Application control settings can include custom password protection, WinTrust handling, protection mode, custom whitelists, network and application access control policies, file certifications, and file protection rules.

**Application control client features**

The Endpoint Security client (deployed to managed devices) gives administrators a powerful new tool for controlling what applications run on enterprise desktops and servers, and how those applications are allowed to execute.

Application control 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 application control component uses a variety of proprietary techniques to reliably detect malware even before a signature has been identified.

**Supported device platforms and antivirus products**

For up-to-date detailed information on which device platforms and antivirus products support application control (endpoint security), see the endpoint security landing page at the Ivanti User Community:

https://community.landesk.com/support/docs/DOC-23838

---

**IMPORTANT: Endpoint security is not supported on core servers or rollup cores**

You should not install/deploy endpoint security to a core server or a rollup core. However, you can deploy endpoint security on an additional console.

Do NOT deploy application control to devices with any other antivirus product installed.

**Application control licensing**

In order to use Endpoint Security and application control, you must first activate your core server with a license that allows their use.

For information about licensing, contact your reseller, or visit the Ivanti website:

Ivanti Home Page
Role-based administration with endpoint security

Endpoint security, 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 Ivanti 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. Endpoint security is included in the Agent Settings right, which appears under the Security rights group in the Roles dialog box. In order to see and use endpoint security features, a user must be assigned the necessary Agent Settings access rights.

With the Agent Settings right, you can provide users the ability to:

- See and access the endpoint security features in the console's Tools menu and Toolbox
- Configure managed devices for endpoint security protection
- Manage endpoint security settings (password protection, signed code handling, action, protection mode, file certifications, file protection rules, etc.)
- Deploy endpoint security install or update tasks, and change settings tasks
- View endpoint security activity for protected devices
- Define endpoint security data threshold settings for recording and displaying endpoint security activity

Endpoint security main tasks outline

The list below outlines the main tasks involved in configuring, implementing, and using endpoint security protection. See feature-specific help topics for detailed conceptual and procedural information.

- Configure managed devices for endpoint security protection (deploying the agent to target devices).
- Configure endpoint security options with endpoint security 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.
- Discover file and application behavior on devices with the endpoint security learn mode.
- Enforce endpoint security protection on managed devices with the endpoint security automatic block mode.
- View endpoint security activity for protected devices.
Configure devices for Endpoint Security 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 application control.

You can configure devices for Endpoint security either during initial device agent configuration or with a separate installation or update task.

To install or update Endpoint Security 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 application control settings.)
5. Select one of the settings from the available list to apply it to the agent configuration you’re creating. You can create new settings or edit existing settings by clicking Configure. Make sure you select the Endpoint Security components that you want to use from the Default policy page.
6. Finish specifying settings for the agent configuration and then click Save.

Understand the application control learn mode

Application control can run in one of the following protection modes: Disabled, Learning, Logging, or Blocking.

Using the application control learn mode

Below is a description of the application control learn mode process:

- In learning mode, application control learns what kind of applications are installed on the device, how they behave, and their rights (privileges).
- Application control 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 Application control settings dialog box.)
- Administrators can customize application control settings to allow and deny privileges for relevant applications.
Learning mode can be applied to managed devices generally allowing application control violations to occur until a new application control setting 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.

IMPORTANT: Keep in mind that both the core server and managed device must be operating in learn mode in order for the action history communication to take place.

Application blocking

One of the best ways to protect endpoints from malware is with application blocking. When this is enabled, only white-listed applications can run. Application blocking is managed through agent settings. You should consider having a separate agent setting for devices needing application blocking, since you may not want to block applications on servers, for example.

If you don’t want all devices to block the same applications, you can create custom blocked application groups. For example, perhaps one department needs one set of applications blocked, and a different department needs a different set of applications blocked.

For detailed information and a video covering these scenarios, visit the Ivanti Community:

- How to use Application Blocking in LDMS Patch and Compliance Manager (https://community.ivanti.com/docs/DOC-34999)
- Video--Blocking Applications (https://community.ivanti.com/docs/DOC-33761)

To enable application blocking in agent settings

1. Click Tools > Configuration > Agent settings > Distribution and Patch. Create a new agent setting there or edit an existing one.
2. Click Patch-only settings > Scan options. Select the Blocked applications option.
3. Click Save.

To configure blocked applications

1. Click Tools > Security and compliance > Patch and compliance.
2. On the toolbar, switch to the Blocked applications view.
3. If you haven’t already, update the blocked applications list. Click the Download updates toolbar button. Click Windows > Security and select Applications to block. Click Download now.
4. Once the applications to block list finishes downloading, in the Blocked applications tree click Unassigned to see the list of blockable applications.
5. Select the applications you want to block in the Unassigned list and move them to the **Block** tree.

6. The selected applications will now be blocked on devices.

Changes to the **Block** tree take effect on managed devices the next time the vulnerability scanner runs.

**Application behavior script blocking**

File protection rules can block the most common way endpoints get infected by malware or ransomware—when a user is tricked (usually by a phishing email) into opening an attachment or downloading a file from the internet that contains the malware. Most of those files users are tricked into opening are from known types, such as Word documents with macros, JS (JavaScript) files, and other types of scripts.

Using file protection rules, you can set rules that prevent JS files and other scripts from being used by users (note that this does not limit users from using JavaScript in their browser). By blocking the usage of scripts (which most users do not need to use), a large portion of this attack vector can be eliminated.

It is most likely that users will not need to run scripts on their computers; however, in some cases legitimate third-party applications may need to run scripts. For that reason, it’s recommended that you start using file protection rules in learning mode (i.e., set the application behavior mode to learning). In this mode, the EPS agent learns which applications are running scripts and will not block their usage once you change to blocking mode.

For example, using file protection rules, you can configure the following rule: Don’t allow WSCRIPT and CSCRIPT to run *.JS files. Once enforced, users will not be able to use the Microsoft scripting engine (WSCRIPT/CSCRIPT) to run .JS files. Make sure to enable the Allow trusted files to bypass the rule option to bypass this protection for applications that were discovered using WSCRIPT to run .JS files during the learning period.

**Execution chain and internet origin blocking**

Two new options were added in 2017.1 to file protection rules that help block users from running scripts from a browser or mail application even though the scripts were downloaded inside a zip file.

- Apply if process is in the execution chain
- Apply only to files downloaded from internet
When the **Apply if process is in the execution chain** option is enabled, monitored programs are any program in the “chain of execution.” For example, if a user runs Chrome and opens a .JS file downloaded by Chrome (i.e., the user double-clicks the .JS file after it has been downloaded by Chrome), the chain of execution will be Chrome > WSCRIPT > JS. When this option is enabled, the “monitored program” can be Chrome and the “protected files” can be *.JS. This will ensure any JS file that runs from Chrome is blocked.

In 2017.1 there's also a new out-of-the-box file protection rule that is designed to prevent script execution from a browser or a mail application. This rule prevents a set of defined browsers and mailers from running CMD, CSCRIPT, WSCRIPT, and PowerShell. It will block any attempt to run a script by a browser or a mail app (this applies only to scripts that run "outside" the browser—not JavaScript running in the browser as part of a website).

There is one common case where using **Apply if process is in the execution chain** will not block the execution of scripts—when the script is packed into a zip file and the user extracts the zip using the native Windows ZIP extractor (not a third-party app). However, this rule will work to block an attachment zip file if a user opens it with WINZIP and then runs a script which was inside the zip file.

To solve the above problem, a second option, **Apply only to files downloaded from the Internet,** is available. By default, every file that is downloaded by a browser is flagged by the browser as "downloaded from the internet.” This flag is kept with the file even if the file is copied (note that this flag only applies to files on a NTFS file system). When this option is enabled, the rule will only apply to files that have this flag enabled.

A new out-of-the-box rule uses this feature to prevent script execution from files downloaded from the internet by a browser (“Prevent access to downloaded scripts”). When a user downloads a zip file from the internet, if the zip includes a script (.BAT, .CMD, .JS, .VBS), the script will be blocked from executing, even if the zip was extracted using the native Windows zip application and even if the file was saved to disk and extracted at a later stage.

**To enable execution chain or internet origin options in a file protection rule**

1. Click **Tools > Security and compliance > Agent settings.**
2. In the tree under **Agent settings > My agent settings > Security > Endpoint Security,** right-click and click **New,** or double-click an existing configuration.
3. On the **Default policy** page, select the application control setting you want to modify and edit it.
4. On the **File protection rules** page, modify or add the rule you want.
5. You’ll see the **Apply if process is in the execution chain** option and the **Apply only to files downloaded from internet** option on the rule configuration page.
Configure Ivanti Firewall settings

The new Ivanti Firewall tool is an important component of Endpoint Security that lets you protect managed devices from unauthorized application operations and connections.

With Ivanti Firewall settings, you can create and configure trusted programs (applications), trusted network scopes, and connection rules to protect managed devices from unauthorized intrusions.

IMPORTANT: Ivanti Firewall and Windows Firewall compatibility

The Ivanti Firewall complements the Windows Firewall, and both can be enabled and running at the same time on managed devices.

Component of Endpoint Security

Ivanti 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 chapter to learn about:
Using Ivanti Firewall settings

Firewall settings give you complete control over how the Ivanti Firewall operates on target devices. This section describes how to create and manage Firewall settings.

Creating Ivanti Firewall settings

To create Ivanti Firewall settings

1. In the Agent Settings tool window, right-click Ivanti Firewall, and then click New.

2. On the General settings page, enter a name for the settings, enable the Ivanti Firewall service, and then specify the protection mode. For information about an option, click Help.

3. On the Trusted file lists page, add and edit application executable files you want to be able to connect to and from the network and the Internet. You can also define the trusted scope.
4. On 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.

**Ivanti Firewall settings help**

Use this dialog to create and edit Ivanti Firewall settings. When creating Firewall settings, you first define the general protection mode, and then add and configure specific trusted file lists, 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 Ivanti Firewall and configure the protection mode.

This page contains the following options:

- **Name**: Identifies the Firewall settings with a unique name.
- **Enable Ivanti 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.
  - **Blocking**: All security 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.
  - **Learning mode for**: 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.

  **NOTE**: These two time period options are executed successively. In other words, if both are selected, the learning mode period runs first and when it expires the logging mode period runs.

- **Logging mode for**: Specifies a period of time during which the applications that run are recorded in an action history file on the core server.
- **Learning**: All applications are allowed to run. Additionally, all of the applications that are run on the device are learned and added to the trusted file list.

- **Log only**: Security violations are allowed, but are recorded in an action history file on the core server.

- **File sharing**: Specifies file sharing privileges allowed by the Ivanti Firewall settings.
  - **Allow file sharing from the trusted scope (network)**: Allows files to be shared within the trusted scope you’ve defined.
  - **Allow file sharing from outside the trusted scope (Internet)**: Allows files to be shared outside of the trusted scope you’ve defined.

**About the Trusted scope dialog box**

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 scope**: Lists all of the trusted scopes.

- **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.

- **Batch import IP address...**: Lets you select multiple

- **Import...**: Lets you import subnet ranges from managed devices contained in the core database inventory.

**About the Connection rules dialog box**

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 box**

Use this page to configure connection rules.

This page contains the following options:

- **Name**: Identifies the connection rule with a descriptive name.
- **Direction**: Indicates whether the connection rule restricts inbound or outbound connections.
- **Action**: Indicates whether the connection rule allows (accepts) or prevents (drops) connections.
- **Protocol**: Specifies the communication protocol for the selected ports.
- **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.
- **IP address 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.
- **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 overview**

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.

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, wireless, 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 Application Control and Ivanti Firewall tools.

Supported platforms

Device Control works for managed devices running supported Windows versions.

Restrict device access with Device Control settings

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:

- Android, BlackBerry, and Apple iOS devices
- USB devices such as drives, keyboards and mice, printers, and scanners
- Cell phones and other mobile 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
Creating device control settings

To create device control settings

1. Click Tools > Security and compliance > Agent settings.
2. Under All agent settings, right-click Device Control, and then click New.

3. On the General Settings page, enter a Name.
4. Select the Enable device control check box.
5. On the other pages, customize the options you want. For more information about the options on the dialog box, see “Agent settings: Device control” (249).
6. Click Save to save the settings.
7. Under Endpoint security, double-click the endpoint security setting that you want to use to apply the device control settings.
8. On the Default policy page, check Device control and select the device control setting that you want to apply.
9. Click Save to save the settings.
Deploy Device Control settings

Once you’ve created a Device Control setting, you must deploy it to managed devices before it will be active.

Device Control is deployed via Endpoint Security settings.

To deploy device control settings

1. Click Tools > Security and compliance > Agent settings.
2. On the Agent settings toolbar, click the Create a task button, and click Change settings.
3. Under Task type, select the option you want.
4. In the settings list, select Endpoint security and select the Endpoint security setting that enables the device control setting you want.
5. Click OK.
6. The setting is added to the Scheduled tasks window. In this window, drag devices onto the setting icon.
7. 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 “Scheduling tasks” (415).

Create custom messages when unauthorized devices or volumes are detected

In the Device control settings dialog, you can customize the message text that the user sees when unauthorized devices or 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 Ivanti Endpoint Security service on managed devices. When the service receives notification from the OS that a new USB device has been inserted, the 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 Ivanti Endpoint Security 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.

Device network isolation and remediation (new in 2017.1)

When you suspect an endpoint is running malware, the best practice is to isolate the endpoint from the network to ensure the malware doesn’t spread to other endpoints.

The Endpoint Security for Endpoint Manager isolation capability provides an end-to-end solution for you to respond quickly to security threats and remediate them as soon as possible. Using Endpoint Security for Endpoint Manager, you can:

1. Isolate a device directly from the management console by right-clicking it in the network view and clicking Isolation. There is no need to physically “walk” to the endpoint.
2. Open a remote-control session to the isolated device to help you estimate the damage.
3. Deploy any type of software or script to the endpoint. Specifically, this is useful to deploy a one-time antivirus scanner that requires you to download its latest virus definitions from the internet. Endpoint Security for Endpoint Manager allows you to enable access to the internet for specific software while the rest of the device is isolated.

All the above capabilities can be done from one simple view, ensuring faster time to remediation.

A specific icon is shown in the console for each isolated device. The icon represents the EPS client, acknowledging it was able to isolate the endpoint.

How network isolation works

When you select the Isolation option for a device in the network view, a new window opens allowing you to start a remote-control session immediately and select a software package to deploy (a list of software packages is imported from the software distribution settings).
Once you select the desired options and click OK, the core immediately tries to notify the endpoint using the standard push mechanism. If the endpoint cannot be connected directly from the core, such as when the endpoint is connected over a CSA, the core will use another push technique that leverages the remote-control push capabilities to notify the endpoint.

Once the EPS agent is notified, the EPS agent will block any network traffic in/out of the device on all ports except the Endpoint Security for Endpoint Manager and remote control communication ports. This allows the core to continue managing the endpoint once the device is isolated. EPS also allows DNS traffic, ensuring the Ivanti agent can continue to operate. The EPS agent only allows traffic to/from the core/CSA on the specific opened ports, which can only be used to send/receive traffic from the management console.

If you required a software package to be deployed or a remote-control session to start, the relevant agent components are notified so those processes can begin.

If you want to allow a specific process to connect to the internet while the device is isolated from the network, open the EPS agent UI and look for the process. Right-click and select the relevant option.

**IMPORTANT:** The remote-control agent must be installed on the endpoint for the core to push the isolation command to endpoints connecting through CSA.

In addition to the above, you can use the other remediation capabilities of the product once the endpoint is isolated. These capabilities include:

- Remote file view and management (delete remote files).
- Processes view and kill a process.
- Full inventory analysis—understanding which applications were installed on the endpoint, when, and when last run.
- Full remote access to Windows logs.
- Shut down or reboot the endpoint.

If the malicious software was removed from the endpoint, you can "release" the endpoint from isolation. Otherwise, use provisioning to re-image the endpoint.

**Removable storage device handling**

USB connections on managed devices are restricted by a service called the Ivanti Endpoint Security service. When a new volume is mounted, the service receives notification from the operating system. The 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 service will take action. The 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 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 service is installed, the 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 service will consider it a removable device.

You can control removable storage devices in the following ways

- Allow full access
- Allow read-only access
- Force encryption
- No access
- Show a custom message when an unauthorized storage device is blocked.

**Configure Device Control alerts**

Device Control settings use the alert management system for alerting. Device Control can trigger alerts on these events:

- Device Control - Hardware keylogger suspected
- Device Control - Protection override
- Device Control - ShadowCopy oversize file
- Device Control - Unauthorized CD/DVD blocked
- Device Control - Unauthorized device blocked
- Device Control - Unauthorized volume blocked

**To create a Device control alert**

1. Click **Tools > Configuration > Alerting**.
2. In the **Alerts** tree, right-click **LDMS default ruleset** and click **Edit**.
3. Scroll down to the Device Control alerts.
4. Configure the alert actions you want. For more information, see "Alerting basics" (890).

**View the unauthorized device list**

On each computer, Device Control stores a connection and action history for devices that were connected.

You can view this information from the Network view by clicking **Inventory** on a device's shortcut menu. Then click **Security > Device Control**.
Device Control settings help

Use this dialog box to create and edit Device Control settings.

This dialog box 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 the 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 the settings.

About the Storage volumes page

Use this page to specify options for storage volumes that connect to a client configured with this setting.

- **Storage volumes**: Specifies the access level for any storage volume that wasn’t present on the client when the setting was installed. (Note that if a device containing a volume was attached when the setting was installed, the Ivanti Endpoint Security 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 setting. 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 Ivanti Management > Ivanti Encryption Utility). 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 setting. 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.
  - **Allow password hints:** Lets the end user enter a hint that can help them remember the encrypted folder password. The password hint can’t be an exact match to the password itself. The password hint can’t 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 user:** Displays a message box when a user connects an unauthorized storage device. For more information, see “Device Control settings help” (812).

**About the Configure exception (for storage volumes) dialog box**

Use this dialog box 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 the tabs on this page to configure devices, interfaces, and manage exceptions.

**Devices tab**

Select a device, and in the **Access** column, select whether you want to **Allow**, **Block**, or **Always allow** the device.

**Notify end user:** Displays a message box when a user connects an unauthorized device. For more information, see “Device Control settings help” (812).

**Interfaces tab**

Select an interface, and in the **Access** column, select whether you want to **Allow** or **Block** the device.

**Block wireless LAN 802.11X:** Blocks a wireless LAN802.11X connection.

**Notify end user:** Displays a message box when a user connects an unauthorized device. For more information, see “Device Control settings help” (812).

**Exceptions tab**

Use the exceptions tab to configure exceptions for detected devices. An exception allows a specific device to connect even if that device’s class is blocked. Use the filters at the top of the Configure exception window to filter the list. Select the devices you want an exception for, and decide whether you want the exception based on the instance path or hardware ID. Add the selected exceptions by clicking Add to exception list.
About the Shadow copy page

Use this page to enable and configure shadow copy on managed devices configured with this setting.

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 setting.
- **Log events only**: Indicates that only the file copy activity is recorded in a log file, not the actual files that are being copied.
- **Local cache settings**: Specifies the location on the local drive where the shadow copy files and log file are stored.
- **Exceptions**: Click to create exceptions. You can add exceptions based on hardware ID, media serial, or bus type.

About the CD/DVD/Blu-ray page

Use this page to control CD/DVD/Blu-ray connections

- **CD/DVD/Blu-ray drives**: Select the access level you want for these drives. Click **Exceptions** if you want exceptions for specific drives or drive types.
- **Devices / Interfaces**: Use the check boxes to block devices and interfaces from accessing the client.
- **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 device.
LANDESK Antivirus

Ivanti Antivirus overview

Ivanti 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 Agent Settings tool.

**IMPORTANT: Antivirus agent**
The Antivirus agent is distinct from the Patch and Compliance security scanner agent.

Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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 Ivanti Antivirus, you can:

- Download the latest virus definition\pattern file updates (the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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 Ivanti® Endpoint Manager powered by Landesk or Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk, the Patch and Compliance tool is included by default. However, without a Endpoint Security for Endpoint Manager content subscription, you can only scan for Ivanti software updates and custom definitions. A Endpoint Security for Endpoint Manager content subscription enables you to take full advantage of the Patch and Compliance tool (and Agent Settings tool) by providing access to additional security content (definition types), including antivirus scanner detection rules and the actual Ivanti 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" (734))
- Custom vulnerability definitions
- Driver updates
- Ivanti 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 Endpoint Security for Endpoint Manager content subscriptions, contact your Ivanti reseller, or visit the Ivanti website:

Ivanti Home Page

Using Download Updates

Note that the Updates page of the Download updates dialog box includes several antivirus updates in the definition types list, including one named Ivanti Antivirus Updates. When you select Ivanti Antivirus Updates, both the scanner detection content and the Ivanti Antivirus virus definition file updates are downloaded.
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.
NOTE: **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

For up-to-date detailed information on which client platforms support Ivanti Antivirus, see the OS Compatibility Feature Matrix document at the Ivanti User Community:

[Ivanti User Community Home Page](#)

---

### Role-based administration with Ivanti Antivirus

Ivanti 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 box. In order to see and use Antivirus features, a user must be assigned the necessary Security Configurations access rights.

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 Ivanti Antivirus. Each of these procedures are described in detail in subsequent sections.

Basic steps in implementing and using Ivanti 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.

Configure 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.

Considerations regarding Antivirus deployment

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 choose to automatically remove existing antivirus software from target devices when deploying Ivanti Antivirus, either during initial agent configuration or as a separate Antivirus install/update task.

IMPORTANT: Clear password protected antivirus software

If the existing antivirus software product is password protected, you must first clear the password before Ivanti Antivirus can uninstall the software.
Configure 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 Ivanti Antivirus option. Now you can access the options on the Ivanti Antivirus page.
4. Click the Security and Compliance group, and then click Ivanti Antivirus.
5. If you want to automatically remove an existing antivirus product from target devices, select the Remove existing antivirus agent option.
6. Select an antivirus setting from the available list to apply it to the agent configuration you’re creating. You can create new settings or edit 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 settings for the agent configuration and then click Save.

You can also configure devices for Antivirus with the Security Configurations tool.

Use 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 and Compliance> Agent settings) 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 and compliance > Agent settings.
2. Click the Create a task toolbar button, and then click Install/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 Ivanti Antivirus. You can select an antivirus setting from the available list to apply it to the task you’re creating. You can also create new settings or edit existing antivirus settings.
6. If you want to display the installation progress in the security scanner dialog on target devices, select the Show progress dialog on client option.
7. If you want to automatically remove an existing antivirus product from target devices, select the Remove existing antivirus agent option.
8. Select a scan and repair setting from the available list to apply its reboot configuration to the task you’re creating. You can create new settings or edit 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 targeted devices during Antivirus agent installation.
9. Click OK.

Update virus definition files

Antivirus lets you download the most current virus definition files from the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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. They can be 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 box directly when creating an Antivirus task.
NOTE: 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 Ivanti 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content server via an Internet connection.
To download virus definition file updates

1. Click **Tools > Security and Compliance > Agent settings**.
2. Click the **Download updates** toolbar button. The dialog box opens to the **Antivirus** page. (You can also access the **Download updates** dialog box 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk 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, select the **Put new definitions in the Unassigned group** check box.
7. Now click **Ivanti 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 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 box 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, select the **Make backups** option. You can restore definition file backups at any time. 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.

**IMPORTANT:** 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 scheduled tasks 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 box, making sure to select Ivanti Antivirus updates in the definition type list on the Updates tab, configure virus definition file options on the Ivanti Antivirus tab, and then click the Schedule Update button. The Scheduled update information dialog box 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.

**NOTE: 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 box 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.

**Enable 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.

**NOTE: Ivanti Antivirus system tray icon indicator**

When real-time antivirus protection is enabled, the Ivanti 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 box. 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 box.

Real-time email protection provides an ongoing scan of incoming and outgoing messages. Antivirus scans the message body as well as attached messages’ 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
- A 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 box.

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

### Configure antivirus scan options with antivirus settings

Antivirus gives you complete control over how antivirus scans run on targeted 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, and so on. 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
- Specifying 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 **Ivanti Antivirus** group in the **Agent settings** 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.

To create antivirus settings

1. In the Agent settings tool, right-click the Ivanti Antivirus object, and then click New.
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 setting associated or assigned to it, the default settings are overridden. You can also choose to use the device's default setting 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 box that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select existing antivirus settings as the default or use the Edit button to create 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 > Ivanti Management > AV Settings.

Configuring which files to scan (infectable files only, exclusions, heuristics, riskware)

You can specify which files (items) you want to scan and 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" (828)
- "Excluding items from antivirus scans and real-time protection" (830)
- "Using heuristic analysis to scan for suspicious objects" (831)
- "Scanning for riskware (extended database)" (831)

All files or infectable files only

You can scan all files or infectable files only on the Virus scan and Real-time protection pages of 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
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 antivirus settings.

NOTE: 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 Ivanti Antivirus. This feature is called the trusted items list, and is configured on the General page of 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 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.

Examples of riskware include 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 choose 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 Ivanti Antivirus icon in the system tray** option is selected 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 scan 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.

1. The infected object is 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 (the user that is logged in when the infected file is discovered) is allowed to delete or modify backup files.

**Evaluate 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 restricting virus definition file updates to a pilot test folder, and then applying 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 Ivanti Antivirus tab, click Restrict them to a pilot test first.
2. If you don’t want to manually move tested virus definition files from the pilot test folder to the default folder (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8), click Schedule approval to create a scheduled task that specifies a time to approve the pilot test files. Fill in the fields in the task that appears in the Scheduled tasks tool. When the specified time arrives, the virus definition files are automatically approved and moved.
3. To download the most recent virus definition files from the Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content server, click Get latest definitions.

4. To immediately approve the virus definition files currently residing in the pilot test folder, click Approve now. This moves the virus definition files from the pilot test folder to the default folder (\LANDesk\ManagementSuite\dlogon\antivirus8\win\bases8).

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 the 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.

Scan devices for viruses

This section provides information on scanning managed devices for known viruses as well as suspicious objects.

IMPORTANT: 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 Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk content subscription. For information about content subscriptions, contact your Ivanti reseller, or visit the Ivanti website:

Ivanti Home Page

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

Run 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.

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 **Ivanti 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 target all devices. You can also start the antivirus scan of all devices immediately.

9. If you want to ensure that the scan uses the latest known virus definition files, select the **Update virus definitions** option.

10. Select an antivirus setting from the available list (or create a custom setting for this scan by clicking the **Configure** button), to specify 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 list. For more information about configuring the antivirus scan with antivirus settings, see “About the Ivanti Antivirus settings dialog box” (226).

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.)

**Run 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 **Ivanti 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

**Run 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 **Ivanti Antivirus** taskbar icon, and then select **Scan my computer**. Or from the Antivirus dialog box, click **Scan my computer**.

**Back up virus definition files**

If you want to save older versions of downloaded virus definition files, use the **Virus definition backups** settings on the **Ivanti 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.

**Configure 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 Ivanti 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 box.

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 view. Right-click a device, select Security Information, select the Antivirus type in the Type drop-down list, and then select the Antivirus History object.

**Generate 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 Ivanti Administrator right (implying full rights) or the specific Reporting roles.

For more information about using the Reports tool, see "Using reports" (381).

**Viewing antivirus information in the Executive Dashboard**

You can also view antivirus scan information in the Ivanti web console Executive Dashboard. This data is useful in identifying virus outbreaks and to show antivirus protection over time.

Ivanti 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

**Remove Ivanti Antivirus from devices**

If you want to remove Antivirus from managed devices, you can also do that as a separate task.

**To remove Ivanti Antivirus**

1. In the console, click **Tools > Security and Compliance > Agent settings**.
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 targeted devices, select the **Show progress dialog on client** option.
6. Select a scan and repair setting from the available list to apply its reboot configuration to the task you’re creating. You can create new settings or edit 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**.
FIPS

About FIPS 140-2 support

The Federal Information Processing Standard (FIPS) 140-2 is a US government security standard that defines an allowable set of cryptographic functions. Ivanti® Endpoint Manager powered by Landesk doesn’t use its FIPS 140-2 mode by default, but you can enable it. FIPS 140-2 support in Endpoint Manager encrypts communication from managed Windows devices through the CSA to the core server. The encryption method is FIPS-enabled SSL.

FIPS support requires Endpoint Manager Version 9.5 SP1 or later and a Ivanti Cloud Services Appliance with Gateway service version 4.3 or later.

The Endpoint Manager components that support FIPS 140-2 are:

- The broker service on the core server. This service handles communication with the CSA.
- The remote control viewer, both HTML and legacy.
- The broker daemon on the CSA.
- Proxyhost.exe on the device. This process handles general Endpoint Manager agent communication.
- The remote control agent on the device.

No other components in the system are FIPS-enabled, such as the console, roll-up core, and so on.

You’ll need to do the following steps to enable FIPS 140-2. Each step is described in more detail later on.

1. On the CSA, enable FIPS mode.
2. On the core server’s LDMS console, enable FIPS mode.
3. Roll out the Endpoint Manager agents on Windows devices with an agent configuration that uses the CSA and FIPS.

Enabling FIPS on the CSA

To enable FIPS on the CSA, you must either use the built-in CSA console or use the CSA Web interface, available from http://<CSA IP address or name>/gsb. The default CSA username is admin, and the password is whatever it was changed to during CSA installation.

To enable FIPS on the CSA

4. Directly on the CSA or using the CSA Web management interface, log in and click the Gateway service button on the left side.
5. Change the Server FIPS 140-2 mode option to 1.
6. Click **Save**.

**Enabling FIPS on the core server**

Enabling FIPS on the core server generates new security certificates. **This means that you won’t be able to manage existing clients until you redeploys updated agents that include the new certificates.** You won’t be able to just do an agent update either, because of the client/core certificate mismatch. If you need FIPS 142, we generally recommend that you enable it at the beginning of an Endpoint Manager deployment.

When you enable FIPS, the core server rebuilds all agent configurations so that they include the new security certificate. This takes a few minutes. If you have a lot of agent configurations, it will take longer.

The old core certificate is backed up here. The folder name includes the backup date.

```
C:\Program Files\LANDesk\Shared Files\Keys\Backup (<backup date and time>)
```

If you disable FIPS after enabling it, and later re-enable FIPS, the core will reuse the certificate you created the first time you enabled FIPS. In this case you wouldn’t have to redeploy agent configurations a second time.

**To enable FIPS on the core server**

1. On the core server, open the Ivanti Management Console.
2. Click **Configure > Services**.
3. On the **General** tab, select **FIPS 140-2 is enabled for this core server**.
4. Carefully read the confirmation dialog box reminding you that you won’t be able to manage clients until you update their agent configurations. If you’re sure you’re ready, click **Yes**.

**Updating FIPS agent configurations on Windows devices**

Once the core server finishes rebuilding agent configurations with the new security certificate, edit your Windows agent configurations and make sure they’re using your FIPS-enabled CSA. After that, you’ll need to redeploy agents to all of your managed devices, including non-Windows devices.

**To select the CSA used by an agent configuration**

1. Click **Tools > Configuration > Agent configuration**.
2. On the **Client connectivity** page, click **Configure**.
3. Select an existing setting and click **Edit** or create a new one.
4. On the **Cloud Services Appliance** page, select **Enable cloud Services Appliance communication** and select the CSA you want this client connectivity setting to use.
5. Click **Save** and then click **Close**.
6. On the **Client Connectivity** page, make sure the client connectivity setting you configured is selected.
17. Deploy the updated agent to managed devices.

**Verifying FIPS 140-2 mode is working**

You can verify FIPS 140-2 mode is active by checking log files on the core server, CSA, and managed Windows devices.

On the core server, check the BrokerService.exe log file, which tracks communication between the core and the CSA. Look for **FIPS Mode: 1** entries, which indicate FIPS is enabled. A value of 0 means it's disabled.

C:\Program Files\LANDesk\ManagementSuite\log\BrokerService.log

On managed Windows devices, check the ProxyHost.exe log file, which tracks communication between the managed device and the CSA. Look for **FIPS Mode: 1** entries, which indicate FIPS is enabled.

C:\Program Files\LANDesk\LDClient\proxyhost.log

Also, on managed Windows devices check the Ivanti Remote Control agent status by double-clicking it in the system tray. At the bottom of the dialog box, **FIPS 140-2 mode enabled** appears if FIPS 140-2 is enabled.

On the CSA, check /var/log/messages.
Power management

Ivanti® Power Manager overview

The Ivanti 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.

How it works

The Ivanti agent that is deployed to every managed device includes a power management option. When you choose to deploy a power management policy to a device, it is enabled as part of the agent.

You define policies based on the specific needs of different types of managed devices. You can then deploy the policies to groups of devices in your organization. For example, you would define one policy for servers that need to be running continuously and a different policy for desktops that are typically not in use overnight and on weekends.

![Power management configuration interface](image)

Each policy contains one or more power schemes, which are specific rules for power-related actions. Each scheme applies to one device type during a specified time. For example, you can
- Apply standby or hibernate rules that are in effect for a desktop or laptop during hours of regular use
- Define schemes for monitors to turn off after a period of inactivity
- Define schemes to automatically power devices during certain hours

If a user is working on a computer when the policy would normally shut it off, a client interface notifies the user, who can delay the shutdown as needed.

**Power management toolbar buttons**

The power management tool includes a set of tool buttons that allow you to complete various power management tasks.

<table>
<thead>
<tr>
<th>Power management</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Delete" /> Delete: Deletes the selected power management policy.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /> Refresh: Refreshes the items displayed in the left pane.</td>
</tr>
<tr>
<td><img src="image" alt="Schedule" /> Schedule: Click to schedule the deployment of the selected power management policy.</td>
</tr>
<tr>
<td><img src="image" alt="Reporting" /> 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. You can also run a report that shows the power and cost savings across a specified time interval.</td>
</tr>
<tr>
<td><img src="image" alt="Historical data" /> Historical data: Click to collect client usage information for more accurate estimation of power usage.</td>
</tr>
<tr>
<td><img src="image" alt="Customize" /> Customize: Lets you customize the settings that define overall power usage for specific manufacturers and computer models.</td>
</tr>
<tr>
<td><img src="image" alt="Application management" /> Application management: Lets you manage processes that may be running when a power policy is applied.</td>
</tr>
</tbody>
</table>

**Create a power management policy**

Power management uses policy-based management to send stand by, hibernate, shut down, and turn on instructions to your managed computers. Power management policies enable you to control specific computers and groups of computers.

To create a new power management policy, use the [Power management dialog](#).

**Tools > Security and Compliance > Agent Settings > Power Management > Power Management settings**
Deploy a power management policy

After you create a policy, you must schedule it to run on a managed device or a group of devices. After the task is successfully completed, the Ivanti agent on the target devices includes the power policy and uses the power schemes in the policy.

To deploy a power management policy

1. Click **Tools > Power management > Power management**.
2. Click a policies folder in the tree view and select the policy.
3. Click the **Schedule** button on the toolbar and select **Schedule policy**.

   The **Scheduled tasks** tool opens with the power policy selected.
4. Drag a device or group from the network view onto the policy.
5. Right-click the policy and click **Start now**.
6. To start the task at another time, select the policy, click the **Properties** button on the toolbar, and specify the time to start the policy task.

The tasks status panes show which devices have successfully completed the task. If the task can't be completed on any devices, the reason for the failure is shown.

**NOTE:** The Ivanti agent on targeted devices must have power management enabled for a power policy to function. If you deploy a policy and receive an error that the policy task can't be launched on a device, make sure that the device's agent has power management enabled.

Remove a power management policy

You can remove power management policies from all managed devices or from groups of devices. This is done by creating a scheduled task that is applied to all devices. After the task is successfully completed, the Ivanti agent on the target devices no longer includes the power policy.

To remove a power management policy

1. Click **Tools > Power management > Power management**.
2. Click the **Schedule** button on the toolbar and select a **Turn power management off** option.

   If you select the global option, power management is removed from all managed devices.

   If you select the group option, select the device group or query for which you want to remove power management, and then click **OK**.
3. In the Scheduled tasks tool, right-click the **Turn power management off** task and click **Start now**.

4. To start the task at another time, select the task, click the **Properties** button on the toolbar, and specify the time to start the removal task.

The tasks status panes show which devices have successfully completed the task. If the task can’t be completed on any devices, the reason for the failure is shown.

**Customize wattage settings**

The Power Management tool includes a utility that lets you customize the wattage settings for similar computers for more accurate power management reporting. The settings that you select and create in this dialog box are used in report calculations.

![Custom wattage settings dialog box](image)

**Default settings**

The default settings displayed in the **Custom wattage settings** dialog box are based on the type of computer referenced in a report.
For a desktop computer, default wattage settings are based on the average settings of a typical desktop computer. For laptop computers, the default settings are lower because laptops typically use less power.

**To change the default wattage settings**

1. Click **Tools > Power management > Power management**.
2. On the toolbar, click the **Customize** button (⚠️) and select **Custom wattage settings**.
3. Select the **Chassis type** (Desktop or Laptop).
4. In the fields under **Computer**, change the wattage settings to specify wattage used by the chassis type you selected, in different usage states.
5. In the fields under **Monitor**, change the wattage settings to specify wattage used by the monitor when on full power and on standby.

**Custom settings for specific models**

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 an Ivanti inventory of an Inspiron 531s computer.

**To add wattage settings for specific hardware models**

1. Click **Tools > Power management > Power management**.
2. On the toolbar, click the **Customize** button (⚠️) and select **Custom wattage settings**.
3. Clear the **Default settings** check box.
4. Select the **Manufacturer** and **Model** for the device type you want to use.
5. Click **Close** to save the data for that model.
6. Repeat steps 2-4 for each model you want to include in power usage calculations.

The wattage settings you save are matched to managed devices that you include in reports.

**Custom settings for other models**

When the **Default settings** check box is selected, the wattage settings fields display the average power usage of a typical desktop or laptop computer. When the **Default settings** check box is cleared, use these fields to enter power usage settings for specific computer brands and models that aren't in the manufacturer and model lists.
To add custom wattage settings for other hardware models

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. For accuracy, you’ll need to gather the usage information from the manufacturer’s sources.

1. Click Tools > Power management > Power management.
2. On the toolbar, click the Customize button (⚠️) and select Custom wattage settings.
3. Clear the Default settings check box.
4. Type the Manufacturer name and the Model name/number for the device type you want to use.
5. Select the Chassis type that matches the device.
6. Add wattage data for the computer and monitor in different usage states.
7. Click Close to save the data for that model.

Schedule a remote wakeup

Power management schedules a “turn on” command through a device's BIOS. If the BIOS can’t schedule wake up events, or can’t schedule them through Windows, then the “turn on” event will not be scheduled. When this happens, there are several possible ways to resolve the problem:

- Enable plug and play events in the BIOS
- Enable events in the BIOS
- Update the manufacturer BIOS

Some BIOSes don’t support this feature at all. In that situation, a scheduled task for Wake on LAN can be used to power on devices at a specific time.

If a managed device is configured to use Wake on LAN (WOL) or Intel vPro wake up, you can schedule a remote wakeup to power on the device at a specific time. This feature wakes devices that are in standby or hibernate mode as well as devices that are powered off.

If both WOL and Intel vPro wake up are enabled, the Intel vPro feature is run first and WOL is run second.

To schedule a remote wakeup

1. Click Tools > Power management > Power management.
2. Click the Schedule button on the toolbar and select Schedule remote wakeup.

   The Scheduled tasks tool opens with the task selected.
3. Drag a device or group from the network view onto the task.
4. Right-click the task and click Start now.
5. To start the task at another time, select the task, click the **Properties** button on the toolbar, and specify the time to start the task.

The tasks status panes show which devices have successfully completed the task. If the task can’t be completed on any devices, the reason for the failure is shown.

**Managing applications that conflict with power policies**

Applications running on managed devices can conflict with the power management policies you create. Some applications must be allowed to continue running even if the policy has a shut-down command for the device. Other applications should not interfere with the policy and need to be terminated as part of the shutdown process.

The power management alert log helps you identify which processes running on managed devices can conflict with power policies. These conflicts are logged with the device name, time, and process name. Review these log entries to determine which applications are causing conflicts.

The **Application management** button ( ) on the power management toolbar includes three options that let you manage potential conflicts with applications:

- **Identify process-sensitive triggers**: The processes that you include in this list will be allowed to run even if the power policy has a shutdown command. The power policy will wait until the processes have terminated and will then continue to enforce the policy.

- **Identify processes to terminate at shutdown**: The processes that you include in this list may interfere with the power policy, causing a state of “insomnia” (inability for the device to shut down or standby). If these processes are running, the power policy will terminate them so it can continue.

- **Identify processes to ignore**: The processes that you include in this list do not need attention from the power policy and don’t need to be included in alert logs.

Instructions for using these options are found in the following topics:

"Configure applications that should not be shut down" (848)

"Configure applications that should be shut down" (849)

"Configure applications to ignore in alert logs" (850)

**Configure applications that should not be shut down**

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 Endpoint Security for Endpoint Manager 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.

**To identify applications that should not be shut down**

1. Click **Tools > Power management > Power management**.
2. Click the **Application management** button on the toolbar and select **Identify process-sensitive triggers**.
3. Add, modify, or delete process names to the list.
4. When the list is complete, click **OK**.

![NOTE: The list you create here will only apply to a managed device if you have enabled the process-sensitive trigger option in the power management policy for that device.]

**Click here for descriptions of options in the Process sensitive trigger list dialog box**

- **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 **Historical data** information. This includes processes that are listed in the power management alert log.
- **Delete**: Removes the selected process from this list.
- **Modify**: Click this button to change the name of the .exe file.
- **All**: Selects all the processes in the list.
- **None**: Clears all the processes in the list.

**Configure applications that should be shut down**

Use the **Identify processes to terminate at shutdown** toolbar button to stop processes that can delay a power policy option. 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 that prevent the device from going into standby or shutting down.

**To identify applications that should be terminated as part of a shutdown**

1. Click **Tools > Power management > Power management**.
2. Click the **Application management** button on the toolbar and select **Identify processes to terminate at shutdown**.
3. Add, modify, or delete process names to the list.
4. When the list is complete, click **OK**.
NOTE: The list you create here will only apply to a managed device if you have enabled the end process list option in the power management policy for that device.

Click here for descriptions of options in the End process list dialog box

- **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 **Historical data** info. This includes processes that are listed in the power management alert log.
- **Delete**: Removes the selected process from this list.
- **Modify**: Click this button to change the name of the .exe file.
- **All**: Selects all the processes in the list.
- **None**: Clears all the processes in the list.

Configure applications to ignore in alert logs

Use the **Identify processes to ignore in exception logs** toolbar button to designate processes that do not need attention from the power policy. Adding processes to this list can reduce the size of log files related to power management, which helps you focus on the applications that are of interest in monitoring problems with power management.

To identify applications that can be ignored in alert logs

1. Click **Tools > Power management > Power management**.
2. Click the **Application management** button on the toolbar and select **Identify processes to ignore in exception logs**.
3. Add, modify, or delete process names to the list.
4. When the list is complete, click **OK**.

Click here for descriptions of options in the Processes to ignore dialog box

- **Add**: Adds a process that is a known .exe that can be ignored.
- **Import**: Adds a process from information gathered from the client machines using **Historical data** info. This includes processes that are listed in the power management alert log.
- **Delete**: Removes the selected process from this list.
- **Modify**: Click this button to change the name of the .exe file.

Viewing power management reports

The power management tool allows you to generate and view power, cost savings, and historical reports. Reports are made up of composite calculations of either wattage or cost savings. They are based on estimated costs of power and an average of active use on the selected computers that you associate with a report.

There are two types of savings reports:
• **Wattage**: compares the number of kWh (kilowatt hours) used when power management policies are in effect with the number used if no power management policy is in effect.

• **Money Savings**: creates an estimate of the cost savings gained when power management policies are in effect.

Savings can be calculated by day, week, month, or year. If you have collected historical data, you can run historical reports of the same types.

### How reports are created

Power management processes on managed devices track the time that each device is in active use. Reports are created from an XML file that gathers the usage information and calculates an average length of time that computers are in use.

Each time you run a report, you select individual devices or groups of devices. The report then gathers data for those devices and presents a summary of usage. The hours in use are multiplied either by average wattage for the device type (wattage reports) or the estimated cost savings of keeping the device powered down (money savings reports).

The following elements contribute to the calculations in reports. You can modify any of these elements to make reports more accurate for your situation.

• **Cost per kWh**: a standard average is used as the default. If you know the actual cost per kWh for your electrical billing, change this figure.

• **Custom wattage settings**: by default, reports use the average wattage settings for desktops and laptops. If you want to use more specific data you can use data for certain manufacturers and models.

• **Client usage data**: by default, an average of daily client usage is used for calculations. If you want to use more specific data you can apply historical data taken from your managed devices for report calculations.

When you run a savings report, use the **Savings report** dialog to select options and preview the results.
Run a power management report

Use the Reporting button on the power management toolbar to run savings and historical reports.

NOTE: Reports require that you first create computer groups with at least one device or queries, in the network view. You’ll use groups and queries to select the devices that are included in reports.

To run a power management report

1. Click Tools > Power management > Power management.
2. Click the Reporting button on the toolbar and select Savings report or Historical report.
3. Select a policy name from the drop-down menu, then click Select targets. Select groups or queries for the devices you want to include in the report. Click OK.

The items you select are listed, with an associated cost per kWh. The total number of machines in the groups is also displayed.
4. If you want to calculate using a different cost per kWh, change the number in the Cost per kWh field. To remove a group or query from the report, click its Delete button. Click Refresh report to update the graph after you make any changes.
5. Select a graph type (wattage or money savings).
6. Select the currency symbol that you want the report to display.
7. Under the graph, select the time frame for the report (from 1 day to 1 year).
8. To export a copy of the report in .htm format, click Export and specify a location to save the file.

NOTE: To run a historical report, you must first have collected historical data for managed devices (using the Historical data toolbar button). If you have no historical data, the report won’t create a graph and won’t export a report file.

Use historical data for power reports

You can collect power usage data for managed devices if you want to create reports that represent actual device usage over a period of time. Data is stored in the database and is then used when you run a report that includes the devices from which you collect data.

Use the Historical data toolbar button to start and stop data collection or to delete data from the database.

After you have collected client usage data, you can replace the default client usage data with actual historical data gathered from your managed devices.

To replace usage assumptions with historical data

1. On the Power management toolbar, click the Customize button and select Replace client usage assumptions with historical data.
2. Select the groups or queries from which you want to use historical data.
3. Select a time period, either the latest week of data or a period of time.
4. Click Generate default usage table.

The new data is used to generate reports. It replaces the average usage data that is used by default to estimate usage savings.

Related topics

Instructions for using historical data options are found in the following topics:

"Collect client usage data" (853)

"Delete old client usage data" (854)

Collect client usage data

To collect client usage data

1. Click Tools > Power management > Power management.
2. Click the Historical data button on the toolbar and select an action (Start collecting the client usage info or Stop collecting the client usage info).

A task opens in the Scheduled tasks window, identified with the date and time.
3. Drag individual devices, groups, or queries from the network view onto the task.
4. To start the task now, right-click it and select Start now.
5. To schedule the task to begin at a later time, select the task and click the Properties button on the Scheduled tasks toolbar. Click Schedule task > Start later and select scheduling options.

The two panes in the Scheduled tasks tool show the progress of the task, including which devices could not complete the task and why.

### Delete old client usage data

**To delete old client usage data from the database**

After you have collected data over a period of time and then have used that data to run reports, you may want to delete the old data from the database. This ensures that historical data is recent.

1. Click Tools > Power management > Power management.
2. Click the Historical data button on the toolbar and select Delete old client usage data.
3. Specify a date and click Delete.

Historical power consumption and usage information prior to the specified date is deleted from the database.

### Generate an XML file for default usage calculations

Power management reports use average data for different types of computers (desktop, notebook, or laptop). When you generate a report for a group of computers, the computers in that group are matched with the average wattage data for corresponding computer types. Data is therefore based on an average but not on specific usage.

An XML file contains this average data. If you have collected historical data from your managed devices, you can generate a new XML file that uses data from your own managed devices rather than from averages. This XML file replaces the default file and thus reflects the power usage in your organization and provides more accurate savings reports.
To generate a new XML file for default usage calculations

1. Click **Tools > Power management > Power management**.
2. On the toolbar, click the **Customize button** and select **Replace client usage assumptions with historical data**.
3. Select the device groups or queries that you want to use to calculate data.
4. Select the time period from which you want to calculate new data. You can choose the latest week or specify a period of time.
5. Click **Generate default usage table**.

A new XML file is created. The data in this file will be used in savings report calculations.

**NOTE:** To generate a new XML file, you must have collected historical data from managed devices for at least the time period that you select in this dialog box. If there is not sufficient historical data, you won't be able to generate a new XML file.

**View the power management alert log**

As power management policies run on managed devices, there can be situations in which devices don't respond to power actions as expected. For example, a process running on a device may continue to run even when a command to change power states is sent to the device.
The alert log lists the details of such conflicts. You can use the information in this log to manage applications on devices, specifying which applications should be allowed to continue running or should be shut down when a power action is scheduled to run.

To view the power management alert log

1. Click **Tools > Power management > Power management**.
2. Click the **Alert log** node in the tree view.
3. To find alerts for a specific device, or for a date range, type a search string in the **Find** box and select a column, or select a date range, and click the **Search** button.

When you have identified processes that create conflicts, use the **Application management** options on the toolbar to change how the power policy runs when certain applications are running on a device. For more information, see "Managing applications that conflict with power policies" (848).
Mobility Manager

Welcome to Ivanti Mobility Manager

Ivanti® Mobility Manager helps you take control of the mobile devices used in your company. It simplifies device provisioning, helps enforce corporate policies, and allows an administrator to lock or wipe lost or stolen devices.

Ivanti® Mobility Manager adds these tools to the Endpoint Manager console:

- **Android and iOS agents:** Allows you to manage Android and iOS devices, remotely lock, unlock, or wipe them, or configure device settings.

- **Mobile inventory:** An addition to your inventory that lists mobile devices that are under management or, if you set up the connection to an Exchange server, devices that have connected to your Exchange server.

- **Mobile software packages:** Distribute apps to mobile devices from a web server, or from the Google Play Store or Apple App Store.

In addition to these tools, there are certain tasks added to the console that can be performed using your Microsoft Exchange Server (EAS 2007 or 2010):

- Discover devices. Configure your server to report a list of devices that have connected. Use the list of discovered devices to determine devices that need to be under management.

- Wipe devices. Use a command sent through the EAS to wipe a device that connects to your server. This wipe is a factory reset.

- Create connection rules (Exchange 2010 only). Connection rules determine which device types can access mailboxes.

Mobility Manager is installed by default with the Endpoint Manager core server. However, you must perform some tasks to set up the notification services. For information on getting started, see the following sections:

- "Get started with Mobility Manager" (858)
- "Device tasks" (875)
- "Use Mobility Manager with an Exchange server" (883)

**Mobility Manager components and traffic**

By default, Mobility Manager is installed with Endpoint Manager 10.0.

The diagram below shows the components that interact when you use Mobility Manager.
1: Android or iOS devices, 2: GCM (Google Cloud Messaging for Android) or APNS (Apple Push Notification) services, 3: firewall, 4: Ivanti Cloud Services Appliance (CSA), 5: LDMS 10.0 core server with Ivanti Mobility Manager Services.

Devices connect to the Ivanti® Endpoint Manager powered by Landesk core server through a Ivanti Cloud Services Appliance (CSA). When you send profiles or commands to the devices, the traffic is sent to the devices using the appropriate protocol (GCM for Android devices or APNS for iOS devices).

You MUST have a CSA in order to manage Android and iOS devices.

**Get started with Mobility Manager**

When you enroll mobile devices in Mobility Manager, you can perform actions to manage them, and also send software and configurations to the devices. Agent settings allow you to deploy software, certificates, Exchange settings, and Wi-Fi credentials to devices. You can also require a passcode on the device or restrict what can be used on the device.

---

**IMPORTANT:** To manage mobile devices, you MUST have a CSA installed and configured, and you MUST configure a connection between Mobility Manager and an LDAP server.

---

To manage devices using Mobility Manager, perform the following tasks:

1. **Make sure your CSA is configured in the console.** To check, click **Configure > Manage Cloud Services Appliances**. If the connection to the CSA is configured, it appears in the list.

2. **Make sure the core can connect to your LDAP server.** To check, click **Configure > Manage Active Directory Sources**. If the connection to Active Directory is configured, it appears in the list.

3. **(Recommended) Add DNS TXT records to allow mobile devices to resolve the address of the CSA.** For more information, see "Add DNS TXT records" (859). If you do not add the TXT record, you may consider taking other steps to prevent users from typing in a long URL on their devices when they enroll, such as using a URL shortener.

4. **Set up credentials for using Google Cloud Messaging and Apple Push Notification services.** For more information, see "Set up notification services" (860).
5. **(Recommended) Get a certificate for signing iOS profiles.** If you don't sign the profiles with a certificate from a certificate authority, the user is warned that the profile is not trusted when he attempts to enroll his device. For information on setting up a certificate to sign iOS profiles, see "Set up iOS profile certificates" on page 863.

6. **(Optional) Set up a Google Apps account for Chromebook management.** For information on the steps to make Chromebooks appear in the inventory, see "Manage Chromebooks" (869).

7. **Create agent settings to configure the devices.** Agent settings for mobile devices include: "Agent settings: Exchange/Office 365" (292), "Agent settings: Mobile Connectivity" (295), and "Agent settings: Mobile Security" (297).

8. **Create software packages for the devices.** For information on creating software packages, see "Distribute content to mobile devices" on page 878.

9. **Enroll devices.** Using the Mobility Manager, you can enroll mobile devices as well as iMacs and Macbooks. After devices are enrolled, they appear in the inventory and you can perform actions such as wipe or locate.

You can create agent settings and software packages for devices after they have been enrolled. The other configuration tasks should be completed before you begin enrolling devices.

In most situations, an administrator doesn't need to change settings for how frequently devices check in. However, if you are in a testing environment or you notice performance issues with the CSA, you may want to make changes to how mobile devices check in. For more information, see "Configure check-ins" on page 865.

**NOTE:** Mobility Manager offers limited features through your Exchange/ActiveSync (EAS) server, if you set it up. This allows you to view the devices that connect to the EAS server, send a remote wipe to devices, and configure the EAS connection rules from the Endpoint Manager console. For more information about setting up Mobility Manager with the EAS server, see "Use Mobility Manager with an Exchange server" on page 883. If you ONLY want EAS features, you do not need to set up the CSA, DNS TXT records, credentials for notification services, or the certificate for signing iOS profiles.

### Add DNS TXT records

We recommend that you add DNS TXT records to allow mobile devices to resolve the address of the CSA. This makes the enrollment process much easier for users. The following scenarios show the differences in the enrollment process with or without the TXT records.

**When the TXT records exist**

1. Download and install the Ivanti agent.
2. Open the agent and type in a corporate email address and password.

The agent uses the email address to determine where to send the DNS query. The TXT record provides the URL to the CSA and the mobility endpoint, which the agent uses to enroll the device.
**When the TXT records do not exist**

1. Download and install the Ivanti agent.
2. Open the agent and type in a corporate email address and password.
   
   The agent attempts to determine the URL to the CSA.
3. When it fails, the device user is prompted to type in the URL to the CSA, including the name of the core. The agent connects to the CSA and enrolls the device.

Since the URL may be long and complicated (see below), the extra step may introduce errors and cause support calls. If you do not add the TXT record, you may consider taking other steps to prevent users from typing in a long URL on their devices when they enroll, such as using a URL shortener.

**To create the DNS TXT record**

Create one record for Android devices and one record for iOS devices. Use the following patterns:

- **android-enroll**=https://[fully qualified public name of the CSA]/rtc/[core name]/MDM/api/v1/enroll/AndroidEnroll
- **iOS-enroll**=https://[fully qualified public name of the CSA]/rtc/[core name]/MDM/api/v1/enroll/IosEnroll

For example:

- **android-enroll**=https://mbroker2.landesk.com/rtc/slc-core-mdm27/MDM/api/v1/enroll/AndroidEnroll

**Set up notification services**

To manage Android and iOS devices, you must set up notification services.

- Android devices use Google Cloud Messaging (GCM), which requires you to have a Gmail account, project ID, and API key.
- iOS devices use Apple Push Notification Service (APNS), which requires you to have a APNS certificate.
- Windows 10 devices use Windows Push Notification Services (WNS), which requires you to have a Windows developer account.

We do what we can to make this easier, but Ivanti cannot provide, submit, or obtain these credentials for or on behalf of your organization. Once you have created the credentials, enter them in the console.

**IMPORTANT:** The APNS certificate expires after a year. You must replace the certificate before it expires, or else you will be required to re-enroll iOS devices.
To set up GCM credentials

1. Make sure you have a Gmail account.
2. Log in to the Google Developers Console website:
   https://cloud.google.com/console
3. Click **Create Project**.
4. Enter a project name and click **Create**.
   A page appears that displays the project ID. Write down the project ID.
5. On the left, click **APIs & auth > APIs**.
6. Click **Cloud Messaging for Android** under Mobile APIs.
7. Click **Enable API** at the top of the screen.
8. Navigate to **APIs & auth > Credentials**.
9. Click **Add credentials**.
10. Click **Server key**.
11. Provide a name to help you identify the server key.
12. (Optional) Leave the IP address blank. Not specifying an address allows the API key to function for any server regardless of its IP address.
13. Click **Create**.
   The page refreshes with the generated server API key. Write down the API key.
14. From the Endpoint Manager console, click **Configure > Device Discovery**.
15. Select the Mobility page from the navigation on the left.
16. In the Android Notification Settings section, enter the **Google Project Number** and **Server API Key** you received in the Google Developers Console.
17. If users must have the Android for Work agent installed, select the **Require Android for Work Agent** and set a **Remind Later Delay** time. When a user unlocks their device and the delay time has elapsed, they'll be prompted to install the Android for Work agent.
18. Make sure that the **Mobility CSA** option is set to the correct CSA.
19. Click **OK**.

To set up an APNS certificate

1. Make sure you have an Apple ID to create the certificate with.
3. Click **Start**.
4. Perform the steps indicated to create a private key and certificate.
5. Click **Next**.
6. Perform the steps indicated to upload the certificate and download an Ivanti-signed certificate.
7. Open another browser tab and navigate to https://identity.apple.com/pushcert
8. Enter your Apple ID and password to sign in.
9. Select **Create a certificate**.
10. From the Create a New Push Certificate page, browse and upload your signed certificate file.
    The Apple Push Certificates Portal appears with the status confirmation.
11. Click **Continue**.
12. Click **Download**.
    The MDM_ LANDSK Software, Inc_Certificate.pem certificate downloads.
13. From the apnsportal.wavelink.com browser tab, click **Next**.
14. Perform the steps indicated to export the signed certificate to PKCS #12 format.
15. From the Endpoint Manager console, click **Configure > Device Discovery > Mobility**.
16. In the iOS Notification Settings section, click **Browse and browse to the certificate file**.
17. Provide the password to the certificate in the **Certificate Password** text box.
18. Make sure that the **Mobility CSA** option is set to the correct CSA.
19. Click **OK**.

**To set up WNS**

1. Make sure you have a **Windows Developer account**. If you don't, there is a one-time cost of $15 associated with creating an account.
2. Sign in to your account and click on the Dashboard link.
3. Click **Create a new app**. This launches a page for reserving a product name. You'll be creating a dummy app here, so set an app name of any value. The process of creating this app is to establish WNS settings. The app itself will not be built or shipped. Once the app is successfully created, you are navigated to the app overview page.
4. Click **Services > Push Notification > WNS/MPNS**.
5. In the Windows Push Notification Services (WNS) and Microsoft Azure Mobile Apps section, click on the **Live Services Site** link. This navigates you to the Application Registration Portal. This should show the name of the application you created previously.
6. Copy and paste the **Application Secrets** field into a word processor document. Under the Platforms section, also copy the **Package SID** and **Application Identity** fields. These values will be used in the console to set up Windows Notification Services for Windows 10 mobile devices.
7. Click **Save** to retain your WNS settings.
8. From the Ivanti® Endpoint Manager powered by Landesk console, navigate to Configure > Device Discovery > Mobility.

9. Under the Windows Notification Service (WNS) for Windows 10 Mobiles, paste the values from the text document you created before. The Application Identity should be input for the PFN, the Package SID to the Package SID field, and the Application Secret to the Client Secret field.

10. Click Configure Domain Mappings.

11. Enter your corporate domain and click Add. The domain to enter here is found in the core_mapping.json file.

12. To check this, launch Internet Information Services (IIS) Manager. In the Connections pane, navigate to Sites > Default Web Site > EnrollmentServer. Open the core_mapping.json file. Copy and paste the domain contained in the quotes to the MDM Domain Mappings dialog.

13. Ensure that a certificate exists for WNS. This must be signed from any certificate authority. Wildcard certificates are allowed. The certificate created during the initial Ivanti® Endpoint Manager powered by Landesk install does not allow enrollment, so you must create a separate one. Add it to the server with the corporate domain name.

14. Once the certificate is added to IIS, right-click Default Web Site and select Edit Bindings.

15. Double-click on the site binding for port 443. For the SSL certificate field, select the certificate you’ll use for WNS enrollment.

Once complete, you can now enroll Windows 10 mobile devices and desktop PCs.

Set up iOS profile certificates

When settings or software are pushed to devices through the Apple Push Notification Service (APNS), the device downloads them in a profile. iOS performs a security check to see if the profile has been signed using a certificate and if the device trusts the certificate. When the profile is installed, the device user is informed whether the profile is from a trusted source or not.

You have the option to leave the profile unsigned, sign it with the core certificate, or sign it with a certificate that has been signed by a certificate authority.

![IMPORTANT: If you change this option after devices have enrolled, all iOS devices are required to re-enroll.]

- **No signing.** When you leave the profile unsigned, the profile may be vulnerable to attacks. Users are notified when they attempt to install the profile that it is not trusted and hasn’t been signed.

- **Core certificate.** This uses the existing core certificate to sign the profile. Users are notified when they attempt to install the profile who it has been signed by, but warns them that it is not trusted. The name displayed to the user is the common name associated with the core certificate.
• **Third-party certificate.** When you sign the profile with a signing certificate from a certificate authority, users are notified when they attempt to install the profile that it is signed and trusted. The name displayed to the user is the common name associated with the certificate. The certificate must be in a PKCS#12 format (.pfx or .p12). It can be a wildcard certificate, and it can be the same or a different certificate than one used elsewhere in your environment. If you use the APNS certificate to sign profiles, be aware that it must be replaced every year.

**WARNING:** You should always replace the signing certificate with a certificate that has the same private key before it expires. If the certificate expires without a replacement, or if the private key changes, you may be required to re-enroll iOS devices.

**To set up iOS profile signing**
1. From the Endpoint Manager console, click *Configure > Device Discovery > Mobility*.
2. In the iOS Profile Signing section, choose the desired profile signing option. If you are using a third-party certificate, upload the certificate file and provide the password for the certificate.
3. Click OK.

**Configure SCEP**

**Configure > Device Discovery > SCEP Configuration**

Connecting to a SCEP server allows you to dynamically provision certificates. Each time a device is added, your SCEP server will automatically distribute a certificate to it. This effectively secures your corporate network and devices from random (non-SCEP) device enrollments and access. SCEP is used for securing iOS [Wi-Fi payloads](#).

Use of this feature assumes that the following services are set up and fully configured:

- Active Directory
- Certificate Services, including Microsoft Network Device Enrollment Service (NDES). It is highly recommended that this server is running Windows Server 2012 R2 or newer.
  - The NDES server should be configured to allow more than the 5 passwords per hour. It is recommended 20 passwords per hour via registry setting.
- Network Policy Server (RADIUS)
- EAP-based wireless infrastructure
- In the LDMS console, configure Directory to connect to Active Directory; pass-through user authentication is not sufficient.
When connected to a SCEP server, Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk communicates with it through the CSA. The SCEP server should then make any certificate requests to a certificate authority, which then publishes the certificate to an access point. The certificate is then distributed on a device-by-device basis.

The credentials referenced here must be set up from the machine hosting your SCEP server. We do not document the process for accomplishing this.

The SCEP Configuration dialog has the following fields:

- **SCEP Server URL**: The NDES server hostname or IP. Both HTTP and HTTPS are supported, though we recommend using HTTPS. Only include HTTPS followed by the hostname or IP; do not include a full path. Only Microsoft NDES is supported, thus only the first part of the URL is needed.
- **Username**: The username you created when installing NDES
- **Password**: The password for the NDES user.
- **Domain**: The NDES user’s domain.

To ensure a proper connection with your SCEP server, click **Verify**. If successful, then click **Apply**.

![Verify](Image)

The **Verify** button is designed with a limited number of challenge IDs that it can submit in an hour to verify connections, so use it sparingly. To reset the password counter, restart IIS on the NDES server.

**Configure check-ins**

After a mobile device enrolls, the core server tells it to periodically check for new settings or software. By default, the device is notified to check in every 24 hours. You can modify the check-in frequency and other associated settings to manage traffic in your environment. The following options are available:

- **Delay between device batches**. If you have a large number of mobile devices that all need to check in, the server notifies them in batches to prevent too many devices attempting to check in at the same time. This is the length of time in between batches. By default, the server sends notification to 100 devices, then waits for 1 minute before contacting the next batch.
- **Device batch size**. The maximum number of devices that the server can notify to check in at the same time.
- **Device check-in expiration**. The minimum length of time the server waits before repeating a notification to check-in. This setting can be overridden by scheduled push tasks or when an administrator sends a sync command from the inventory.

---

*Copyright © 2017, Ivanti. All Rights Reserved.* [Terms of Use](#)
- **Device check-in frequency.** The length of time between device check-ins. The server waits until this period has elapsed since the last check in and then notifies the device to check in again.

- **Device check-in poll interval.** The interval that the server waits before it evaluates which devices need to check in.

These settings are used when you schedule settings and software in policy-based tasks. If you perform a scheduled push task, the server uses the batch delay and batch size settings, but ignores the expiration and frequency settings.

**To configure mobile device check-ins**

1. Click **Configure > Device Discovery**.
2. Select Mobility in the tree on the right, and click the **Advanced Settings** button.
3. Configure the settings and click **OK**. To change them back to the default settings, click **Reset**.

**Enroll devices**

With Mobility Manager, you can enroll your Android and iOS devices, Macbooks and iMacs, and Chromebooks. You can enroll these devices using an Ivanti agent app, or using Apple's Device Enrollment Program (DEP).

Enrolling a device allows you to manage settings and apps on the device. You can also sync, wipe, lock, or unlock the device from the console.

**NOTE:** For unenrolled devices that are discovered through the Exchange Server, you can only perform device discovery and wipe.

Once a user enrolls their mobile device, that device appears in the **Network View** and you can view the device's inventory information.

If you plan to distribute documents or links to users, they must also install the Ivanti Workspaces app.

**To enroll an Android device**

1. Download the Ivanti agent from the Google Play store by navigating to the URL below:


2. From the device Notifications, tap the application to install it.

3. The app asks if you want to allow the application to be a device administrator. Tap **Activate**.
4. Provide the user’s email address and password and tap Enroll.

If the device can determine the server address using a DNS lookup, it enrolls the device. If the device is unable to determine the server address using a DNS lookup, it prompts you for the URL to the server. Provide the enrollment URL provided by your administrator.

As the device is enrolled, the user is prompted to accept the profile. If the profile has not been signed, or has been signed by a certificate that the device doesn’t trust, there is a warning displayed to the user. The user must install the profile in order to be managed.

Once the user has installed the profile, settings are applied and the device downloads the software assigned to it.

**To enroll an iOS device**

1. Download the Ivanti agent from the Apple App Store by navigating to the URL below:

   ![QR Code](https://itunes.apple.com/us/app/landesk-agent/id1071187320)

2. Open the app.

3. Provide the user’s email address and password and tap Enroll.

   If the device can determine the server address using a DNS lookup, it enrolls the device. If the device is unable to determine the server address using a DNS lookup, it prompts you for the URL to the server. Provide the enrollment URL provided by your administrator.

   As the device is enrolled, the user is prompted to accept the profile. If the profile has not been signed, or has been signed by a certificate that the device doesn’t trust, there is a warning displayed to the user. The user must install the profile in order to be managed.

   Once the user has installed the profile, settings are applied and the device downloads the software assigned to it.

If you are enrolling an iMac or Macbook as a mobile device, the process here is identical. However, these devices must install a different enrollment app, which can be found on "Manage Mac devices" on the next page.

**To enroll a Windows 10 device**

1. From the device, navigate to Settings > Accounts > Work access.

2. Tap Enroll in to device management.

3. Enter your Email address and then tap the Enter key.

4. Enter the Server address and then tap the Enter key.
5. Enter your **Password, User name, and Domain**.

6. Tap **Connect** and then **Done**. The Windows Phone 10 device will automatically sync with the service.

---

**Manage Mac devices**

Enrolling an iMac and Macbook as an MDM device allows you to manage settings and apps on the device similarly to an iOS device. You can also sync, wipe, lock, or unlock the device from the console.

---

**NOTE:** For unenrolled devices that are discovered through the Exchange Server, you can only perform device discovery and wipe.

---

Once a user enrolls their iMac or Macbook, that device appears in the **Network View** and you can view the device's inventory information. You can enroll multiple users on a Mac device; however, the device itself is enrolled only once. This way you can differentiate packages on a per-user or device basis.

If you plan to distribute documents or links to users, they must also install the Ivanti Workspaces app.

**To enroll an iMac or Macbook device**

1. Download the Ivanti Macintosh MDM agent from the Apple App Store.
2. Open the app.
3. Provide the user’s email address and password and click **Enroll**.
   
   If the device can determine the server address using a DNS lookup, it enrolls the device.

   If the device is unable to determine the server address using a DNS lookup, it prompts you for the URL to the server. Enter the enrollment URL provided by your administrator. Acceptable entries include:

   - Core
   - CSA/core
   - CSA/rtc/core
   - http://csa/core
   - https://csa/core

   Once the device is enrolled, the user is prompted to accept the profile. If the profile has not been signed, or has been signed by a certificate that the device doesn’t trust, there is a warning displayed to the user. The user must install the profile in order to be managed.

   Once the user has installed the profile, settings are applied and the device downloads the software assigned to it.
These devices can also be enrolled using the Ivanti Agent. This means it is considered a hybrid device and can receive both mobile and desktop applications.

**Manage Chromebooks**

Chromebooks must be managed using Google Apps APIs, since administrators cannot install an agent on the device. When you manage Chromebooks through Ivanti® Endpoint Manager powered by Landesk, the devices appear in the inventory and you can view the device details. However, there is no additional functionality for Chromebooks from the Ivanti management console.

In order to manage Chromebooks, you must have a Google Apps for Work account that is bound to your domain name. You must also purchase Chromebook licenses in order to manage the devices. When you have purchased licenses and associated them with the Google Apps account, they appear in the Google Apps account under **Device management**.

---

NOTE: The steps for setting up a Chromebook for management through Google may change at Google's discretion. If that is the case, we recommend you find instructions from Google to perform these actions.

---

To manage Chromebooks, perform the following steps:

**Enroll the devices in Google Apps for Work**

If you do not have a Google Apps account already, you must create one in order to manage Chromebooks. Cost is based on the number of users. You must also have Chromebook licenses in order to manage the devices.

If the device has already been used, you may need to perform a factory reset on the Chromebook before it can be enrolled.

Follow the instructions from Google to enroll devices:

[https://support.google.com/chrome/a/answer/1360534](https://support.google.com/chrome/a/answer/1360534)

**Enable API access and create a client ID**

1. Log in to the Google Apps account ([https://admin.google.com](https://admin.google.com)) and click **Security > API reference**.
2. Enable the **Enable API access** option.
3. Log in to the Google Developers Console ([https://console.developers.google.com](https://console.developers.google.com)) and create a project.
4. Open the project by clicking on it.
5. In the navigation tree, click **APIs and auth > APIs > Admin SDK**. Click **Enable API** if it isn’t already enabled.
6. In the navigation tree, click **APIs and auth > Credentials**.
7. Click **Add credential**.
8. Click **Service account**.
9. Select the key type P12.
10. Click the Create Client ID button. The Client ID file is downloaded. Save the file to a safe place. You’ll need to provide this file when you provision Ivanti with the ID.
11. Make a note of the Client ID and Email address values shown under the service account.

Test the API on Google servers (optional)
2. In the tree on the left, click Chromeosdevices > list.
3. Click Try it now.
4. Enable Authorize requests using OAuth 2.0 and a dialog will pop up.
5. Select Authorize. The switch should turn from red to blue.
6. For the customerId field, enter my_customer.
7. Click Execute. You should see some or all of your Chromebook devices listed in JSON format at the bottom of the page.

Configure API access with the ID you created
1. From the Google Apps account, click Security > Show more > Advanced settings > Manage API client access.
2. Provide the Client ID in the Client Name text box. For the API scope string, type: admin.directory.device.chromeos.readonly
3. Click Authorize.

Configuring external access to domain
Some additional configuration is necessary for LANDesk to be able to access Chromebook device information.
1. In your Google Apps account (https://admin.google.com), go to the Dashboard home and select Security.
2. Scroll down and click Show more.
3. Click Advanced settings > Manage API client access. Here you can restrict Ivanti® Endpoint Manager and Endpoint Security, powered by Landesk or other external apps from potentially accessing sensitive data beyond Chromebook devices (Ivanti only requests Chromebook device information from a Google Apps account).
4. In the Client Name field, enter the Client ID you saved earlier and enter the following API scope string needed to access Chromebook device inventory from Google: https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly.
5. Click Save.
Provision Ivanti with the ID

1. Log in to the Ivanti® Endpoint Manager powered by Landesk management console.
2. Click Configure > Device Discovery.
4. Click the Add button.
5. Provide the Admin email associated with the Google Apps account, the service account email (the email address that you noted when creating the client ID), and the Client ID file.
6. Click Test Credentials to verify the information.
7. Use a scheduled task to retrieve inventory information from Google.

Manage Windows 10 PCs

Enrolling a Windows 10 PC as an MDM device allows you to manage settings on the device similarly to a Windows 10 mobile device. You can also sync, wipe, lock, or unlock the device from the Ivanti® Mobility Manager console.

If you want to enroll Windows 10 devices, you must have the following items set up or completed:

- Windows 10 Anniversary Edition or newer (build 1607)
- Signed certificate for MDM Discovery
- Windows Notification Service (WNS)

To enroll a Windows 10 PC

1. Navigate to Settings > Accounts > Access work or school.
2. Click Enroll only in device management.
3. Enter your email address.
4. Log in to your preferred work portal by entering any details requested, such as email, password, and server.
5. Once the setup is complete, click Done.

These devices can also be enrolled using the Ivanti® Endpoint Manager powered by Landesk Agent. This means it is considered a hybrid device and can receive both mobile and desktop settings.

Software distribution is currently not supported for Windows 10 devices.
Use Apple's Device Enrollment Program (DEP)

Apple allows eligible organizations to perform setup-free deployment of iOS devices through the Device Enrollment Program (DEP). Mobility Manager is designed to work with this program, eliminating the need to individually set up each iOS device purchased. By using DEP through Apple, you can associate mobile device management services with any newly-purchased device and automatically apply policies to it prior to shipping. When your Smart device arrives from Apple, it already contains all policy changes you require and can immediately be distributed.

To participate in Apple DEP with Mobility Manager you need the following:

- DEP-enrolled Apple IDs
- iOS 8.0+ devices purchased directly through Apple
- OSX 10.10+ Mac devices purchased directly through Apple

**To enable DEP with Mobility Manager**

1. **Ensure your CSA and mobility settings are fully configured.** If they are not, this functionality cannot be used. To configure your CSA, see “Configuring the Ivanti Cloud Services Appliance (Management Gateway)” on page 977. To configure mobility settings, see “Get started with Mobility Manager” on page 858.

2. **Enroll in the Apple Device Enrollment Program.** You must enroll an administrator Apple ID with the credentials needed to utilize this feature. As part of this process, you must also set up two-step authentication.

3. **Add Mobility Manager as an MDM server.** This process associates Mobility Manager with Apple Device Enrollment Program as an MDM.

4. **Install your server token on Mobility Manager.** After adding Ivanti as an MDM, you receive a server token file to associate with Mobility Manager.

5. **Configure settings as needed.** You can determine which steps of the first-time setup that users will see on the device, as well as what level of management you’ll enforce.

6. **Ensure devices are purchased directly from Apple.** Devices must be purchased directly from Apple using an enrolled Apple ID. Once purchased, you can distribute policy changes to them with Mobility Manager. To enroll your Apple ID for DEP, see Apple Deployment Programs. To verify if an iOS device was purchased directly from Apple, continue to the next step.

**CAUTION:** You cannot apply DEP policies to devices purchased prior to completing this process. Only devices purchased after will function as intended.

**Add Ivanti as an MDM**

To begin using DEP, you must have an account enrolled in Apple’s Deployment Program. After this criterion is met, you can add Mobility Manager as an approved MDM server to begin applying policy
changes to iOS or Mac OS devices purchased.

**To configure DEP for Mobility Manager**

1. From the Navigate to **Configure > Device Discovery > Apple Device Enrollment Program.**
2. Click **Add.**
3. Click the **Download Public Key File** button and name your public key file.
4. Navigate to **deploy.apple.com** and log in with your Apple ID.
5. Click **Device Enrollment Program > Manage Servers.**
6. Click **Add MDM Server.**
7. Enter a name for the server and click **Next.**
8. Click **Choose File** to browse for and upload the public key file you downloaded from Mobility Manager.
9. Click **Next.**
10. The service generates a server token. Download the token and then click **Done.**

Enrollment is enabled and you can now assign devices to the Mobility Manager server by order number or serial number from the Apple Deployment Programs Console. When a device is assigned to Mobility Manager, it becomes managed by Ivanti and it receives all restrictions, policies, and software packages associated. However, if a device is not DEP-enabled (i.e., wasn’t purchased through Apple or after setting up DEP), it will not automatically enroll or skip setup screens.

**Configure DEP settings**

After integrating Mobility Manager with Apple DEP, you can manage the initial setup of iOS and Mac OS devices. This management functionality allows you to skip the setup of key features, while also allowing you to enable supervisor mode to limit the capabilities of users.

**To configure settings**

1. From the **Apple Device Enrollment Program** window in the Console, browse for and upload the server token you downloaded from Apple DEP.
2. Enter a **DEP Token Alias.**
3. Select any configuration options and setup items to skip during the initial setup. Users will not encounter any screens selects from this window.
4. Click **OK** to save the changes. Any devices purchased with Apple DEP are automatically configured and enrolled using these settings.

**Add devices to manage**

With Apple DEP, you must specify all devices to manage by device serial number or order number.

**To add devices you want to manage with DEP**

1. From the Apple DEP Web page, click **Manage Devices.**
2. Enter all serial numbers or order numbers, separated by commas.
3. Click the Choose Action drop-down menu and select Assign to Server.
4. Select the MDM server you just added.

All devices associated with the serial numbers or order numbers entered will perform the DEP setup as configured in Mobility Manager.

**Set up DEP iOS and Mac OS devices**

Devices configured with Apple DEP still require some individual setup during their initial launch. This differs from the standard first-time launch of an iOS device where a user would set up the device as their own and perform tasks like enabling Location Services, entering iCloud credentials, and other configurations. These devices skip any setup screens you selected, and automatically enroll in Mobility Manager.

**To set up DEP devices**

1. After powering on the device, begin the setup.
2. Select a nationality and language.
3. Select a WiFi network and connect to it.
4. An alert appears to indicate that the device will be managed by Ivanti. The device user is then prompted to log in using their corporate credentials, such as those used for Active Directory.
5. Continue through the initial setup as instructed.

The device is automatically enrolled with Mobility Manager and receives any policies associated with the user account or device.

**Use Android for Work**

Enrolling a device with Android for Work allows you to encrypt your device drive, manage settings and apps on the device, and apply a work profile to only control work-related functionalities. You can also sync, wipe, lock, or unlock the device from the console.

---

**NOTE:** For unenrolled devices that are discovered through the Exchange Server, you can only perform device discovery and wipe.

**NOTE:** You can only enroll devices with Android 5.1+.

**NOTE:** If your device is already enrolled using the standard Ivanti Agent, you must unenroll the device and enroll using the Ivanti Android for Work agent. However, do not remove the Ivanti agent; this is still needed for additional management tasks.

Once a user enrolls their mobile device, that device appears in the Network View and you can view the device’s inventory information.

If you plan to distribute documents or links to users, they must also install the Ivanti Workspaces app.
To enroll an Android device

1. Download the Ivanti Android for Work Agent from the Google Play store.


2. From the device Notifications, tap the application to install it.

3. The app asks if you want to allow the application to be a device administrator. Tap **Activate**.

4. Provide the user's email address and password and tap **Enroll**.

   If the device can determine the server address using a DNS lookup, it enrolls the device. If the device is unable to determine the server address using a DNS lookup, it prompts you for the URL to the server. Provide the enrollment URL provided by your administrator.

As the device is enrolled, the user is prompted to accept the profile. If the profile has not been signed, or has been signed by a certificate that the device doesn't trust, there is a warning displayed to the user. The user must install the profile in order to be managed.

Once the user has installed the profile, settings are applied and the device downloads the software assigned to it.

**Device tasks**

When you send a command to a mobile device, such as scan now, it can take several seconds or more for the device to receive it. How quickly a device will respond to a remote command depends on your core and network configuration, the level of network congestion, and the phone's data capabilities, among other things.

**Agent settings for mobile devices**

When you manage Android and iOS devices, the agent is available through the Google Play store or the Apple App Store and must be installed by the user. After the agent is installed, you can configure agent settings for passcodes, wi-fi networks, and Office 365 or Exchange servers.

See the following pages for agent settings that can be configured for mobile devices:

- "Agent settings: Exchange/Office 365" on page 292
- "Agent settings: Mobile Compliance" on page 294
- "Agent settings: Mobile Connectivity" on page 295
- "Agent settings: Mobile Security" on page 297
Require certificates

Configure > Security > Mobile Security

Enabling this option requires that all enrolled mobile devices have an individual certificate for security purposes. Devices without certificates will not receive sensitive payloads from Mobility Manager, such as WiFi passwords or certificates. All devices enrolled after 2016.3 are automatically granted an individual certificate and will receive payloads. However, devices enrolled prior to 2016.1 must be manually re-enrolled to receive certificates. Certificates are uploaded and distributed to devices using "Agent settings: Mobile Connectivity" on page 295.

Scan a mobile device

Managed devices are configured to connect to the server every 24 hours. If you want to scan a device immediately to update the displayed information, use the Scan Now command from the Ivanti console. The command requests the device to connect and pull any updates available, and it updates the device information shown in the Ivanti console.

To run an on-demand inventory scan

1. Find the device in the Network view.
2. Right-click it and click Scan now. The device is requested to connect. The command is only sent once, so if the device is unreachable at the time the command is sent, the device waits until its scheduled update time.

Update a mobile device

You can force a managed mobile device to check in, update its settings, and update the device information on the core.

Managed mobile devices automatically check for updates every 24 hours, so you don't have to do manual updates unless you want real-time information or to apply a change immediately. The command requests the device to connect and pull any updates available, and it updates the device information shown in the Ivanti console.

To update a mobile device’s policies

1. Find the device in the Network view.
2. Right-click it and click Sync. The device is requested to connect. The command is only sent once, so if the device is unreachable at the time the command is sent, the device waits until its scheduled update time.
Lock or unlock a mobile device

You can remotely lock managed mobile devices if they are stolen or lost. The mobile user will need to enter their passcode to unlock the device. If the device doesn’t have a passcode, users can unlock the device without entering a passcode.

If the user forgets his passcode, you can also unlock the phone and remove the current passcode. If you have passcode settings enforced on the device, the user is prompted to create a new passcode when he accesses the device.

If the device is turned off or out of range when the command is sent, it may not receive the command.

Any desktop computer, such as a Macbook or Windows 10 machine, cannot be locked or unlocked remotely.

To lock or unlock a mobile device

1. Find the device in the Network view.
2. Right-click it and click Lock or Unlock. When you unlock the device, the passcode is removed.

Wipe a mobile device

When a device is lost, stolen, or assigned to a new user, you may want to wipe the device to remove any personal or sensitive information.

There are two methods for wiping a device, depending on whether the device is enrolled or only discovered through the Exchange server.

- Enrolled devices are wiped through the Mobility tool.
- Discovered devices are wiped through the EAS server.

Wipe an enrolled device from the inventory

There are three wipe options for managed devices:

- **Selective wipe/Unmanage.** Removes all the agent settings on the device. For example, a selective wipe would remove app restrictions or WiFi passwords. It does not uninstall the Ivanti agent.

- **Selective wipe/Delete.** Removes the agent settings and also deletes the device from the inventory.

- **Wipe.** Removes all personal files and applications from the device and restores the device to its factory settings. This option removes the Ivanti agent from the device. This option doesn’t work with desktop machines, such as Windows 10 PCs, iMac, or Macbooks.
When you send a wipe command, it is sent through the notification service (either GCM or APNS depending on whether it is an Android or an iOS device). The command is sent immediately and cannot be canceled.

If the device is unreachable when the command is sent, the notification service caches the command temporarily. If the device comes online again while the command is cached, the command is delivered to the device and it is wiped. If the device does not come online within 24 hours, the wipe command is not delivered.

If a mobile device has both the MDM and Agent applications installed, wiping a device using the Mobility Manager still removes the Ivanti profile.

**To execute the wipe command**

1. Find the device in the Network view.
2. Right-click it and click **Wipe...** Then select the type of wipe you want to perform. You are prompted to proceed with the command.

**Wipe a discovered device using the EAS server**

On a Microsoft Exchange server, the wipe is associated with both the user and the device. Once the wipe command is sent to the server, the device’s status in the Mobility management tool is set to "Wipe pending". The next time the device attempts to log in, the wipe command will execute and the device will be wiped immediately. Because the wipe does not actually occur until the next time the device logs in, the wipe command can be canceled at any time prior to the device check-in.

**To execute the wipe command**

1. Find the device in the Network view.
2. Right-click it and click **EAS Wipe.** You are prompted to proceed with the command.
   
   When the device is wiped, it is also removed from the inventory.

**To cancel a wipe command**

To cancel a Wipe command (only available on devices being wiped through EAS), right-click on the device and select **Cancel wipe**.

**Distribute content to mobile devices**

Use Mobility Manager to distribute apps, documents, or links to mobile devices.

To distribute documents or links, the device user must have both the Ivanti Agent and the Ivanti Workspaces app installed. Use a universal link or document package created in the Distribution packages tool. For more information about types of packages, see "Understanding distribution package types" on page 458. For more information about distributing packages, see "Distribute a package" on page 470.
Distribute free apps from the Google Play store or the Apple App Store, or distribute apps that you have the .apk or .plist and .ipa files for.

Software distribution is currently not supported for Windows 10 devices.

For software, the package that is sent to the device does not contain the app, it only contains the location of the app. When the device receives the package, the device contacts the server (either the app store or your server) that hosts the app and downloads it. If the app server is unavailable (for example, if the app server is only available on the domain and the device is not currently on the domain), the device will attempt to download the app the next time that it checks in with the core server.

Use one of the following methods for distributing apps:

- **App store.** When the free app is available in the Google Play store or the Apple App Store, you can search for the app or provide the URL. Mobility Manager uses the information from the app store to populate the package. You can only distribute free apps from an app store.

- **Manifest URL.** If you have an app that was developed by or for your company, distribute it by putting the app (either the .apk file, or the .plist and .ipa files) on a web server. The software package tells the device the location of the server to retrieve the package from, and the device downloads and installs the package. The device must be able to connect to the web server where the app is hosted. The server that delivers the app can use either http or https. When you use a manifest URL, you must also know the package ID and package version. You can get that information from the app developer. A package ID may also be known as the bundle ID or package name.

  An example of an Android package ID: com.google.android.apps.maps

  An example of an iOS package ID: 418167706

**NOTE:** Mobility Manager does not use the preferred server information. Even if the app is stored on a preferred server, you must specify a URL to the server, and that is the only server the device will attempt to download the app from. If the server requires a password to access the app, the download will fail.

Software packages are specific to an operating system. You cannot have one package that delivers the same app to both Android and iOS devices. However, you can create one package for each operating system and then put them in the same bundle.

When you need to distribute a new version of an app that has already been distributed, create a software package with the new app, increment the version number, and use the same package ID. The device will detect that it is a new version of an app it already has, and update the app rather than uninstalling and re-installing.

**To create a software package for Android or iOS**

1. Click **Tools > Distribution > Distribution packages.**
2. Choose the folder where you are creating the package and click the **New** button in the toolbar.

3. Choose the type of package you want to create. Android and iOS packages are classified as Mobile packages, and Mac computers with the Macintosh MDM agent receive packages through the **Macintosh > Macintosh MDM** option.

4. On the Package information page, type a description of the app.

5. Select the method for distributing the app.
   - For **App store**, use the search box to find the app. When the search finds the app on the app store and you select it, the **Location**, **Package ID** and **Package version** fields are populated.
   - For **Manifest URL**, provide the path to the app. If it is an iOS or Mac app, provide the path to the .plist file. This must be an address to a web server that the device can reach. You also need to provide the **Package ID** and the **Package version** for the app.
   - For **VPP**, select an existing **Token alias** and then click the arrow icon. This presents a list of all apps associated with the VPP token. This option is only available for iOS and Macintosh MDM packages. If no tokens appear, see "Associate Apple Volume Purchasing Program (VPP) account" below.

6. Click **Save**.

   If you lack sufficient app licenses to distribute apps to all enrolled devices, Mobility Manager will deliver software packages until all licenses are used up. All remaining devices will display as a failed deployment.

### Associate Apple Volume Purchasing Program (VPP) account

Apple allows users to purchase multiple licenses and distribute them across multiple iOS and Mac OS devices through the Apple Volume Purchasing Program (VPP). From the Mobility Manager, you can view your available and used VPP licenses and revoke licenses you own from devices. This functionality may also be used for free apps.

> **IMPORTANT:** Users still retain the ability to purchase apps on their iOS and Mac OS devices through their individual Apple ID accounts.

You cannot purchase Apple VPP licenses through Mobility Manager. Licenses must be purchased from iTunes using an Apple ID enrolled in VPP, and then you can distribute them through Mobility Manager using a Software Distribution Package.

To manage software licenses with Apple VPP:
1. **Enroll in Apple's Volume Purchasing Program.** You must have a corporate Apple ID enrolled in VPP to use this functionality. Once you’re enrolled, use the [Apple Deployment Programs](#) website to purchase bulk software licenses.

2. **Enable VPP.** From the Mobility Manager, you add the VPP token created from Apple’s Deployment Program to manage app licenses associated with the account.

3. **Deploy licenses to enrolled devices.** Using a software package, deploy apps managed with Apple VPP.

4. **Revoke licenses as needed.** You can reclaim licenses from devices at will from the Console. Even if a device is unenrolled, you must perform a manual reclamation of the license to reassign it.

### Configuring Apple VPP

In Ivanti® Endpoint Manager powered by Landesk, you can activate Apple VPP integration to view and manage how all of your purchased licenses are distributed. Mobility Manager allows you to identify the total number of licenses currently in use, what devices or users possess licenses, and the number of remaining available licenses.

When a license is deployed to a user’s device through a software package and associated with the device’s Apple ID account, it appears on the user’s Purchased Apps list. They can then download and install the app on all other iOS devices associated with their Apple ID, even if the device isn’t managed by Mobility Manager.

### To manage application licenses from Mobility Manager

1. From the Console, click **Tools > Distribution > Distribution packages > Volume Purchase Program Configuration**.

2. Click **Add VPP Token**.

3. Provide a token alias and then browse for the token file you downloaded from Apple’s website.

4. Click **Add**.

   All application license purchases associated with your Apple ID display in the Associated applications pane.

---

**NOTE:** Multiple tokens may be added. However, tokens should not be shared between multiple cores.

In the Console, double-clicking on an application name will display a dialog listing all licenses currently in use. Each license identifies the device it is assigned to by either device name for group enrollment or user account for LDAP.
To install VPP apps on an iOS or Mac OS device

- After deploying the VPP settings from the Console, all affected devices may receive a prompt to install the deployed apps. Users must accept this prompt and sign in with the device’s Apple ID to receive VPP licenses on the device. This will not charge the device’s Apple ID account.

Each time a licensed app is deployed, users are prompted from the device to sign in with their Apple ID. Signing in is required to identify all corporate-owned licenses installed on the device and add them to their Purchased Apps list. This does not give Ivanti® Endpoint Manager powered by Landesk access to the Apple ID account associated with the iOS device, so users can use their personal account if needed.

Reclaiming Licenses from a Device

Each app license distributed via VPP can only be given to one user. When a license is assigned, it is unavailable for reallocation until you reclaim it from the device. Users can still purchase their own license and download the app.

Unenrolling a device or performing a factory reset at the device level will not reclaim a license automatically. You must manually reclaim such licenses. However, if an administrator removes the device from the inventory or performs a device wipe through the Console, the software license is made available for reallocation.

To reclaim application licenses

1. From the Console, click **Tools > Distribution > Distribution packages > Volume Purchase Program Configuration**.
2. Double click on the application you wish to reclaim a license for. A list of users with licenses displays.
3. Select the user you wish to reclaim a license from, and then click **Reclaim selected**.
   The license is reclaimed and now displays under the column of available licenses.

If a license is revoked from a device

Revoking a software license from a device causes one of the following actions at the device level:

- On iOS devices, the application is removed from the device the next time the agent syncs.
- On Mac OS devices, you can continue using the software as part of a 30-day grace period, after which the app will no longer launch. This grace period does not prevent administrators from immediately reassigning a revoked license to another device. Revoked licenses are immediately available for use.
Un-enroll mobile devices

If a user wants to remove his mobile device from management, he can uninstall the Agent just as he would any app. Users who have iOS devices that are being managed need to go into **Settings > General > Profiles** and remove the MDM profile. If the profile is password protected, the user is prompted for the password in order to remove the profile.

When a user uninstalls the apps, it does not remove the device from the Network view or the Mobility tool.

An administrator can unenroll a device through the console by performing a selective wipe. A selective wipe removes the MDM profile and the associated settings from the device, and may also remove the device from inventory. For more information, see "**Wipe a mobile device**" on page 877.

Use Mobility Manager with an Exchange server

When you set up credentials to connect to an Exchange server (including Office 365), you can discover mobile devices that have connected to the Exchange server, modify the Exchange server connection rules, and perform an EAS wipe on devices that connect to the server.

When you discover devices through the Exchange server, the devices show up in the inventory view. To wipe a device through the Exchange server, find the device in the inventory, right-click it and select **EAS Wipe**. The wipe command is sent to the device the next time it attempts to connect to the Exchange server.

NOTE: Even if you choose to use only the limited set of features available through the Exchange server with Mobility Manager, you must set up the CSA, LDAP connection, and credentials for the Exchange server.

For more information on setting up a connection with the Exchange server and viewing mobile devices, see:

- "Configure the Exchange server connection" below
- "Discover mobile devices" on the next page
- "Connection rules" on page 885

Configure the Exchange server connection

To use your Exchange server for mobile device discovery, you first need to provide credentials to authenticate to the Exchange server in your environment. This allows you to discover mobile devices and manage their access to the servers.

NOTE: When you gather information about your Office 365 accounts for asset management or
To provide the server authentication information

1. Click Configure > Device discovery.
2. Select the type of server, either Exchange 2007, Exchange 2010, or Office 365.

For Exchange 2007 servers

1. Make sure the Microsoft Exchange Server 2007 Management Tools are installed on your core server.
2. If the core server is running on Server 2008 R2, make sure PowerShell 3.0 is installed.
3. Specify the login credentials.
4. Click Test connection to verify the credentials work.
5. Click OK.

For Exchange 2010 servers or Office 365

1. Specify the server domain\server name and login credentials.
2. Click Test connection to verify the credentials work.
3. Click OK.

NOTE: Microsoft Exchange is currently limited to one server per version (2007, 2010, or Office 365).

With the authentication information configured, you can now discover mobile devices and display their information in the mobile device inventory. For information on other options available with Exchange 2010 or Office 365, see "Connection rules" on the next page

Discover mobile devices

To discover devices connecting to your Exchange server that are not currently being managed, Mobility Manager uses mobile device connection information from the Exchange mail server. Agentless discovery doesn’t require any communication with the actual mobile device, but only mobile devices that have connected to a corporate mail box can be discovered.

You must have the Exchange information configured in order to connect to the Exchange server and discover devices. For information on configuring the connection to the Exchange server, see "Configure the Exchange server connection" (883).

To discover mobile devices

1. Click Configure > Device discovery.
2. Confirm that the server settings are correct and click Discover now. Or click Schedule discovery to create a scheduled task for device discovery.
Once the information is retrieved from the Exchange server, the devices appear in the device inventory. To perform an EAS wipe on the device, right-click it and select EAS wipe. The wipe command is sent to the device the next time it connects to the Exchange server. If the device is enrolled, the regular Wipe option is available, instead.

**Connection rules**

If your company uses Microsoft Exchange 2010 or Office 365, you can use Mobility Manager to manage Exchange connection rules that allow you to configure what devices can connect to an Exchange mailbox. The Microsoft Exchange 2007 server environment doesn’t support connection rules. Connection rules are used to allow or deny connections for specific device types.

By default, Mobility Manager does not manage connection rules, so if you have connection rules configured on the Exchange server already, they are not modified. However, if you configure connection rules through Mobility Manager, those rules override any rules configured on the Exchange server.

NOTE: Connection rules are applied to any device that connects to the Exchange 2010 server, regardless of whether it has an agent installed or not.

Since the Apple mobile device model list is fairly small, it’s easy to identify the devices you’re interested in managing:

- iOS
- iPad
- iPhone

Android is more complicated because there are so many manufacturers providing Android devices. With Android devices, you’ll need to pay more attention to the much larger variety of device types that exist in the Android ecosystem.

Fortunately, it’s fairly easy to find out a device’s type. When a user tries accessing their Exchange mailbox from a mobile device that is blocked by a connection rule, that user receives an email with information about why the mobile device was denied access. Included in that email is the mobile device’s device type.

Administrators can use the information from this email to add the blocked device type to an exception list if they want to allow that device model access.

If mobile devices have already connected to your Exchange server, and you want to continue to allow those devices regardless of whether they meet the connection rule criteria or not, use the grandfather option.
Grandfather mobile devices

You can grandfather all mobile devices that connected to your Exchange 2010 or Office 365 server in the past. Grandfathering allows these devices access regardless of any future connection rules you consider. This can be useful when you’re deploying Mobility Manager and you want to be sure existing mobile devices aren’t affected.

Use this option carefully. It modifies the server whitelist and is not reversible using the LDMS console. In other words, once you’ve enabled grandfathering, the only way to remove a whitelisted device is to use the Exchange console to manage the whitelist manually.

To allow previously connected devices regardless of the connection rules

1. Click Configure > Device Discovery.
2. In the navigation tree, click Exchange ActiveSync and then click the Exchange 2010 or Office 365 link.
3. Make sure the Exchange manages my connection policy checkbox is not enabled, and enable the Allow previous connected devices (grandfather) checkbox.
4. Click OK.

Apply mobile device connection rules

Once you’ve configured a Mobility Manager connection to a Microsoft Exchange 2010 server or Office 365, you can then configure ActiveSync connection rules.

There are three connection rules you can apply:

- **Allow all mobile devices to connect**: Any user can access an Exchange mailbox from a mobile device.

- **Do not allow mobile devices to connect**: Mobile devices can’t access an Exchange mailbox. You can refine this rule by creating exceptions for certain mobile device types (iPad devices, for example).

- **Allow only managed devices to connect**: Mobile devices that are enrolled in Mobility Manager can access an Exchange mailbox. You can refine this rule by creating exceptions for certain mobile device types (iOS devices, for example).

The default device list already defines exceptions for some common device types. If you don’t see the device type you want to manage in the list, you can add new device types.

Connection rules take effect when you click OK or Apply in the configuration dialog. There is no additional deployment required.
To apply connection rules

1. Click **Configure > Device discovery**.
2. In the navigation tree, click **Exchange ActiveSync** and then click the **Exchange 2010** or **Office 365** link.
3. Make sure the **Exchange manages my connection policy** checkbox is not enabled.
4. If necessary, add device types to the list so you can make an exception for them.
5. Enable the checkbox next to each device type you want to allow to connect.
6. Click **OK**.
Alerting

Alerts and monitoring overview

Ivanti® Endpoint Manager powered by Landesk alerting and monitoring give 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 initiate solutions by logging the event, sending an e-mail or pager message, running an application, or powering off the device.

The following general types of monitoring are available in Endpoint Manager:

- Monitoring (pinging) devices for network connectivity
- Basic hardware and software monitoring for all devices
- Performance monitoring of selected hardware features
- Hardware-dependent monitoring using manufacturers' monitoring technology

Endpoint Manager provides integrated alerting for these different types of monitoring. The alerts that you choose to apply to specific devices are contained in alert rulesets that you distribute.

All alerts and monitoring are dependent on the type of hardware, firmware, and related features for each device. Some monitoring options are not supported on different types of devices. In some cases the implementation of a hardware standard may differ between manufacturers, so what works on one device may not work the same on another.

Understanding alerts, rules, and rulesets

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.

As you define 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. You can deploy alert rulesets to one or more devices to monitor the items that are important for that kind of device.

Alerts agents and rulesets

To generate alerts for a managed device, the Ivanti alerting agent must be deployed to that device. A default alerting agent and alert ruleset are deployed to every managed device when you install the standard agent on the device. 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 Ivanti 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.

Understanding performance monitoring

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 Real-time inventory and monitoring 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.

Hardware-specific monitoring

Endpoint Manager includes support for the following monitoring technologies for different manufacturers’ hardware:

- IPMI (Intelligent Platform Management Interface)
- IPMI BMC (baseboard management controller) configuration
- Dell DRAC (Dell Remote Access Controller)
- Intel vPro technology, including Intel AMT (Active Management Technology)

Real-time inventory and monitoring overview

Ivanti® Endpoint Manager powered by Landesk provides real-time updates of inventory data and monitoring status through the Real-time inventory and monitoring console.

This console is available only for devices that have the Ivanti agent with Real-time inventory and monitoring options selected.

Opening the console

You can open the Real-time inventory and monitoring console in two ways:

- Right-click a managed device in the network view and select **Real-time inventory and monitoring**. This option is unavailable if the device does not have the monitoring option
selected in the Ivanti agent.

- Open the Health dashboard (click Tools > Reporting/Monitoring > Health Dashboard). Right-click a device and select View details. The Real-time inventory and monitoring console opens for all devices, but real-time data is not provided if the device does not have the monitoring option selected in the Ivanti agent.

### Alerting basics

To generate alerts for a managed device, the Endpoint Manager alerting agent must be deployed to that device. A default alerting agent and alert ruleset are deployed to every managed device when you install the standard agent on the device. That agent follows the rules defined in the alert rulesets for that device.

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.

#### 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, and so on.
- **IPMI event**: An event detectable on IPMI devices has occurred, including changes to controllers, sensors, logs, and so on.
- **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 Real-time inventory and monitoring console.

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.

**Alert actions for 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

Alert actions are configured when you define 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.

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.

Default rulesets

When the monitoring agent is installed to a managed device, the **Ivanti default** ruleset is installed 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
- Ivanti Antivirus status
- Network access control status
- Client database utility
- Security and Patch Manager alerts

You can modify the Ivanti default ruleset to include the alerts you want to monitor.
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).

Process for deploying rulesets

The general process for deploying alert rulesets to managed devices is as follows:

1. Create or edit the ruleset.
2. Create a task to schedule deployment of the ruleset.
3. Select the devices to which you will deploy the ruleset, and run the scheduling task.
4. If a ruleset includes performance monitor alerts, open the Real-time inventory and monitoring console for each device with that ruleset and define the performance monitor counters for the device.

Related topics

"Configuring alert rulesets" (895)
"Deploying an alert ruleset" (893)
"About performance monitoring" (910)
"Working with agent configurations" (112)

Deploying an alert ruleset

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.
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.

   A new task is created in the Scheduled tasks tool.

8. Drag devices from the network view to the new alert task.

9. Right-click the task and select Properties. Make sure you have the correct target devices, then select options to schedule it, and then click Save.

Notes

- 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 Real-time inventory and monitoring 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.
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 Ivanti 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.

NOTE: You can 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.

Removing all rulesets from a device

You can remove all rulesets from one or more devices without deploying any new rulesets.

You can remove all rulesets if you have one or more rulesets in effect on a device and want to replace them with a new ruleset. When you have multiple rulesets in effect on a device, unpredictable results may occur because similar alert rules may have conflicting actions, and unintended results can occur.

To remove all existing rulesets

1. Click Tools > Configuration > Alerting.
2. On the toolbar, click the Create a task icon and select Remove all rulesets.
3. Click OK.

Configuring alert rulesets

The Alert rulesets page displays all the alert rulesets that you can deploy to managed devices. There are three rulesets that appear by default, and you can create custom rulesets to apply specific types of monitoring to different kinds of devices.
The alert rule sets that appear by default on the Alert rule sets page are:

- **Core alert ruleset**: This rule set ensures that alerts originating on the core server are handled. This rule set is installed on the core server but can't be installed on other devices, and you can only have one core alert rule set. You can edit the rule set but can't delete it from the core server. This rule set contains a predefined group of alert types, including Device Monitor, Intel vPro alerts, and Serial Over LAN Session alert types.

- **LDMS default ruleset**: This rule set is deployed by default to all Ivanti managed devices. It includes alerts for security features included in Endpoint Manager, such as real-time inventory and monitoring, network access control, inventory scanner, and Security and Patch Manager alerts.

- **Provisioning ruleset**: This rule set 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 rule set is used to send alerts related to the progress of the provisioning task. The rule set is included in the provisioning agent and does not need to be manually deployed. You can edit this rule set 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 rule sets you can create custom rulesets and apply them to 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.
Conflicts between rulesets

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.

Default log action

Every time you create an alert rule, a rule is automatically created with a "Log handler configuration" action. This happens so that every alert is always logged at the core server.

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

Click here for an example of how to configure a ruleset.

Example: Configuring an alert ruleset for disk space problems

The following procedure demonstrates a simple example of the first step in configuring a custom alert ruleset. In this example, a single alert rule is added to a ruleset.

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. Depending on your screen resolution, you may want to resize the columns to read items in the lists.

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 box, 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.

    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 alert to local NT event log as the action, then in the right column click Rules > Edit. Use this dialog box 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 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.

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.

When you have created a ruleset, you then edit the ruleset to add alerts and associated actions.

Edit an alert 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.

![Endpoint Manager User Interface](image)

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.
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.

Three time rules are available by default. You can also define different time rules if needed.

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.
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.

Details about defining actions and time filters, and editing rule properties, are found in the following topics.

**Define or edit a Monitoring alert**

You can define an alert under the Monitoring section of alerts, and you can edit an existing Monitoring alert (for example, to change the polling frequency).

1. In the left column of the Alert ruleset page, click **Alerts**.
2. In the tree view of alerts, scroll down to the **Monitor** section. You can create or edit an alert only under the Monitor heading.
3. Select a category (for example, **Chassis**), then click **Tasks > New** in the right column.
4. Add information in the **Name**, **Description**, and **Polling interval** fields as needed, then click **OK**.

The alert is listed under the category you selected and is available to add to a ruleset.
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.

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 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.

**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 box, enter data in the fields (described below).
4. Click **Save**.

The time filter appears in the list and is available to associate with alerts. Fields in the **New filter** dialog box include the following:

- **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.
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 respective list.
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, select the Health check box.
6. Click OK to save your changes.

Clone an alert rule

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.

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 box, 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.
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.

**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.
2. Click **OK** at the success message.

The XML files with published ruleset data are stored in the Idlogon 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 update 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. We strongly recommend that you publish rulesets every time you make any changes to them.
About performance monitoring

Endpoint Manager provides several methods for monitoring a device's health status. While alert rulesets are defined at the core console and deployed to multiple devices, on individual devices you can also define performance monitoring counters to monitor specific performance issues.

You can define performance counters and monitor them for various kinds of data on your devices, such as:

- Hardware components (such as drives, processors, and memory)
- Hardware sensors (such as fans, voltages, and temperatures)
- OS components (such as processes and services)
- Application components (such as bytes per second transferred by the system's Web server)
- Usage levels

When you select a performance counter you also specify the frequency for polling the item, as well as specify the performance thresholds and number of violations that are allowed before an alert is generated. After you define a performance counter, you can then open the Monitoring page in the Real-time inventory and monitoring console and view a summary of your monitored alerts.

In order to be alerted for performance monitor items on a device, you must include a Performance monitor rule in the ruleset for that device.

Process for monitoring performance items on devices

To monitor performance of various items on your managed devices, complete the following three general tasks:

- Install a monitoring agent on devices
- Create performance monitoring rules for individual devices
- View performance monitoring data

Notes

- If you want to simply ping devices regularly to monitor their connectivity, use the device monitor feature.
- Communications to the monitoring agent are via HTTP over TCP/IP in the form of GET or POST requests. Responses to requests are in XML documents.
- When you run and store a query on the health status of devices (Computer.Health.State), the state in the database is represented by a number. The numbers correspond to the following states: 4=Critical, 3=Warning, 2=Normal, 1=Informational, null or 0=unknown.
Hardware monitoring is dependent on the capabilities of the hardware installed on a device, as well as 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, monitoring data will not be available.

If reporting from a specific machine appears to have stopped, you can use restartmon.exe in the LDCLIENT folder to restart the collector and all monitoring providers. This utility is for machines on which reporting has been installed, and reporting has stopped. Use this utility to restart the collector and providers without having to reboot the device.

Related topics
"Alerting basics" (890)
"Monitoring devices for network connectivity" (930)

Deploy a monitoring agent on devices

Endpoint Manager provides an immediate summary of a device's health when the Real-time inventory and monitoring agent is installed on the device. The monitoring agent is one of the agent components that can be installed on managed devices.

The Real-time inventory and monitoring agent checks the device's hardware and configuration on a regular, periodic basis and reflects any changes in the device's health status. The device's status is shown in three places:

- The status icon in the Devices lists in the network view
- Health status shown in the Health Dashboard (click Tools > Reporting/Monitoring > Health Dashboard)
- Data shown in the Real-time Inventory and Monitoring dashboard for the device (right-click the device in the network view and select Real-time inventory and monitoring)

For example, a monitored device with a disk drive that is filling up can display a warning status icon when the disk is 90% full, changing to a critical status icon when the disk is 95% full. You may also receive alerts for the same disk drive status if the device has an alert ruleset that includes performance monitoring rules for a drive space alert.

Create performance monitoring rules

You can choose what performance items are monitored on a device by defining monitoring rules that specify what the monitoring agent checks on the device. To do this you need to deploy a ruleset to the device that includes a Performance monitoring alert rule.
There are a large number of performance counters that can be monitored. When you create a performance monitor rule you can turn any of these items on or off, specify how frequently to check them, and, for some items, set performance thresholds. You can also select services running on the devices that you want to monitor.

The overall process for creating performance monitoring rules is as follows:

1. Include Performance monitoring as a rule in the alert ruleset for the device.
2. Deploy the alert ruleset to the device. (You can target multiple devices to deploy the ruleset to multiple devices, but then need to define performance monitoring on individual devices.)
3. Create performance monitoring rules on the device using the Real-time inventory and monitoring console. Some events such as services also require that you select each service you want monitored (see detailed steps below).

**To select a performance counter to monitor**

1. Click **Tools > Reporting/Monitoring > Health dashboard.**
2. In list of devices, double-click the device you want to configure.
   The Real-time inventory and monitoring console opens in another browser window.
3. In the left navigation pane, click **Monitoring.**
4. Click the **Performance counter settings** tab.
5. From the **Objects** column, select the object you want to monitor.
6. From the **Instances** column, select the instance of the object you want to monitor, if applicable.
7. From the **Counters** column, select the specific counter you want to monitor.
8. If the counter you want doesn't appear in the list, click **Reload counters** to refresh the list with any new objects, instances, or counters.
9. Specify the polling frequency (**every n seconds**) and the number of days to keep the counter history.
10. In the **Alert after counter is out of range** box, specify the number of times the counter will be allowed to cross the thresholds before an alert is generated.
11. Specify upper and/or lower thresholds.
12. Click **Apply.**

**Notes**

- Performance log files can quickly grow in size; polling a single counter at a two-second interval adds 2.5 MB of information to the performance log daily.
- A warning alert is generated when a performance counter drops below a lower threshold. When a performance counter exceeds an upper threshold on a Windows device, a critical alert is generated.
When you set thresholds, remember that alerts will be generated regardless of whether an upper or lower threshold is crossed. In the case of something like disk space, you may want to be alerted only if the device is running low. In this case, you would want to set the upper threshold to a high enough number that you would not be alerted if a lot of disk space became available on the device.

Changing the Alert after counter is out of range number lets you focus on an issue when it is a persistent problem or when it is an isolated event. For example, if you are monitoring the bytes sent from a Web server, you will receive alerts when the bytes/sec consistently runs high. Or, you can specify a low number such as 1 or 2 to receive an alert whenever your anonymous FTP connections exceed a certain number of users.

When you edit services in a monitoring rule, the Available services list displays known services from the inventory database. No services are displayed in the Available services list box until an agent has been deployed to one or more devices and an inventory scan is returned to the core.

Generate an XML file for a ruleset

As part of the deployment process, an XML page is created that lists the deployed ruleset and devices the ruleset was deployed to. This report is saved on the core server in the Ldlogon directory, and is named with a sequential number assigned by the database.

If you want to view this XML page separately from deploying a ruleset, click the Generate XML button and then click the link to view the XML file. Generating a ruleset as XML also allows it to be displayed in the list of available rulesets in the Agent configuration settings.

View performance monitoring data

The Monitoring page lets you monitor the performance of various system objects. You can monitor specific hardware components, such as drives, processors, and memory, or you can monitor OS components, such as processes or bytes per second transferred by the system's Web server. The Monitoring page includes a graph that displays real-time or historical data for counters.

In order to monitor a performance counter you must first select the counter, which adds it to the list of monitored counters. When you do this you also specify the frequency for polling the item and set performance thresholds and the number of violations that are allowed before an alert is generated.

To view monitored performance counters

1. Click Tools > Reporting/Monitoring > Health dashboard.
2. In the list of devices, double-click the device you want to configure.
   The Real-time inventory and monitoring console opens in another browser window.
3. In the toolbox, click Monitoring.
4. Click the Active performance counters tab, if necessary.
5. In the Counters drop-down list, select the counter you for which want to see a performance graph.
5. Select **View real-time data** to display a graph of real-time performance.
6. To display a graph showing performance over a period of time, select **View historical data** (Keep history) when you select the counter.

**Notes**

On the performance graph, the horizontal axis represents time that has passed. The vertical axis represents the units you are measuring, such as bytes per second (when monitoring file transfers, for example), percentage (when monitoring percentage of the CPU that is in use), or bytes available (when monitoring hard drive space). The line height is not a fixed unit. The height of the line changes relative to the extremes in the data; for one counter the vertical axis might represent 1 to 100 and for another it might represent 1 to 500,000. When the data varies across a wide extreme, minimal changes can appear as a flat line.

Monitored counters are listed with columns for how often they are checked, the number of times the counter is out of range for an alert to be sent, and the upper and lower threshold settings.

Selecting another counter refreshes the graph and resets the units of measurement.

If you receive an alert generated by a counter in the list, right-click the counter and click **Acknowledge** to clear the alert.

**Stop monitoring a performance counter**

1. Click **Tools > Reporting/Monitoring > Health dashboard**.
2. In the list of devices, double-click the device you want to configure. The Real-time inventory and monitoring console opens in another browser window.
3. In the toolbox, click **Monitoring**.
4. Click the **Active performance counters** tab, if necessary.
5. Under **Monitored performance counters**, right-click the counter and click **Delete**.

**View the global alert log**

Use the global **Alert log** page to view alerts sent to the core server. The log is sorted by time (GMT) with the most recent alert at the top.

**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**.

**NOTE:** 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.

**Click here for descriptions of alert log 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.
- **IP address:** The IP address of the device on which the alert was generated.
- **Instance:** Provides more detailed information as to the situation in which the alert was generated.

**View a device's alert log**

Use the **Alert log** page to view alerts sent to a managed device. The log is sorted by time (GMT) with the most recent alert at the top.

**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**.
4. Click **Logs > Alert log**.
5. 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 Real-time inventory and monitoring console.

---

**NOTE:** 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.

---

**Click here for descriptions of alert log 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.
- **Instance:** Provides more detailed information as to the situation in which the alert was generated.

---

**Monitoring the contents of log files**

Log file monitoring is an option available in the performance monitoring rules. This monitoring agent scans log files on managed Windows devices for specific strings or expressions, and generates alerts when they are found. This is useful if you want to be alerted when a particular condition exists that can be traced through a log file.
You can monitor a text file generated by any application, including .htm and .xml files (however, Unicode files can’t be monitored). After you specify which file to monitor and define rules using regular expressions, the file will be monitored as long as the log file monitoring rule is contained in a ruleset that is in effect on that device.

The first time text in the log file matches a regular expression, an alert is generated. The alert is generated only once for that file even if there are multiple matches. Later, if the file changes so there is no longer a matching condition, then the agent begins scanning for that regular expression again and will generate an alert on the next occurrence of the match.

You can also scan log backup files that are created when a log file becomes too large and older entries in the file are appended to a different file (a "rolling" log file). However, "wrapped" log files, which remove older entries within a single log file to make room for new entries, are not supported.

For this monitoring option, you must specify the location and exact name of the file on the managed device, and you specify the search criteria with a regular expression. When a string in the file matches the expression, an alert action is generated if you have defined a Log file monitoring alert type in the appropriate alerting ruleset.

You can include log file monitoring in any alerting ruleset you have defined. The following procedure describes the five general steps for setting up log file monitoring:

1. Create a log file monitoring rule in an alert ruleset.
2. Specify which log file to monitor on the managed devices.
3. Define the monitoring rules for that file, using regular expressions.
4. Select a severity level for the rule and name the instance so it will be identified in alerts.
5. Apply action and time rules and save the rule in the alert ruleset.

**Notes**

- Log file monitoring is supported only for managed Windows devices.
- Any time you edit or delete a rule, you need to publish the alert ruleset that the rule appears in. The changes you make will not apply to devices until the ruleset has been published (or until you redeploy the ruleset with a scheduled task).
- This feature maps log files into memory to use less memory during a search. Runtime memory is allocated for this as linear regular expression searches occur. Because Windows locks the file when it is mapped into memory, you may encounter issues with some applications.

**Related topics**

"Configuring alert rulesets" (895)

"Set up a log file monitoring rule" (918)
**Set up a log file monitoring rule**

1. Click **Tools > Configuration > Alerting.**
2. Under **Alert rulesets**, select the ruleset you want to edit, then click **Edit** on the toolbar.
3. In the left column of the **Alert ruleset** window that opens, click **Alerts.** Under the **Monitor** folder in the list of alerts, click **Log file monitoring.**
4. Click **Tasks > New** in the right column.
5. In the **Log file monitoring** dialog box, type a name and description for the log file monitoring rule.
6. To change the frequency at which the item is monitored, change the **Polling interval** settings.
7. Click **Log file configuration** to specify which log files are monitored, what you are monitoring for, and how you will be alerted.
   Regular expressions are used to define what content in the log file should be monitored. When the monitoring service finds a match for the regular expression in the log file, it follows the alert rules to notify you of the occurrence.
8. Click **Manage.** In the **Regular expression management** dialog box, add a descriptive name and a regular expression, then click **Add.** Repeat for each regular expression you want to use for monitoring log files. When you have added them all, click **OK.**
   You can add as many regular expressions as you want in this dialog box. Note that you need to create a new rule for each expression that you want to search for, and each rule is applied to only one log file. In other words, each rule includes one regular expression and one log file.
9. Select a regular expression in the **Regular expression** drop-down list.
10. Enter the path and complete filename of the log file you want to monitor in the **Log file path** box. This must be a specific filename, and only that filename will be monitored (for example, c:\logs\error.txt)
11. If you want to include backup files for the log file, enter the path and complete filename of the backup file in the **Backup log file path** box (this step is optional). This also needs to be a complete path and filename for a specific file.
12. Type an **Instance** descriptive name. This identifies the log file monitoring rule in the alert notifications you receive.
13. Select the severity level you want to apply to this alerting rule.
14. If you want to monitor only new entries in the log file (beginning at the time the monitoring rule is deployed to the device), click **Monitor changes to log files.** (This option is typically used for log files so the agent doesn’t keep scanning the same existing text.)
   If you want to monitor all existing and all new entries in the log file, click **Monitor entire log file.** (This option is typically used to monitor other less dynamic files, such as configuration files.)
15. Click **OK** to add the rule to the list of logfile monitoring rules.
16. Repeat steps 4-15 to add other logfile monitoring rules.  
   After you have created the logfile monitoring rules you want, you need to add them to the ruleset. You can add multiple monitoring rules and apply action and time rules to them, depending on how you want to be notified when log file changes trigger alerts.

17. With the rules listed under **Log file monitoring**, click **Rule > New** in the right column. Three boxes or “wells” are displayed at the bottom of the page.

18. Drag one or more rules into the **Alerts** box.

19. Click **Actions** on the left column, then drag one or more action rules into the **Actions** box. The actions you add here will be applied to each rule that you added.

20. Click **Time** on the left column, then drag a time rule into the **Time** box.

21. Click **OK** to add the new rules to the ruleset.  
   To view the new logfile monitoring rules in the ruleset, click **Rules summary**. Each rule is displayed on a separate line, and you can edit individual rules or clone a rule and make copies with different actions, time rules, or severity states. If you want the alerting rule to affect device health, double-click the rule in the **Rules summary** list and select the **Health** check box.

22. After you have added the log file monitoring rules to the ruleset, click **Publish** to save the changes to the ruleset. The changes will be applied to individual devices the next time you deploy the ruleset, or the next time the device's inventory service runs.

**Notes**

- Log file monitoring is supported only for managed Windows devices.
- Any time you edit or delete a rule, you need to publish the alert ruleset that the rule appears in. The changes you make will not apply to devices until the ruleset has been published (or until you redeploy the ruleset with a scheduled task).
- This feature maps log files into memory to use less memory during a search. Runtime memory is allocated for this as linear regular expression searches occur. Because Windows locks the file when it is mapped into memory, you may encounter issues with some applications.

**Managing Dell DRAC devices**

Ivanti® Endpoint Manager powered by Landesk 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, Endpoint Manager 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 Endpoint Manager you can also open this utility directly from the Endpoint Manager interface.

In addition, Endpoint Manager 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 Endpoint Manager 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 Endpoint Manager**

Three logs from the OpenManage Server Administrator utility are displayed in the Endpoint Manager 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 Endpoint Manager 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 Endpoint Manager 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, Endpoint Manager only defines usernames at the Administrator level.

To add or edit usernames and passwords for a DRAC-enabled device

1. In the Endpoint Manager 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

Ivanti® Endpoint Manager powered by Landesk 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 Endpoint Manager 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 Ivanti 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>BMC only*</th>
<th>BMC + agent</th>
<th>Agent (no IPMI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-band management enabled</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>In-band management enabled</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Device can be discovered**</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Read environment sensors</td>
<td>X</td>
<td>X</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Power on/off remotely</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Read &amp; clear event log</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Configure alerts</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Read OS information</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Graceful shutdown</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Read SMBIOS information (processor, slots, memory)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>IP syncing (OS to BMC)</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>BMC only*</td>
<td>BMC + agent</td>
<td>Agent (no IPMI)</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Watchdog timer</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>BMC communicates with core server</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Local Endpoint Manager components communicate with core server</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Full range of Endpoint Manager management features</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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, detect that 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, Endpoint Manager 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 Endpoint Manager agents with IPMI management features.

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.
CAUTION: 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 Endpoint Manager from successfully communicating with IPMI-enabled devices.

The following configuration options are available:

- "Changing watchdog timer settings" (924)
- "Changing power configuration settings" (925)
- "Changing BMC user settings" (925)
- "Changing the BMC password" (926)
- "Changing LAN configurations" (926)
- "Changing Serial Over LAN (SOL configurations)" (928)
- "Changing IMM configurations" (928)

### 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). Endpoint Manager 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 Endpoint Manager 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 Endpoint Manager 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 **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

Endpoint Manager authenticates to a BMC with a user name/password combination that is unique to the BMC (separate from any other Endpoint Manager user names). Endpoint Manager 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 Endpoint Manager 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 **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. Type a user name.
6. To set a password, select the Set password check box, then type the password and confirm it.
7. Select the privilege levels for LAN and serial access.
8. Click Save changes.

**Changing the BMC password**

Endpoint Manager 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 Endpoint Manager 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 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.

> CAUTION: If you choose to set a 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 Endpoint Manager 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 **LAN configuration**.
4. Select **Always available** in the LAN communication 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 steps below).
10. Click **Apply** to save your changes.

**NOTE:** 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 **Acknowledges 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.

**CAUTION:** 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 Endpoint Manager 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 **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 Endpoint Manager 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 **IMM configuration**.
4. Select the check 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, and HTTPS.

5. Click **Apply**.

**Configure device monitoring alerts**

If you want device monitoring to notify you when managed devices come online or go offline, you must 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 need to define each 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 box 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**.
14. Click **Publish** to publish any changes you made and close the **Ruleset** window.

**NOTE:** When you configure alert settings, they apply to all of the devices you’re monitoring.
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.

Click here for details about the Configure device monitoring dialog box

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 box 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.

Turning off the ModemView service

The ModemView service is the service/driver that monitors modem calls (both incoming and outgoing) and generates an alert if it sees one. This service uses about 10 Mb of memory because it uses MFC. You may not want it to be running, especially if you don’t have a modem on the device.

To turn the ModemView service off

1. On the device (either directly or via remote control) click Start > Control Panel > Administrative Tools > Services.
3. Under Startup Type, select Manual, and click OK.
You can also click **Stop** under **Service Status.**
Intel vPro

Provisioning Intel vPro devices

To enable vPro provisioning in an Ivanti environment, simply enter a password in the Intel vPro general configuration dialog box. In most cases, this is all that is required to provision and manage all vPro machines on your network.

The Intel vPro general configuration dialog box lets you enter and change the password used with the default vPro administrator account. This password is applied to all new Intel vPro devices during the provisioning process. You can also change this password on all currently managed Intel vPro devices. If a vPro password has been previously set on a device not managed by the current Core, the password will not be changed. The device will not be provisioned until the local password matches the password on the Intel vPro general configuration dialog box or the machine has been Full Unprovisioned in the ME BIOS.

NOTE: Intel vPro requires the use of a strong password to enable secure communications. Passwords should meet these requirements.

Provisioning methods

There are three main methods available for provisioning vPro.

1. Host Based provisioning – zero-touch (version 6.2 and above)
2. Remote provisioning – zero-touch (version 2.3 and above)
3. Options available via the Ctrl-P menu on the vPro machine – one-touch
   - Provisioning ID / Provisioning Pass phrase (PID/PPS)
   - Manual vPro enablement via firmware

The first two options are zero-touch. This means provisioning can be accomplished through the network and physical access to the device is not required. The third method requires someone to visit each device to enable vPro options using a setup utility. This utility is accessed at boot time before the OS is loaded.

NOTE: The only time you should have to use the third option is if you have older vPro devices (pre 6.2) and you cannot implement the certificate infrastructure required for remote configuration.

Supported vPro versions

Ivanti provides support for provisioning and management of vPro version 2.3 up to the latest version (currently 9.x). Both Client Control Mode and Admin Control Mode are supported in version 6.2 and later.
The following graphic outlines the type of provisioning available for each version of vPro.

![Provisioning Diagram]

**NOTE:** PID/PPS is no longer available in version 9. Version 9 also requires a new API – WS-MAN. Hello Packets are also phased out beginning with version 6.2.

### Configuring Intel vPro devices

Devices equipped with Intel vPro functionality should be configured (or “provisioned”) 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.
Intel vPro provisioning options

There are three general ways you can provision Intel vPro devices. The provisioning method you use depends on the Intel AMT version number of the devices you manage and also on your own preferences. Information about each provisioning method is provided in other help topics as noted below.

One-touch provisioning (using provisioning IDs)

With one-touch provisioning you can use Endpoint Manager 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.

For more information, see “Using provisioning IDs (one-touch provisioning)” (939).

Zero-touch provisioning (remote configuration using certificates)

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 Ivanti 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.

For more information, see "Remote provisioning (zero-touch provisioning)” (937)

Automatic provisioning for Intel vPro 6.2 and higher

Endpoint Manager automatically provisions Intel vPro devices with AMT version 6.2 and higher. If you have entered a password in the Intel vPro General Configuration dialog box, but you have not set a PID on the devices or provided a zero-touch certificate, your devices are provisioned using Client Control mode. This mode limits some Intel vPro functionality, reflecting the lower level of trust required to complete the device setup.

If you have entered a password in the Intel vPro General Configuration dialog box and you have either set a PID on the devices or you have provided a zero-touch certificate, devices are provisioning using Admin Control mode, which has no limitations to Intel vPro functionality, reflecting the higher level of trust associated with the device setup.

For more information, see "Host-based provisioning (automatic provisioning)” (937).

NOTE: 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.

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 Ivanti 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 Ivanti agents, you can’t push an agent configuration, 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 the share where you have saved a self-contained client installation package and running the executable file for the agent configuration.

Before pulling the agents, we recommend that you change a setting in the Configure Services utility that forces the core server to check for the AMT GUID as part of identifying a device.

**To use the AMT GUID as an identity attribute**

1. Click **Start > Ivanti > Ivanti 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.

**Intel vPro general configuration**

The General Configuration dialog box includes configuration options that you must set before you can manage Intel vPro-enabled devices.

**NOTE:** Enter a password in this dialog box only if you intend to enable Intel vPro features for applicable managed devices. The password is saved in the database and applied globally for provisioning Intel vPro devices, so you must understand how to set up and configure each version of Intel vPro devices.

**Setup and Configuration**

The Intel vPro General Configuration dialog box lets you change the password used with the default "admin” account. This password is applied to all new Intel vPro devices when you provision them. You also have the option of changing this password on all currently managed Intel vPro devices. This option is recommended so that all devices will have the same credentials.

- **Password:** Enter a secure password to communicate with and to provision new Intel vPro devices. For devices that you will manage, the "admin" 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 box. This password is saved in the database and applied globally for provisioning Intel vPro devices.

- **Synchronize to all managed vPro machines when password is modified:** Select this check box to apply the password to all currently managed Intel vPro devices.

**Using a strong password**

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)
Automatic provisioning for Intel vPro 6.2 and higher

Endpoint Manager automatically provisions Intel vPro devices with AMT version 6.2 and higher. If you entered a password in this dialog box, but you have not set a PID on the devices or provided a zero-touch certificate, your devices are provisioned using Client Control mode. This mode limits some Intel vPro functionality, reflecting the lower level of trust required to complete the device setup.

If you have entered a password in this dialog box and you have either set a PID on the devices or you have provided a zero-touch certificate, devices are provisioning using Admin Control mode, which has no limitations to Intel vPro functionality, reflecting the higher level of trust associated with the device setup.

Host-based provisioning (automatic provisioning)

Ivanti® Endpoint Manager powered by Landesk automatically provisions Intel vPro devices with AMT version 6.2 and later. If you entered a password in the Intel vPro general configuration dialog box and you have not set a PID on the devices or provided a provisioning certificate, your devices will be provisioned using Client Control Mode. This mode limits some Intel vPro functionality due to the lower level of trust required to complete the device setup. If a provisioning certificate is present on the core, the device will be provisioned using Admin Control Mode.

NOTE: Host-based provisioning does not require any configuration at the client. A vPro-capable machine (version 6.2 and later) will be provisioned during the Ivanti agent install if the vPro password has been entered at the core.

Remote provisioning (zero-touch provisioning)

For vPro devices with AMT version 2.3 and later, zero-touch provisioning is still possible. Remote provisioning lets you configure a vPro device in a factory default state to a fully provisioned state (Admin Control Mode) through the use of SSL certificates created specifically for vPro management.

Remote provisioning prerequisites

There are two main requirements for remote provisioning to work:

1. Provisioning certificate
2. DHCP option 15 support
Provisioning certificate

Intel requires a certain level of nonrepudiation in order to allow vPro provisioning to occur. This removes the burden of secure identity verification from the end user. For example, when a machine is provisioned in Client Control Mode, the user will be required to allow a KVM session. When the KVM session is initiated from the console, the user is prompted with a 6-digit number in a pop-up window. The user must then contact the person who initiated the KVM session (typically by phone) and relay the 6-digit code. This puts the burden of security on the end user. While this is acceptable in some environments, many organizations want to leverage infrastructure to provide a secure environment without interrupting the end user. Using certificates, a machine can be provisioned in Admin Control Mode and the end user is not required to relay the code.

With the provisioning certificates in place on the core, remote provisioning is as seamless and easy as host-based provisioning. When the agent is installed on the machine, vPro is provisioned in Admin Control Mode. This is accomplished through an exchange of certificate information and leverages organizational naming.

The following are the steps that occur between a vPro device and the Ivanti core during the Ivanti agent installation. The first step has been modified to reflect the Ivanti implementation.

1. The Ivanti web service receives a provisioning request from the vPro device during agent install. This initiates the provisioning process.
2. The provisioning server (Ivanti core server) sends the provisioning certificate to the client with the certificate’s full chain of trust including the root certificate via a secure AMT API call. This root certificate would reflect the certificate authority vendor used and will include the certificate authority vendor’s thumbprint.
3. The AMT firmware on the client computer parses the provisioning certificate, verifies that the chain of trust is not broken, extracts the root certificate thumbprint and compares it against the thumbprint’s table present in the client’s Intel® AMT firmware. Provisioning stops here if no match is found.
4. The client computer gets the domain from DHCP Option 15 setting and verifies that the suffix matches the CN field from the certificate. The way a match is determined depends on the client computer’s Intel® AMT firmware version and the provisioning certificate type used. Provisioning stops here if no match is found.
5. The remote configuration certificate is now successfully verified and provisioning process continues as normal.


Obtaining and installing an Intel Provisioning Certificate

An Intel Provisioning Certificate is required for remote configuration. The certificate must be purchased from an approved certificate vendor (Verisign, GoDaddy, etc) and must be a supported class.
NOTE: Before you purchase a certificate, verify in the vendor’s documentation or support information which certificates are supported on your device.

When you purchase a certificate, you need to provide a CSR (certificate signing request) file to the vendor you are purchasing the certificate from. This file is generated for your Ivanti product along with a private key file. You must specify the correct DNS domain information as part of the CSR process to ensure it matches your DNS infrastructure. 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.

Once the provisioning certificate has been obtained, it needs to be stored on the Ivanti core. Copy all the certificate files (including the private key generated by the CSR process) into the folder:

```
\<name of Ivanticore server>\vant\Endpoint Manager\amtprov\certStore\cert_1
```

For further information on obtaining and managing provisioning certificates, please visit the Ivanticommunity website: https://community.landesk.com/support/docs/DOC-23304

**DHCP option 15**

DHCP option 15 is required during remote provisioning. This option returns the DNS domain name information as part of the DHCP response from the attached router. As mentioned in step 5 above, the client verifies that the suffix returned by DHCP (for example, landesk.com) matches the CN field from the provisioning certificate for another level of validation in the provisioning process.

NOTE: Remote Provisioning will only work if DHCP option 15 is turned on at the router and the suffix of the certificate matches the client DNS domain information at the vPro device. The Ivanticore server must also have the same DNS domain suffix as specified in the provisioning certificate.

**Using provisioning IDs (one-touch provisioning)**

Intel vPro devices communicate with a provisioning server on the network. This provisioning server listens for messages from Intel vPro devices 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.

Generate a Provisioning ID (PID) and a Provisioning Passphrase (PPS) for every Intel vPro device you want to provision. A PID is an eight-character encrypted ID used to ensure that the user has the credentials necessary to configure an Intel vPro device. A PPS is a 32-character password to authenticate the PID. The PID and the PPS are matched against each other.

**Process for using Intel vPro provisioning IDs**

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 Endpoint Manager 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 Endpoint Manager 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.

1. Specify a new, strong password for provisioning Intel vPro devices.
2. Generate a batch of Intel vPro provisioning IDs (PID and PPS). Print the list of keys or export them to a USB drive.
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.

For detailed instructions for step 1, see "Change the Intel vPro password" (951)

For detailed instructions for step 2, see "Generate a batch of Intel vPro provisioning IDs" (943)

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 provisioning IDs

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

Endpoint Manager 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. The number of IDs available to export is displayed in parentheses next to this option.
3. Enter and confirm the vPro Management Engine password. This is the password that allows you access to Intel vPro management features. The default password is "admin" if you have not already set a password for the Management Engine.
4. Enter a value in the Number of IDs to export text box. 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. In the Specify the location for setup.bin text box, enter a path or browse to the folder where you want to save the setup.bin file.

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, and then click Close.

NOTE: The IDs you generate are listed with other IDs you have generated on the Generate Intel vPro IDs page. The IDs will have a green check mark 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, and then click Close.

The provisioning IDs are added to the core database and are listed on the Generate Intel vPro IDs dialog box.

Generate a batch of Intel vPro provisioning IDs

IMPORTANT: Before you generate Intel vPro IDs, you must first create an Intel vPro password for the default “admin” account, and must synchronize the password with all managed Intel vPro devices. "Changing the password for Intel vPro devices" on page 951.
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 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 6 characters for a prefix.
4. Type a batch name to identify this group of generated IDs.
5. Click **Generate IDs**.
6. To view one batch of generated IDs, select the batch name in the **View batch IDs** list.
7. To print a list of the generated IDs for your reference, click **Print ID list**. The Windows print dialog box opens; select a printer and click **Print**.

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.

**Notes on provisioning keys**

A PID prefix can be 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 6 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.

**Click here for descriptions of the Intel vPro IDs options**

**Generate IDs**

Use this section to enter the criteria for generating the PID and PPS.

- **Number of IDs to generate**: enter the number of IDs you want to generate (usually the number of devices you plan to provision). You must enter a value or the IDs can't be generated.
- **PID Prefix for generated IDs**: Enter a prefix to help identify the PIDs. 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 6 characters for the prefix.
Batch name of generated IDs: Enter a name to identify the batch of generated IDs. It 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, select the batch name in the View batch IDs list to see those IDs.

View batch IDs

The View batch IDs drop-down list shows the batch names you have assigned to IDs. The IDs available in the selected batch name are displayed in the list box.

These IDs 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 displays a green check mark next to the IDs that have been used.

Import/Export IDs

The IDs you generate can be exported to a file named setup.bin. The setup.bin file can be stored on a USB drive that can be transported to other provisioning servers so that IDs that have not already been used can be imported and put to use with other Intel vPro devices.

Print ID List

The Print ID List feature prints the IDs currently displayed in the list. Select a batch name from the View batch IDs list; only the IDs in that batch are printed.

Discovering vPro devices

A separate discovery process is not required to identify vPro-capable devices. Use the standard Ivanti Unmanaged Device Discovery (UDD) process to find all devices on your network.

vPro and the agent install

During the installation of the Ivanti agent, a call is made to the vPro firmware to determine vPro version information, status, and capability. This information is sent back to the core and determines how to provision vPro on each machine and what vPro features are supported.

The following image shows the type of information that is sent to the core during agent install. This information is used during the provisioning process and can also be used for reporting purposes or as an input to a query.
**Intel vPro management features**

After you [provision an Intel vPro device](#) and it appears in the Ivanti inventory database, several management features are enabled. To access these features, right-click the device name in the Network view and select **Intel vPro options**.

The enabled features and amount of visible data depends on whether the device has been provisioned and whether the device is in Client Control Mode or Admin Control Mode. The version of Intel vPro on the device may also determine which menu options are displayed. The Intel vPro Options menu item will not be displayed for non-vPro devices.

Hardware vendors have the responsibility for the vPro implementation on their devices. This can result in only a subset of features available on a given device.

**Intel vPro status**

The Intel vPro status dialog box displays current information about the Intel vPro features that have been enabled and are in effect on the device. This includes general information, power settings, wireless profile, agent presence, system defense, network environment detection, and remote access settings. Features that are not supported on the device appear dimmed.

**Configuring remote KVM access**

You can use KVM access to remotely manage Intel vPro devices (AMT version 6 or later). This allows an IT admin to view the full screen of the client device with complete keyboard, mouse, and video control of the device.

When an AMT device is provisioned, KVM function is enabled by default. However, User-Consent is on. To override this option, disable the KVM default on the core. KVM function is restricted to a licensed core or console. A standalone remote control viewer is unable to use KVM function.
To configure KVM settings on a client

1. Click Configure > Intel vPro Options > KVM Configuration.
2. In the KVM Enablement box, click Enable KVM to enable KVM usage.
3. In the Default User Consent Policy box, select Enable user consent and timeout after and enter a number (in seconds) after which a user must provide a one-time password to the console operator.
4. If you choose not to use the user consent option, click Disable User Consent.
5. In the Session Timeout box, enter a number (in minutes) a remote control TCP session can go inactivity before a session closes. This is disabled if User consent is disabled (previous step).
6. Click OK.

KVM is accessed from the right-click menu at the Ivanti console. The KVM Remote Control option will only appear on devices that have been provisioned, KVM enabled, and that support KVM.

Note: vPro KVM will only work with a device that has integrated graphics. A machine with a discrete graphics chip-set cannot be remote controlled through vPro and the KVM option will not appear in the right-click menu.

KVM restrictions

- KVM does not support applicable remote control policy settings.
- No “view only” or “permission required” remote control policy can be applied to KVM connection. The “permission required” can be treated as “user consent code required” option in AMT configuration and that should be set from AMT setting instead of from the RCViewer.
- KVM does not support the remote control options in the agent configuration.
- KVM does not support File transfer, Remote Execute, Chat, and Draw features with KVM connection.
- KVM does not support the remote control blank screen option.
- If the client machine is provisioned into Client Control Mode, User Consent cannot be disabled.

System defense with remediation

Intel vPro System Defense technology allows network isolation at the level of the Intel AMT chip. Systems that have been compromised and are a threat to the network can be remotely quarantined with the vPro IP addresses remaining open for remediation without posing a threat to the rest of the network. This is a manual process that is accessible from the right-click menu option at the Ivanti console.
Once the machine has been remediated you can restore the network connection to the device. This option is located in both the right-click menu and in Intel vPro general configuration dialog box. When you select **System Defense Remediation**, you will be presented with a list of devices that have been removed from the network. Simply select the devices you wish to restore and click **Remediate**. You will see a pop-up window indicated success or failure of the restore.

The **Client Notification Strings** dialog box allows you to configure whether a notification is shown on the client machine when it is removed and/or restored to the network.

### Accessing devices provisioned with TLS

When you provision an Intel vPro device, the core server installs a certificate on the device for secure https communication. If the device is to be managed by another core server, it must be re-provisioned by the new core server. It is not necessary to un-provision the device before re-provisioning. Certain Intel vPro features will not respond until the device has been re-provisioned 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 or credentials.

### Power management and IDE redirection

Ivanti® Endpoint Manager powered by Landesk includes options to power on and power 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 Endpoint Manager initiates power option commands, it is not always 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 select **Wake up devices** in a scheduled task, Ivanti® Endpoint Manager powered by Landesk 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 following reboot options are available:

- **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.
- **Default Device**: 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.
- **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 the following section.

**IDE redirection options**

When using IDE redirection, make sure that the CD image files are in .iso format or on a physical CD/DVD disc installed on the console’s local computer. Some BIOS may require the CD image to be located on a hard drive.

AMT 9 and later devices support graceful power off and reboot. Older devices do not.

**Intel vPro network security policies**

Intel vPro includes a System Defense feature, which enforces network security policies on managed devices. Ivanti® Endpoint Manager powered by Landesk applies a System Defense policy to Intel vPro devices. Each 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 disconnected from the network until you reconnect the access using the System Defense Remediation feature.

**How Intel vPro System Defense policies are applied**

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 System Defense policy on the device.

**Intel vPro System Defense policies**

Intel vPro System Defense technology allows network filtering at the level of the Intel AMT chip. Systems that have been compromised and are a threat to the network can be remotely quarantined, with certain ports and IP addresses remaining open for remediation, without posing a threat to the rest of the network.

Ivanti® Endpoint Manager powered by Landesk contains the following predefined System Defense policies.

- **BlockFTPsrv:** 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:

<table>
<thead>
<tr>
<th>Port description</th>
<th>Number range</th>
<th>Traffic direction</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ivanti management</td>
<td>9593-9595</td>
<td>Send/receive</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Intel vPro management</td>
<td>16992-16993</td>
<td>Send/receive</td>
<td>TCP only</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>Send/receive</td>
<td>UDP only</td>
</tr>
<tr>
<td>DHCP</td>
<td>67-68</td>
<td>Send/receive</td>
<td>UDP only</td>
</tr>
</tbody>
</table>

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.
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 "admin" 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 box. That password is saved in the Endpoint Manager 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 Endpoint Manager to communicate securely with managed Intel vPro devices.

Host-based provisioning for Intel vPro 6.2 and higher

Endpoint Manager uses host-based provisioning for Intel vPro devices with AMT version 6.2 and higher. If you have entered a password in the Intel vPro General Configuration dialog box, but you have not set a PID (one-touch provisioning) on the devices or provided a zero-touch certificate, your devices are provisioned using Client Control mode. This mode limits some Intel vPro functionality, reflecting the lower level of trust required to complete the device setup.

If you have entered a password in the Intel vPro General Configuration dialog box and you have either set a PID on the devices or you have provided a zero-touch certificate, devices are provisioning using Admin Control mode, which has no limitations to Intel vPro functionality, reflecting the higher level of trust associated with the device setup.

Change the Intel vPro password

To change the password for all Intel vPro devices

1. On the core server, click Configure > Intel vPro options > General configuration.
2. Type a strong password and confirm the password.
3. To apply the password to all currently managed Intel vPro devices, select Synchronize to all managed vPro machines when password is modified.
4. Click OK.
This change will be made when the client configuration is run.

To change the password for one Intel vPro device

1. In the All devices list, right-click a managed Intel vPro device and select Intel vPro options > Change Password.
2. Type the new password, then confirm the password.
3. Click OK.

Editing Intel vPro client notification strings

You can send a message notifying a user when Intel vPro System Defense has detected a problem and disconnected the user’s device from the network. A message box is displayed on the device when it is disconnected from the network, and a second message is displayed after the issue has been resolved and the device has been reconnected to the network (removed from the remediation queue) by the administrator.

Use this dialog box to enter the notification strings that are displayed on managed devices. You can use default message text or you can customize the message.

To use message notifications for Intel vPro System Defense

1. Click Configure > Intel vPro options > Client Notification Strings.
2. Select the Enabled check box to send messages when a device’s network access is disconnected.
3. To customize a message, replace the default text with the message you want to display on the client devices.
4. Click OK.

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, Intel vPro uses the device's Windows wireless profile.
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.

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.
Rollup cores

Installing a rollup core

You can use a rollup core to combine the data from multiple core servers. Ivanti® Endpoint Manager powered by Landesk uses native SQL Server replication to roll up core data. You can use a rollup core database to generate reports based on data from all cores in your organization. You can’t schedule tasks from a rollup core database.

You can roll up data from cores using Endpoint Manager version 9.0 or later. The rollup core must be installed from the latest Endpoint Manager version. All cores must be using the same database type, and SQL Server Express isn’t supported.

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 Endpoint Manager installation. For information on installing the database, see the Ivanti community at https://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 Endpoint Manager installation source. Finish setup.

Configuring SQL server replication for rollup cores

Ivanti® Endpoint Manager powered by Landesk uses native SQL Server replication to roll up data from core servers to a rollup core server. SQL Server replication is almost real-time and extremely efficient, so your rollup database content will be much more current than it was with the old rollup database utility that was used prior to Endpoint Manager 9.6.

Prerequisites

The following pre-requisites must be performed before using SQL Server replication in a rollup core scenario.

- Make sure the Endpoint Manager Setup program’s Replication option is installed on each DBMS SQL Server (publishers and subscriber) that you want to participate in replication. You can verify this by running the SQL Server setup.exe.
- One of the limitations of SQL Express is that it cannot act as a publisher in a replication topology. Therefore, you cannot replicate data from a Endpoint Manager core server using SQL Express as the back-end database.
- Make sure KB2840628v2 is installed (publishers and subscriber DBMS servers). Under "Microsoft .NET Framework 4 Client Profile" updates. If you have KB2840628 installed, make sure it is KB2840628v2. Reinstalling will update it to v2.

**Step 1: Create Windows accounts (publisher and subscriber DBMS servers)**

Using the following table, create Windows user accounts on the machines you have installed Microsoft SQL Server. The "publisher" is the SQL Server hosting the core server’s database. The "subscriber" is the SQL Server hosting the rollup database.

<table>
<thead>
<tr>
<th>User name</th>
<th>SQL Server</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldms_snapshot</td>
<td>Publisher</td>
<td>Used by the replication Snapshot Agent</td>
</tr>
<tr>
<td>ldms_logreader</td>
<td>Publisher</td>
<td>Used by the replication Log Reader Agent</td>
</tr>
<tr>
<td>ldms_distribution</td>
<td>Publisher and Subscriber</td>
<td>The passwords must match on both the Publisher and Subscriber or the Publishers’ Distribution Agent will not be able to connect to the Subscriber database.</td>
</tr>
</tbody>
</table>

**Step 2: Create a replication share and assign Windows user permissions (publisher DBMS servers)**

On the SQL Server hosting the core server’s database (publishers) navigate to the SQL Server folder and create a folder named ReplData if one doesn’t already exist. The default location is:

```
C:\Program Files\Microsoft SQL Server\MSSQL.X\MSSQL\ReplData
```

Share this new folder as ReplData and make sure that the following users have the following permissions in both the Advanced sharing permissions (the Sharing tab) and the Group or user names portion of the Security tab.

```plaintext
C:\Program Files\Microsoft SQL Server\MSSQL.X\MSSQL\ReplData
```

<table>
<thead>
<tr>
<th>Account name</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;computer_name&gt;\ldms_snapshot</td>
<td>Full control</td>
</tr>
<tr>
<td>&lt;computer_name&gt;\ldms_distribution</td>
<td>Read</td>
</tr>
</tbody>
</table>
Step 3: Grant Modify permissions to the distribution user in the SQL Server COM directory (subscriber DBMS server)

On the SQL Server hosting the rollup core server’s database (subscriber), navigate to the SQL Server folder and locate the COM directory. The default location is:

C:\Program Files\Microsoft SQL Server\<latest version>\COM

While highlighting the COM folder, right-click and choose Properties. On the Security tab, add the distribution user to the Group or user names section and click Modify to give the user all rights except for Full control.

Step 4: Configure SQL Server Agent to start automatically (publisher and subscriber DBMS servers)

On the publisher, the SQL Server Agent service needs to start automatically in order for replication to succeed. Do the following:

1. Open the Windows Services dialog by clicking on Start > Run and entering services.msc.
2. Double-click the SQL Server Agent (MSSQLSERVER) service and change the Startup type to Automatic.
3. Click Start to start the service.

Step 5: Allow the SQL Server port to communicate through your public firewall (publisher and subscriber DBMS servers)

On the publisher and each subscriber:

1. From Windows Control Panel, launch Windows Firewall. On the left side, click Advanced settings to open the Windows firewall with advanced security dialog box.
2. Click on Inbound Rules, and on the right click New Rule.
3. Click Port and click Next
4. Click TCP, and next to Specific local ports enter the TCP port number that the SQL Server Agent is configured to use (the default port is 1433). Click Next.
5. Click Allow the Connection and click Next.
6. On the **Profile** page, make sure you leave the options selected (**Domain**, **Private**, or **Public**) that are required in your environment to ensure that all of the SQL Servers can communicate with each other. Click **Next**.

7. Name your rule so you know what it is, something like “SQL Server Replication.” Click **Finish**.

**Step 6: Run the replication definition tool and enter database credentials and publisher information (subscriber DBMS server)**

On the subscriber, run the Ivanti replication utility:

C:\Program Files\LANDesk\ManagementSuite\LANDesk.Database.Replication.exe
Use this utility to enter the database server Windows authentication credentials and publisher definitions.

IMPORTANT: Clicking OK in the replication utility drops all tables in the rollup database so that replication data can be rebuilt from all publishers. Depending on your database sizes, this may take a while. If you haven’t made changes in the utility, click Cancel to exit it instead so the rebuild doesn’t happen.

To enter database server Windows authentication credentials

1. In the Ivanti replication definition utility, click Replication user passwords.

2. Enter your snapshot, logreader, and distribution usernames and passwords.
3. Click OK.

To enter publisher definitions

1. In the Ivanti replication definition utility, click Add.
2. In the **Core server** field, provide a descriptive name. This field is only used to help you organize your publishers.

3. Fill in the remaining fields and click **OK**. If the information you entered isn't correct, the utility will show an error message.

4. Repeat for each core server publisher.

**Step 7: Start replication in SQL Server Management Studio on the publishers**

Inside SQL Server Management Studio on the publishers:

1. Expand **Server > Replication > Local Publications**. Right-click on [DB]: LANDesk and choose **View Snapshot Agent Status**.
2. If it hasn’t started yet, click **Start**.
3. Verify it was successful.
4. Right-click on **Replication** and choose **Launch Replication Monitor**. Verify it is running and that no errors have occurred.

At this point, replication is working. You can further verify it by querying your rollup database.

**Notes**

- If you upgrade a core that is also a publisher, the upgrade will stop replicating the core’s database and you will need to rerun LANDesk.Database.Replication.exe to reinitialize the replication process.
Changing the replication schedule

By default, the subscriber pulls transaction logs from the publishers every 30 seconds. You can change this schedule if necessary. Each publisher has its own replication schedule and they don’t all have to be the same.

To change a publisher’s replication schedule

1. On the subscriber, open SQL Server Management Studio and click SQL Server Agent > Jobs.
2. Right-click the job you want to modify and click Properties.
3. Open the Schedules page, double-click the replication schedule, and make your schedule modifications.

Troubleshooting

I can’t open the Endpoint Manager console after replication due to a licensing error.

You must have at least one 9.6 or later core server listed as a publisher. That core server must be authorized.

Troubleshooting rollup replication errors

Don’t directly modify rollup database data

Ivanti implements SQL Server replication as a one way transactional replication, from the publisher to the subscriber. If you modify “replicated” data on the subscriber, those changes will not be replicated to the publisher. Furthermore, the publisher will not be aware of those changes. If you want to roll back those changes, you will have to use SQL Server’s Replication Monitor and invalidate the snapshot from that publisher and force a new snapshot.

ProductSnapshot replication error after upgrading Endpoint Manager versions

If you see this error message:

The process could not bulk copy into table "dbo"."PRODUCTSnapshot"

The problem is that the ReplProductV view in the upgraded core is out of sync with the older ProductSnapshot table in the rollup database.

To fix this error, the view needs to match the schema. Run sp_help on both the view and the table and make sure the "Nullable" columns match. More than likely, it will be the Version and ProductGUID columns that are out of sync. You can either modify the table in your rollup database (but you would have to alter the views in each non-upgraded core as well):

```sql
alter table productsnapshot alter column version nvarchar(9255) not null
alter table productsnapshot alter column productguid nvarchar(255) not null
```
Or you can modify the view in your upgraded core. In order to modify the view, you will have to stop replicating that view within the properties dialog of the local publication.

**Field size too large replication error**

If you see this error in your replication monitor, the problem is that the view on the core and the table on the rollup have mismatched schemas. While it could be a mismatch in the lengths of the columns, normally this is a mismatch of the NOT NULL attribute of the column. All of the column definitions between Repl<tablename>V on the core and the table name of the rollup must match.

If the error lists a table that ends with Snapshot, that table is used as a temporary table on the rollup. The corresponding view on the core will not contain the word “Snapshot” (e.g. ProductSnapshot = ReplProductV).

**Replication errors with the ISA and IDE tables**

**Problem:** When using an older (or upgraded) version of the Ivanti database, you may run into replication errors with the ISA and IDE tables. The identity columns in the ISA and IDE tables were renamed in 2011.

**Resolution:** Once replication is running, you need to drop the subscriptions and articles for both the ISA and IDE tables. Alter the views and use the old identity column names in the SELECT clause. Create the UNIQUE CLUSTERED indexes for the views and re-add the articles and article filters. Refresh the subscription. Finally, you can manually click on start within the Snapshot Agent Status widow, or wait for the snapshot agent to detect the changes. Consult the Replication Monitor to see that the data is successfully replicated.

Use the script below to fix the problem. Make sure you use the name of your subscriber and database (&lt;your subscriber server name&gt; and &lt;your subscriber database name&gt;) in the sp_dropsubscription procedures.

```sql
--Drop the subscription and article for the ISA table
sp_dropsubscription 'LDMS', 'ISACSO', '<your subscriber server name>', '<your subscriber database name>'
go
sp_droparticle @publication = 'LDMS', @article='ISACSO'
go

--Alter the view for the ISA table and use the old ISAPorts_Idn column in the select list.
alter VIEW [dbo].[ReplISAV] (Computer_Idn, ISA_IDn, DeviceNum, Description, Designation, Location, Manufacturer, Type, COREGUID) WITH SCHEMABINDING AS
SELECT isnull((b.Computer_Idn + 2097152), b.Computer_Idn) Computer_Idn, isnull(cast(b.ISAPorts_IDn as int), cast(0 as int)) ISAPorts_IDn, isnull(b.DeviceNum, 0) DeviceNum, b.Description, b.Designation, b.Location, b.Manufacturer, b.Type, isnull(cast(a.SYSTEMGUID as uniquenidentifier), cast(0 as binary) as uniquenidentifier)) COREGUID FROM dbo.METASYSTEMS a, dbo.ISA b
WHERE a.SYSTEM_IDn = 0
GO

--Recreate the clustered index
create unique clustered index PKReplISAV on ReplISAV (CoreGuid, Computer_Idn, ISA_Idn)
go
```
--Add the article and filter back to the publication
sp_addarticle @publication = 'LDMS', @article='ISACSO', @source_object='ReplISAV', @destination_table='ISA', @type='indexed view logbased', @sync_object='ReplISAV', @pre_creation_cmd='delete', @schema_option=0x00, @status=24, @ins_cmd='CALL sp_LDins_ISA', @del_cmd='CALL sp_LDdel_ISA', @upd_cmd='MCALL sp_LDupd_ISA', @fire_triggers_on_snapshot='FALSE'
go
sp_articlefilter @publication = 'LDMS', @article='ISACSO', @filter_name='CoreGuidISA', @filter_clause='CoreGuid = cast(''C192290A-8FAC-4ABF-8183-D6B911ACFE73'' as uniqueidentifier)'

go
--Drop the subscription and article for the IDE table
sp_dropsubscription 'LDMS', 'IDECSO', '<your subscriber server name>', '<your subscriber database name>'
go
sp_droparticle @publication = 'LDMS', @article='IDECSO'
go

--Alter the view for the IDE table and use the old IDEPorts_Idn column in the select list.
ALTER VIEW [dbo].[ReplIDEV] (Computer_Idn, IDE_IDN, DeviceNum, Description, Designation, Location, Manufacturer, Type, ProdName, COREGUID)
WITH SCHEMABINDING AS
SELECT isnull((b.Computer_Idn + 2097152), b.Computer_Idn) Computer_Idn, isnull(cast(b.IDEPorts_Idn as int), cast(0 as int)) IDEPorts_IDn, isnull(b.DeviceNum, 0) DeviceNum, b.Description, b.Designation, b.Location, b.Manufacturer, b.Type, b.ProdName, isnull(cast(a.SYSTEMGUID as uniqueidentifier), cast(0 as binary) as uniqueidentifier) COREGUID
FROM dbo.METASYSTEMS a, dbo.IDE b
WHERE a.SYSTEM_IDN = 0
GO

--Recreate the clustered index
create unique clustered index PKReplIDEV on ReplIDEV (CoreGuid, Computer_Idn, IDE_Idn)
go

--Add the article and filter back to the publication
sp_addarticle @publication = 'LDMS', @article='IDECSO', @source_object='ReplIDEV', @destination_table='IDE', @type='indexed view logbased', @sync_object='ReplIDEV', @pre_creation_cmd='delete', @schema_option=0x00, @status=24, @ins_cmd='CALL sp_LDins_IDE', @del_cmd='CALL sp_LDdel_IDE', @upd_cmd='MCALL sp_LDupd_IDE', @fire_triggers_on_snapshot='FALSE'
go
sp_articlefilter @publication = 'LDMS', @article='IDECSO', @filter_name='CoreGuidIDE', @filter_clause='CoreGuid = cast(''C192290A-8FAC-4ABF-8183-D6B911ACFE73'' as uniqueidentifier)'

go
--Refresh the subscription
sp_refreshsubscriptions @publication='LDMS'
go
Preferred servers and content replication

Preferred servers and content replication overview

Preferred servers are a way Ivanti® Endpoint Manager powered by Landesk reduces distribution network traffic across subnets. Once configured correctly, preferred servers are included in the order distribution targets will look for distribution files:

1. The target’s local distribution cache.
2. Local peers on the same subnet as the target with source files in their distribution cache.
3. If configured, the closest preferred server.
4. The distribution source originally specified in the distribution package.

Content replication provides a management structure for establishing, synchronizing and updating the files on preferred servers with those on a source server. You don’t have to use content replication with your preferred servers, but using content replication allows administrators to easily ensure that files on the preferred servers throughout their environment are kept up to date on predefined schedules.

Content replication requires you to configure these elements:

- **Preferred server**: This is the server that distribution targets will try to download source files from. Software distribution can access files on preferred servers that were not replicated, though Content replication provides the best solution for keeping these files up to date.
- **Source**: This is the server that has files that need to be replicated to preferred servers. Administrators will set up file structures and files on the source, then use content replication to copy these hierarchies to preferred servers.
- **Replicator**: This is a managed Windows device that copies files from a source to a preferred server. This managed device should have a significant amount of disk space so it can keep data from all sources cached locally. If a managed device used for replication doesn’t have enough disk space, the replicator may have to download some files from the source each time it does a replication job.

Replicators can only replicate content from a source server to a preferred server. The replicated data doesn’t have to consist solely of software distribution data, as long as you don’t mind that data residing on a preferred server. For example, you can also replicate documents and spreadsheets to preferred servers located in remote branch offices.

You can have as many preferred servers, sources, and replicators as you want.
Configuring preferred 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 a preferred server will be available to.

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). UNC package shares work with all packages. HTTP package shares only work with MSI and SWD packages.

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, if available. 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 a WAN link for hashing, so hashing files on a server that’s local to the core will be much faster and use less 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 the list 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.

**Configure preferred 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 a preferred server will be available to.

**To configure preferred servers**

1. Click **Tools > Distribution > Content replication / Preferred servers.**
2. In the Content replication tree, right click **Preferred servers (Targets)** and click **New preferred server.**
3. On the Configuration page, enter the server information and read-only credentials. Click **Test credentials** to make sure the credentials are valid.
4. On the IP address ranges page, enter the IP address ranges you want this preferred server to allow.
5. On the **Selected replicator** pages, select the replicator, run options, and schedule. Click **Help** on each page for more information.
6. On the **Sources** page, select the source paths to be replicated.
7. On the **Write credentials** page, enter the credentials the replicator should use to write replicated files on the target preferred servers. Click **Test credentials** to make sure the credentials are valid.
8. Click **Save.**

**Storing preferred package servers in the registry**

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.
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.

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:

; 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

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 (Tools > Distribution > Content replication / Preferred servers), you also provide credentials that devices should use when accessing the preferred server. For security reasons, make sure these credentials are divided between read only and write access (for more information, see "About the Preferred server properties dialog box" (971)). Managed devices obtain read only credentials from the core and use them to authenticate with that preferred server when downloading a file.

When using preferred servers added to the Server Credentials dialog box, 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 Configuration dialog box), managed devices should be able to access the share.

Configure sources and mirroring

A source server hosts the files that need to be replicated to a preferred server. You can have as many source servers as you want. You’ll need to provide read-only credentials to the source server. On the source server, disable anonymous authentication to make sure the read-only credentials work with standard Windows authentication.

When replicating files from source servers, you have two choices for how to handle existing files on the preferred server’s destination share:

1. Leave the share’s existing files alone and just copy new/changed files.
2. Enable mirroring to copy new/changed files then remove existing files from the preferred server’s share that aren’t on the source server.

Be careful if you choose to enable mirroring. Existing files that aren’t on the source server for that share will be deleted. Be sure to move any important files that exist only on the preferred server share before you enable mirroring.

Also, if you enable mirroring, make sure there is only one source replicating data to the mirrored share. If multiple sources are replicated to a mirrored share, they will conflict, because the mirrored replication will delete data that isn’t part of the mirror.

To enable mirroring for a source

1. Click Tools > Distribution > Content replication / Preferred servers.
2. In the Sources tree, right-click the source you want to mirror and click Properties.
3. On the Mirroring page, select Enable mirroring.
4. Click Save.
Using a source representative

A source representative is a managed Windows device that indexes files on the source server. Source representatives are an optional part of content replication. If your source server has thousands of files, it can take a while for a replicator to index files on its own, especially if that replicator doesn't have a low-latency connection to the source. In this case, designating a managed Windows device near or on the source server to be a source representative can speed up replications, because the replicator can quickly retrieve the file index from the source representative.

Any managed Windows device can be a source representative. It doesn’t need to be a dedicated computer or a server. For it to be effective, it should be able to have a low-latency high-speed connection to the source server. If the source server is a managed Windows device (and not a SAN or Linux device, for example), the source representative can be on the source server.

The source representative uses the source server credentials you specify to build an XML file containing information about all files on the source share. It builds this file on-demand, but not more than once an hour. You don’t need to manually map a drive to the source server or create any network connections to the source server. That will be handled automatically by the management agents.

When a replication job starts that uses a source representative, the replicator will use the XML file from the source representative to decide which files need to be replicated. The source representative's involvement in the replication job is done once it passes the XML file to the replicator.

Assign a source representative

A source representative is a managed Windows device that indexes files on the source server. Source representatives are an optional part of content replication. If your source server has thousands of files, it can take a while for a replicator to index files on its own, especially if that replicator doesn't have a low-latency connection to the source. In this case, designating a managed Windows device near or on the source server to be a source representative can speed up replications, because the replicator can quickly retrieve the file index from the source representative.

Any managed Windows device can be a source representative. It doesn’t need to be a dedicated computer or a server. For it to be effective, it should be able to have a low-latency high-speed connection to the source server. If the source server is a managed Windows device (and not a SAN or Linux device, for example), the source representative can be on the source server.

To assign a source representative

1. Click Tools > Distribution > Content replication / Preferred servers.
2. In the Sources tree, right-click the source you want a representative for and click Properties.
3. On the Source representative page, select the device you want to be a source representative and click the Select button. To make sure you have the right device, you can verify the device attributes at the bottom of the page or click Inventory to see the device’s inventory.
4. Click Save.
Assign a replicator

A replicator is a managed Windows device that copies files from a source server to a preferred server. This replicator should have a significant amount of disk space so it can keep data from all distribution sources cached locally in the software distribution cache. If it doesn't have enough disk space, the replicator may have to download some files from the source each time it does a replication job. Each replicator can replicate multiple sources to multiple preferred servers.

To assign a replicator

1. Click **Tools > Distribution > Content replication / Preferred servers**.
2. Right-click the **Replicators** tree and click **Properties**.
3. On the **Identification** page, select the device you want to be a replicator and click the **Select** button. To make sure you have the right device, you can verify the device attributes at the bottom of the page or click **Inventory** to see the device's inventory.
4. Click **Save**.
5. In the **Replicators** tree, right-click the new replicator and click **Apply settings now**.

You can also quickly designate a replicator by dragging a device from the **Network view** tree onto the content replication window's **Replicators** tree.

NOTE: Make sure the share name on the source and preferred servers are the same. For example, if the share name on your source server is shareddata, the destination share name on the preferred server must be shareddata also. Replicators will create necessary folders after the share name, but a replicator can’t create the share.

The reason this is necessary is that when managed devices use a preferred server to download package files, only the server name in the full package path is substituted. The rest of the path, starting with the share name, remains exactly as in the original distribution package.

Schedule replications

Replication won’t happen until you schedule a replication task. Replication tasks are different than software distribution tasks. You can only schedule replication tasks from the **Content replication** pane.

You can either schedule an on-demand replication task or you can schedule a recurring replication task. One-time only replication tasks are good for testing replication and initially configuring servers for replication.

Once you have a working replication configuration, we recommend using recurring replication tasks configured from the preferred server properties or replicator properties to automate replication. You can then look at the **Content replication** pane’s task tree nodes to see replication schedules, progress, and status.
NOTE: You can schedule replication from either a preferred server or a replicator shortcut menu.

To start a content replication task immediately

1. Click **Tools > Distribution > Content replication / Preferred servers**.
2. Click the **Replicators** tree, right-click the replicator you want to schedule, and click **Start content replication now**.
3. Monitor the replication status in the status dialog box that appears.

To schedule a content replication task

1. Click **Tools > Distribution > Content replication / Preferred servers**.
2. Click the **Replicators** tree, right-click the replicator you want to schedule, and click **Schedule content replication**.
3. A new scheduled task appears in the **Scheduled tasks** pane.
4. Configure the new scheduled task by right-clicking it and clicking **Properties**.
5. The task will run at the configured time.

To schedule a recurring replication task

1. Click **Tools > Distribution > Content replication / Preferred servers**.
2. Click the **Replicators** tree, right-click the replicator you want to schedule, and click **Replicator properties**.
3. In the tree, click **Settings** and then click **Schedule**.
4. In the toolbar click **»**.
5. Configure the schedule you want. For more information, see "About the Selected replicator's Schedule page" (974).
6. Click **Save** to exit the dialog boxes.

To delete a recurring replication task

1. Click **Tools > Distribution > Content replication / Preferred servers**.
2. Click the **Replicators** tree, right-click the replicator you want to schedule, and click **Properties**.
3. In the tree, click **Settings** and then click **Schedule**.
4. Select the schedule you want to delete and in the toolbar click **»**.

**Update replication settings**

Replicators check for new settings each time they run. If you change settings on a replicator but keep the schedule the same, the replicator will get the updated settings automatically the next time it runs. However, if you change the replication schedule, the replicator won’t get the changes until its originally scheduled run time occurs.
For example, if a replicator was originally scheduled to run once a month and you later change the schedule to once a week, the schedule change to weekly might take an entire month to update.

When changing replication schedules, you should schedule a subsequent apply settings task to update the replicators with their new schedule and settings.

**To update replication settings immediately**

1. Click *Tools > Distribution > Content replication / Preferred servers*.
2. In the tree, right-click the preferred server, source, or replicator you want to update, and click *Apply settings now*.

**Monitoring replication progress**

You can monitor replication task progress, status, and history in the *Content replication* pane’s tree view. The tree view has the following nodes:

- **All tasks**: A summary of all running, pending, and not scheduled replication tasks.
  - **Running tasks**: Active replication tasks.
  - **Pending tasks**: Replication tasks that are scheduled to run.
  - **Not scheduled**: Replication tasks that aren’t scheduled to run in the future.
- **Task history**: Replication tasks that have run.

The task views only show the most recent task status. It won’t show a complete task history because in many environments, replication can happen frequently enough that a full log would become unmanageable.

**File replication help**

**About the Preferred server properties dialog box**

Use the Preferred server properties dialog box to configure your preferred servers. For more information, see "Preferred servers and content replication overview" (963).

**To open the Preferred server properties dialog box**

1. Click *Tools > Distribution > Content replication / Preferred servers*.
2. In the *Content replication* tree, right click *Preferred servers (Targets)* and click *New preferred server*. You can also right-click an existing preferred server and click *Properties*.

**About the Configuration page**

Use the *Configuration* page to specify the preferred server name and read-only credentials. Managed devices will use this information to connect to the preferred server.

- **Server name**: The preferred server’s resolvable computer name.
- **Description**: The server description. This appears in the *Replicators* tree’s *Details* column.
- **User name**: The read-only username to access the server.
- **Password**: The password for the user name you entered.
- **Confirm password**: Re-enter the password for the user name you entered.
- **Test credentials**: Tests the credentials to see if they are valid on the server.

**About the IP address ranges page**

Use the *IP address ranges* page to enter a starting and ending IP address range. Only devices within this range can attempt downloads from this server. You can enter multiple IP address ranges.

- **Starting IP address**: The range's starting IP address.
- **Ending IP address**: The range's ending IP address.
- **Add**: Adds the IP address range to the list.
- **Delete**: Deletes the selected IP address range.

**About the selected replicator page**

Use the selected replicator page to select the managed Windows device that you want to be the replicator. A replicator is responsible for copying data from the source server to the preferred server target.

- **Select**: Highlight the device you want to be a replicator and click **Select** to designate it as the replicator.
- **Inventory**: Once you selected the replicator, you can click this button to view the device inventory and verify that it’s the device you wanted.
- **Clear**: Deselects the device as a replicator.

**About the Write credentials page**

Use the *Write credentials* page to specify the preferred server’s write credentials. The replicator will use these credentials to connect to the preferred server so that a replicator can replicate new or changed files to a preferred server.

- **User name**: The username with write permissions to access the server.
- **Password**: The password for the user name you entered.
- **Confirm password**: Re-enter the password for the user name you entered.
- **Test credentials**: Tests the credentials to see if they are valid on the server.

**About the Sources page**

Use the *Sources* page to configure the source paths that you want copied to preferred servers.

- **Source paths list**: Shows sources that you’ve configured. Select a source from this list.
- **Include**: Adds the selected source to the *Included source paths* list. Once a source is in the the *Included source paths* list, its content will be replicated to the preferred server you’re configuring when the replication job runs.
- **New**: Opens a new source properties dialog box so you can configure a new source if the source you want hasn’t been configured yet.

- **Exclude**: Removes the selected source from the **Included source paths** list.

- **Included Source paths list**: Shows sources whose content will be replicated to the preferred server you’re configuring.

**About the Replicator properties dialog box**

Use the **Replicator properties** dialog box to configure a replicator.

**About the Identification page**

Use the identification page to select the managed Windows device that you want to be the replicator. A replicator is responsible for copying data from the source server to the preferred server target.

- **Select**: Highlight the device you want to be a replicator and click **Select** to designate it as the replicator.

- **Inventory**: Once you selected the replicator, you can click this button to view the device inventory and verify that it’s the device you wanted.

- **Clear**: Deselects the device as a replicator.

**About the Preferred servers (Targets) page**

- **Preferred server list**: Shows all preferred servers that you’ve configured. Move servers from this list to the **Included servers** list.

- **Include**: Moves the selected preferred server from the **Preferred server list** to the **Included servers** list.

- **Exclude**: Moves the selected preferred server from the **Included servers** list to the **Preferred server** list.

- **Included servers** list: Preferred servers in this list will be targets for the replicator you’re configuring.

**About the selected replicator Settings pages**

Use the selected replicator settings pages to configure the replicator's run options and schedule.

**About the Settings page**

Use the Settings page to see the replicator’s settings revision number and the actual revision number last reported by the replicator.

- **Current settings revision**: Shows the current revision number. Each time you change and then save the replicator settings, the **Current settings revision** increments by one.

- **Last revision applied by replicator**: Each time the replicator runs it checks for updated settings and then reports the settings revision number it used.

- **Last reported**: Shows the most recent date and time that the replicator ran.
About the Selected replicator’s Run options page

Use the Selected replicator’s Run options page to configure run options, such as bandwidth and user interface settings:

- **WAN bandwidth settings**: 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.

- **LAN bandwidth settings**: 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.

- **Show progress dialog**: Shows a progress dialog box on the replicator. When disabled, the job happens in the background with no notification or status indicators.

- **Allow peer download**: When checked, the replicator will first check local peers for source files that it is replicating. If the replicator can’t find the file on a peer, it will get the file from the source server. This option can reduce the traffic load on your source server.

- **Limit the number of days files are kept in cache**: Replicated files will stay in the local distribution cache on the replicator. By keeping files cached, the replicator doesn’t need to transfer files from the source server for every replication job. If for some reason you want to force the replicator to refresh cached files periodically, check this option and enter the number of days.

Generally, it’s safe to leave this option disabled, since any files that change on the source will automatically be updated in the local cache the next time the replication job runs.

- **WAN bandwidth settings**: Check this option if you want to use your WAN bandwidth settings when pushing files to targets.

- **LAN bandwidth settings**: Check this option if you want to use your LAN bandwidth settings when pushing files to targets.

About the Selected replicator’s Schedule page

Use the selected replicator’s Schedule page to schedule when a replicator runs. Clicking the add button displays the Schedule content replication dialog box. Schedules that you’ve configured appear in the schedule list box. You can edit or delete a schedule by selecting it and clicking the appropriate button.

About the Schedule content replication dialog box

- **Time**:
  - **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).

• **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.

- **Maximum duration**:
  - **Run until replication finishes**: When selected, the replication job runs until it finishes.
  - **End after**: When selected, the replication stops after the amount of time you specify. The job will resume where it left off at the next scheduled replication. This option can be helpful when you’re replicating across a slow link at night and you don’t want replication traffic interfering with daytime network traffic.

- **Select preferred servers to update**:
  - **Update all associated preferred servers**: The replication will happen for all preferred servers associated with this replicator.
  - **Update only the following preferred servers**: The replication will happen only for the preferred servers you select. Use this option if you want to schedule replication at different times for different preferred servers.

**About the Schedule content replication task dialog box**

Use the **Schedule content replication task** dialog box to schedule a run-once replication task. After creating a scheduled task with this dialog, you need to set a time for it to run in the **Scheduled tasks** tool.

- **Task name**: The name for this task that appears in the Scheduled tasks tool.
- **Create a scheduled task**: Creates a scheduled task.
- **Create a policy**: Creates a policy.
- **Add selected (or implied) replicators to target list**: If you’ve selected a replicator or a preferred server, this option will be available. This option will then add as task targets the selected replicator and any additional replicators referenced by the associated preferred server configurations.
- **Replicate only to selected preferred servers**: If you’ve selected a replicator, this option will be available. This option creates a task that only targets the replicators you selected.

**About the Schedule “apply settings” task**

Use the Schedule “apply settings” task to update a replicator with new settings. Access this dialog box from the **Content replication** pane’s toolbar. Replicators automatically check for updated settings before they run. An apply settings task is useful after you’ve assigned a computer to be a new replicator. Scheduling this task will install the replicator software on the computer.
- **Task name:** The name for this task that appears in the Scheduled tasks tool.
- **Create a scheduled task:** Creates a scheduled task.
- **Create a policy:** Creates a policy.
- **Don’t add any replicators to this task:** Leaves the target list blank so you can add your own replicator targets in the Scheduled tasks tool.
- **Add all out of date replicators:** Adds all replicators that report a settings version that doesn’t match the latest.
- **Add only replicators that have not reported (new replicators):** Adds newly designated replicators that have never reported or run. This configures new replicators with the latest settings.
Cloud Services Appliance

Configuring the Ivanti Cloud Services Appliance (Management Gateway)

The Ivanti Cloud Services Appliance (CSA), formerly known as the Management Gateway, is an Internet appliance that provides secure communication and functionality over the Internet. It acts as a meeting place where the 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:

- "Configuring the core server to use a Cloud Services Appliance" (977)
- "Managing client certificates" (978)
- "Creating an on-demand remote control agent package" (979)

Using multiple Cloud Services Appliances

You can install multiple CSAs. For example, you can do this to help balance CSA workloads. When you configure the core server to use multiple CSAs, managed devices can use any of the configured CSAs to connect to the core. The CSA a managed device uses depends on the CSA specified in that device's agent configuration. There is no automatic load balancing or failover. If you want to balance CSA loads, create a custom agent configuration for each CSA and selectively deploy those agent configurations.

Configuring the core server to use a Cloud Services Appliance

The Cloud Services Appliance (CSA) is available for purchase separately as a standalone device, as an installable ISO you can use with your own hardware, or as a VMWare virtual machine image. Once you install a CSA, you need to configure the core to use it.

The **Configure > Manage Cloud Services Appliances** option is only available from the core server's management console. Additional consoles don't have this option. Only users with the Ivanti Administrator right can modify a CSA configuration.

**To connect a Cloud Service Appliance to the core server**

1. In the core server's management console, click **Configure > Manage Cloud Services Appliances**.
2. On the **Cloud Services Appliances** tab, specify the CSA information.
3. If the CSA uses an internal address that is different from its public address (for example, if it's located in a DMZ-type environment), specify the **CSA internal name** and **CSA internal IP address**.
4. If the core will connect to the CSA through a proxy, select **Use proxy** and specify the proxy settings.

5. Click **Apply**. If the CSA settings are correct, the new CSA appears in the list.

You can also select any CSA in the list and change its settings on the right side. Click **Apply** when you’re done making changes. The core server then connects to the CSA and registers with it by installing the core’s security certificate on the CSA.

**Managing client certificates**

Each managed device is required to have a valid digital certificate in order to connect through the CSA. If your core has client certificate-based security enabled, Ivanti agents on managed devices also need a valid certificate to decrypt secure core data. These certificates are generated automatically during agent installation, but they default to an unapproved state that prevents communication through the CSA and secure core data decryption.

You can manage the list of devices that have been granted certificates by blocking or deleting the those device certificates. Use the search box to easily filter the list.

Approve device certificates to allow CSA access and secure core data decryption. The core server defaults to notifying you when the number of unapproved certificates is 10 or more. You can customize or disable this notification at the bottom of the dialog box.

Block a device certificate to temporarily stop it from using the CSA to communicate with the core server or decrypt secure core data. You can unblock it later if you want to restore access.

If you delete a device certificate, it will be removed from the list. The certificate remains on the device. If that device attempts to reconnect later or when it runs a security scan (which triggers a reconnection attempt), it will reappear in the list.

Blocked or deleted devices can still communicate with the core server if they are on the same network as the core server and if the setting for **Dynamically determine connection route** option is selected in the Agent settings tool under **Client connectivity settings**.

There is also an option to **Automatically approve new certificates**. This option isn’t recommended because it gives all new devices access to the core. However, in some instances administrators may want to enable this for a short time, such as when enrolling a lot of devices.

**To approve, block, or delete device certificates**

1. In the core server’s management console, click **Configure > Manage Cloud Services Appliances**.

2. On the **Manage client certificates** tab, select the devices you want to approve, block, or delete. You can use **Shift+click** or **Ctrl+click** to select multiple devices.

3. Click **Approve selected** to approve selected device certificates.

4. Click **Block selected** to block selected device certificates.
5. Click **Delete selected** to delete the selected device certificates from the core server.
6. When finished, click **Apply**.

**Creating an on-demand remote control agent package**

You can create an on-demand remote control agent executable package that can be downloaded by devices that have not been configured to connect through the CSA. This allows them to be remote controlled through the CSA.

There are two parts to the remote control downloadable agent:

- The CSA you want to use.
- The remote control settings file specifying the remote control features to allow.

When creating a remote control package, make sure in **Security settings** that you select either **Local template** or **Windows NT security**. The CSA doesn’t support **Integrated security**.

**To create an on-demand remote control agent**

1. Click **Configure > Manage Cloud Services Appliances**.
2. On the **Remote control agent** tab, select the CSA and remote control settings profile you want to use.
3. Click **Create**.
4. Specify the location to which you want the remote control agent to be saved.
5. Click **Save**.

After creating the remote control agent, you can distribute it on a USB drive or post it to an accessible location for download by managed devices. You can also host the standalone remote control agent executable on the CSA.

**To host a standalone remote control agent executable on the CSA**

1. In a web browser, open the CSA home page (http://<CSA name or IP address>).
2. Click **Software package upload**.
3. On the upload page, browse for the standalone remote control executable package you created earlier.
4. Enter a **Description** for the executable. This appears on the download page.
5. Click **Upload**.

Users can access packages you’ve uploaded from the CSA home page by navigating to the CSA home page (http://<CSA name or IP address>) and clicking **Management Gateway Utilities > Support tools**. Uploaded packages are in the **Available packages** list. Users must have a CSA client certificate to access this page.
**Using the Cloud Services Appliance activity recorder**

You can use the Cloud Services Appliance (CSA) activity recorder log to understand what your CSAs are doing and their relative workloads.

Core servers use a service (BrokerService.exe) to communicate with Cloud Services Appliances. On the core server, each CSA that the core server is configured to use has its own BrokerService.exe process. The service writes CSA activity to a .csv format log file. You can use an application like Microsoft Excel to chart and understand log data.

The Activity Recorder is controlled by an XML file on the core server:

- C:\Program Files\LANDesk\ManagementSuite\BrokerServiceConfig.xml

Comments in this file include directions on how to use it. The main options you may want to change are these:

- `<Enabled>`: True turns on the activity logger, false turns it off. True is the default.
- `<Logging>`: True turns on some extra logging in the activity logger. False is the default.
- `<ActivityLogMaxSize>`: Maximum size in bytes of the debug log before it is rolled over. The default is 10 megabytes (10000000).

Here is a sample log entry:

```
10 Apr 2013 14:55:54, 3440, 6616, ldcsa.mycompany.com, {D226EC08-A522-6C4B-8AC3-29C0EA7061DA}, LMCORE95B:5007, Inventory
```

Each log entry contains the following items (the parentheses contain that item from the example above):

- Date/time (10 Apr 2013 14:55:54)
- Broker service process ID (3440)
- Broker service thread ID (6616)
- Gateway name (ldcsa.mycompany.com)
- Client device unique ID (D226EC08-A522-6C4B-8AC3-29C0EA7061DA)
- Service URL accessed (LMCORE95B:5007)
- Feature, as provided by the feature map (Inventory)

**Customizing activity recorder feature mapping**

CSA requests from clients are in a URL format. The BrokerServiceConfig.xml XML configuration file specifies case-sensitive substrings in the URL and maps occurrences of those substrings to a feature. The substring matching algorithm is plain text and it doesn’t support wildcards or regular expressions. The configuration file includes defaults for the main features, but you can customize the strings if you want.
For example, this XML entry detects "vulscanresults" in the URL and when that occurs, it creates a log entry for "Patch".

```
<Url><PathSubString>vulscanresults</PathSubString><Feature>Patch</Feature></Url>
```

In the XML file, the following attributes control feature mapping:

- **<DefaultFeature>:** If a configured substring can't be found in the URL, it will be categorized by the name given here. **<OutputDefaultFeature>** must be set to True for **<DefaultFeature>** entries to appear in the log.

- **<OutputDefaultFeature>:** If a configured substring can't be found in the URL and this is false, it isn't written to the activity log. If true, it is.

- **<FeatureMapping>:** This is a list of substrings that the activity recorder looks for when watching URL traffic. As soon as it finds one by searching from top to bottom, it logs the entry in the log file and the feature name provided is used in the last column of the log.
Tenant management

Tenant management overview

Tenant management is an add-on to Ivanti® Endpoint Manager powered by Landesk that is available for purchase separately. Tenant management allows you to compartmentalize managed devices and configurations by company. If you’re responsible for managing multiple companies or distinct organizations within your own company, in the past you may have deployed separate Endpoint Manager core servers for each location. You would then have to log in to each core to manage each company or organization.

Using tenant management alongside a Ivanti Cloud Services Appliance greatly reduces the need for multiple core servers. Once you configure tenant management, devices configured for tenants show up in separate scopes within the console. You can then be sure which tenant’s assets you’re managing as you use the console.

Each tenant you create gets its own user management team and scope. You can assign console users to the specific tenant teams and scopes that they need to manage.

Each tenant can also have associated contact information, contract terms, and Ivanti license usage tracking.

These are the main tenant management configuration steps:

1. In the Tenant management tool, create a tenant.
2. In the User management tool, add console users to a team or scope that can see the tenant.
3. In the Agent configuration tool, create an agent configuration, select the proper tenant on the tenant panel, and then deploy it.
4. Use the tenant groups in the console to manage tenants.

Creating a tenant

Use the Tenant management tool (Tools > Administration > Tenant management > New tenant definition button) to create a tenant. You must give each tenant a unique tenant name and ID. The tenant name must be different than any existing RBA scope and team names. The tenant ID is only editable when you first create the tenant.

By default the tenant ID is a GUID, but you can change it to any combination of letters (A-Z, a-z), numbers, and dashes. GUIDs can be hard to remember, so you may consider using something like the customer number.

The remaining information in the Tenant configuration dialog box is optional. If you do add contact information, contract terms, or licensing information, you can see much of that information in columns inside the Tenant management tool.
The licensing information is informational only. Tenant management doesn't limit the number of tenants to the number of Assigned Ivanti licenses you enter. Tracking assigned licenses can be useful for billing or other purposes.

Use the Notes tab to add any additional information that you want.

Creating a tenant automatically creates a corresponding user management team and scope with the same name for that tenant. You'll need to add console users who will be managing that tenant to that tenant's user management team and scope. Only console users who are members of the tenant's user management team will be able to see the tenant’s groups in various parts of the console.

If you rename a tenant, the console will automatically rename the associated user management team and scope to match and it will also rename any other places in the console where the tenant's name appears.

**Create a tenant**

Create a tenant if you want to compartmentalize managed devices by organization or company.

**To create a tenant**

1. Click **Tools > Administration > Tenant management**.
2. Enter a unique **Tenant name**.
3. Change the Unique ID if you don’t want to use the random GUID. Valid characters are A-Z, a-z, 0-9, and hyphens.
4. If you want, enter additional data relevant to the tenant.
5. Click **Save**.

**To add console users who will manage the tenant**

1. Click **Tools > Administration > User management > Teams**.
2. Double-click the new team named after your tenant name.
3. Select the console users who will be managing devices in this tenant.
4. Click **OK**.

**To add console users to the tenant’s scope**

1. Click **Tools > Administration > User management > Scopes**.
2. Right-click the new scope named after your tenant name and click **Properties**.
3. In the **Scope properties** dialog box, select the console users who will be managing devices in this tenant.
4. Click **OK**.
Adding tenant devices

After you’ve created a tenant, you can add devices to the tenant by deploying an updated agent configuration that assigns the tenant to that tenant’s managed devices.

Each tenant you create has its own team group in the agent configuration dialog box. Use this team group to organize agent configurations unique to each tenant.

The Agent configuration dialog box includes a **Tenant** page where you can select the tenant associated with an agent configuration.

If you assign a tenant to an agent configuration that’s not in the tenant’s team group, that configuration won’t be automatically moved to the tenant’s team group. If you want it there, move or copy it manually.

If you’ve already deployed an agent configuration to tenant devices, you don’t have to redploy a full agent configuration to update the tenant setting on a device. Instead, after assigning a tenant in the agent configuration you want, use the **Schedule update to agent settings** toolbar button in the Agent configuration tool to update the settings on targeted devices.

The inventory scanner includes the tenant ID it finds in inventory scans. You can see the tenant name and unique ID in a device’s inventory tree under the **Tenant** node.

Add tenant devices

Add devices to a tenant by assigning a tenant to an agent configuration and then deploying that agent configuration to devices belonging to the tenant.

**To add tenant devices**

1. Click **Tools** > **Configuration** > **Agent configuration**.
2. In the **Agent configuration** tree, click the agent configuration group that matches your tenant name. If you want to use an existing agent configuration, copy and paste it into the tenant’s group.
3. In the **Agent configuration** dialog box, make sure **Assign a tenant to this configuration** is selected and make sure you’ve selected the tenant that you want set for this agent configuration.
4. Click Save.
5. If you’re updating an existing agent configuration on tenant devices, click the Schedule update to agent settings toolbar button. Otherwise, deploy the full agent configuration.
6. Add devices belonging to the tenant to the scheduled task and schedule it to run.

Deleting tenants and tenant devices

Deleting a tenant removes the tenant's group from the console tools that reference it. When you delete a tenant you will be asked if you want to reassign object ownerships associated with it, such as agent configurations, to another console user. If you don't do this, orphaned object ownership will revert back to the root console administrator.

The tenant unique ID remains on tenant devices and won’t be removed when you remove the tenant. If you want, you can remove the unique ID from tenant devices by redeploying agent configuration settings that don’t include a tenant. Leaving the unique ID on tenants causes the inventory scanner to populate the unique ID inventory data, but since the device will no longer have a tenant name associated with it, the device won’t be part of the tenant’s team group.

Delete a tenant or tenant device

To delete a tenant

1. Click Tools > Administration > Tenant management.
2. Select the tenant you want to delete and press the Delete key on your keyboard.
3. If you want to reassign tenant objects to a console user or team other than the root administrator, select the user or team you want.
4. Click OK.

To remove a device from a tenant

1. In the Agent configuration tool, select an agent configuration that has no tenant selected.
2. Click the Schedule update to agent settings toolbar button.
3. Add devices that you want removed from the tenant to the scheduled task and schedule it to run.

Managing devices in a tenant

Once you’ve done the following, you’ll see the tenant as an item throughout many parts of the console:

1. Created a tenant
2. Assigned console rights to manage that tenant
3. Added devices to the tenant
You’ll see the tenant in such areas as:

- Network view, under **Devices**, **Virtual OS hosts**, **Queries**, and **Scopes**.
- Administration toolbox, under **Column set configuration** and **User management**.
- Distribution toolbox, under **Delivery methods**, **Distribution packages**, and **Manage scripts**.
- Power management tool.
- Security and Compliance toolbox, under **Patch and compliance** and **Security configurations**.

You can then use the tenant’s team group in these tools to view and manage devices belonging to a tenant. Only console users with rights to manage a tenant will see that tenant in the console.

An easy way to target tenant devices in a scheduled task is to use the mouse to drag the tenant’s scope from the **Network view** and drop it on the task you want.

**NOTE:** For Windows devices the tenant’s unique ID gets added to the registry:

```
HKLM\SOFTWARE\LANDesk\ManagementSuite\WincClient\Tenant\TenantUID
```

For Macintosh devices the tenant’s unique ID gets added to a plist:

```
/Library/Preferences/com.landesk.ldms.plist
```
Web console

About the Web console

The Ivanti® Endpoint Manager powered by Landesk Web console lets you automate systems management tasks and control desktops, servers and mobile devices. It differs from the Ivanti Management Console in that it is accessed from a browser, not run as a Windows executable.

The Web console uses the infrastructure of your existing network to establish connections with the devices it manages. This greatly simplifies the job of managing your existing network, whether you manage a small network or a large enterprise environment, even when you aren't at your desk.

Starting the Web console

To start the Web console

1. From a networked computer, open a Web browser.
2. In the Address field at the top of the browser, enter a URL that points to the core server, followed by /remote (in the format http://<webservername>/remote).
3. If a login dialog appears, enter your Windows username and password for the core you’re connecting to and click OK.
4. Once you authenticate, links in the left navigation pane appear for the tasks you have rights to perform, such as creating queries, remote controlling clients, deploying software, and viewing reports.

Click here for a description of the Login dialog box

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

- **Username:** Identifies a user. This might be an administrator user or some other type of product user with restricted access. The user must be a member of the LANDESK Management Suite group on the core server. If you’re connecting to a remote core server, enter the domain name and user name.
- **Password:** The user's password.

Troubleshooting

- If the device list and buttons do not appear when you start the console, you may need to activate the core server.
- If you don’t know the URL to the Web console pages, contact the person who installed the Web console, most likely the network administrator for your site.
- If you can’t see some of the left navigation pane links, your network administrator is most likely using Ivanti® Endpoint Manager powered by Landesk role-based administration or feature-level security option that limits you to performing certain tasks that you have the rights to do.
Using the Web console

This topic describes the Endpoint Manager Web console and how to use it.

Remember that if you don’t see a tool, you probably don’t have rights to view it. These rights are determined by the access rights and device scope assigned to you by the Endpoint Manager administrator.

Web console layout

The Web console has four main areas that you interact with:

- The title bar
- The toolbox
- The tool pane
- The action pane

The title bar displays the device you are logged in to and the user you are logged in as. It includes a help link that opens help topics for the Web console.

The toolbox shows available tools, grouped under headings. Click the chevrons next to a heading to expand or close the group.
The right side of the console has variable contents depending on which tool is in use. If this area is divided, the top part is referred to as the tool pane and the lower part as the action pane. The tool pane shows the basic elements of the tool you’ve selected, and typically in the action pane you will either select actions or view the results of the task you are doing.

You can resize the panes and columns of the Web console. You can also expand or reduce the size of toolbar elements so you can view them better.

NOTE: For dialogs and windows to display properly, the Endpoint Manager Web site must be added to the allowed list of the browser’s popup blocker.

Continue reading this topic for information about:

- My devices list
- Device icons
- Using shortcut menus
- Using tools
- Viewing device properties

My devices list

The My devices list is the main window that is displayed when you start the Web console and is the starting point for most tools. It contains the following groups and sub-groups. In addition, depending on your access rights and device scope, you can create your own groups for easier management of devices.

A few commonly used actions in this list include the following:

- Right-click a device in the Devices list to view available options for that device, such as Ping, Remote control, and Target.
- To select multiple consecutive entries in a list, click the first item, press and hold down the Shift key, and then click the last item.
- To select multiple nonconsecutive entries in a list, press and hold down the Ctrl key, and then click each item.
- Double-clicking a device in the All devices list opens a full device inventory window that displays all inventory information for the device.

NOTE: The My devices list also includes Virtual Hosts OS groups.
All devices

The All devices list shows the devices for the currently logged-in user, based on the user’s scope, in a flat list (no sub-groups). When connected to a particular core server, the administrator can see every device managed by that core server. Product 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).

Devices running product agents (Standard management agent and Inventory) automatically appear in the All devices list after they have been scanned into the core database by the inventory scanner. Typically, this scan takes place for the first time during initial device configuration. Once a device is scanned into the core database it is considered to be a managed device—it can now be managed by that core server.

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 (or to move unmanaged devices to a managed devices group), you can use the device discovery tool to scan the network for devices.

The All devices group provides the following information for each device. To sort a column, click on its header; click the header again to reverse the sort. Double-click All devices to open the list.

- **Name**: The device host name, such as the Windows computer name.
- **IP address**: The IP address of the device.
- **Health**: The health and availability status of the device. This can be Normal, Warning, or Critical.
- **Agent**: The current agent running on the device.
- **Device type**: Displays the kind of hardware on the machine (Intel AMT, IPMI, ASIC, or IPMI Advanced).
- **Operating system**: The type of operating system the device is running.
- **Up since**: The date and time the device has been operating without interruption (in the time zone of the database).

When no agents are installed on a device, the name and IP address are the only columns that contain information. In some instances, the operating system will also display.

When you select a device, the device's properties are displayed in the Properties pane below the device list. The Properties pane shows basic device attributes:

- **ID**: The identification number of the device. This number is determined by the sequence in which the device was added to the All devices list.
- **IP address**: The IP address of the device.
- **Manufacturer**: The device’s manufacturer.
- **Model**: The model of the device.
- **Processor speed**: The speed of the device’s CPU.
- **Processor type**: The type of the device’s CPU.
For more actions available in the Properties pane, see "About the Properties tab" (993).

**My devices**

The *My devices* list shows groups of devices created by the currently logged-in user. My devices groups are not visible to, and can't be used by, other users.

**Public devices**

The *Public devices* list shows groups of devices that have been created by a user with Administrator rights. They are visible to other users.

**Virtual hosts OS**

The *Virtual hosts OS* list shows VMware ESX servers that are configured as virtual hosts, that have been discovered by selecting the Virtual hosts option in a device discovery configuration. When you click *Virtual hosts OS* or any sub-groups in the tree view, the hosts are shown as end nodes in the device window. When you click a host name in the tree view, the host is a container and the virtual machines running on it are displayed in the device list.

**Device icons**

Device icons in the *All devices* list show the current health status of each device, if the device includes an agent with the *Real-time inventory and monitoring* option selected. You can update the health status for devices one at a time as you select them in the *My devices* list by clicking the *Refresh* toolbar button.

There are four status icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon-normal.png" alt="normal" /></td>
<td>Device with Normal status</td>
</tr>
<tr>
<td><img src="icon-warning.png" alt="warning" /></td>
<td>Device with Warning status</td>
</tr>
<tr>
<td><img src="icon-critical.png" alt="critical" /></td>
<td>Device with Critical status</td>
</tr>
<tr>
<td><img src="icon-unknown.png" alt="unknown" /></td>
<td>Device with Unknown status</td>
</tr>
</tbody>
</table>

**NOTE:** These icons require at least a 16-bit color-depth setting to display correctly. If the icons in your console appear out of focus, change your color settings in the Windows Display Properties.
Using shortcut menus

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

To view an item's shortcut menu, right-click the item. For example, when you right-click a managed device in the My devices list, its shortcut menu will typically display the following options:

- **Remove from group**: Removes the item from a user-defined group.
- **Target**: Moves the selected device to the Targeted devices list. (If targeted devices don't appear in the Target list, click Refresh on the Targeted devices tab.)
- **Ping device**: Verifies the device is responding.
- **Tracert device**: Sends a trace route command to view a network packet being sent and received and the number of hops required for the packet to reach its destination.
- **Scan device**: Scans the device for vulnerabilities. Click Start scan.
- **Remote control**: Launches the remote control window, allowing direct access to the selected device from the console.

The help does not cover every console item's shortcut menu, but we recommend that you right-click any item to see the options that are available.

Using tools

Tools are grouped in the toolbox into sections, with headings such as **Device view** and **Remote access**. Click the chevrons next to a heading to expand or close the group.

An administrator sees all of the tools in the toolbox. Other users will see only the tools (features) that are allowed by their assigned rights. For example, if a user doesn't have the Reports right, the **Reports** tool doesn't appear in the toolbox.

Here is a complete list of tools:

- **My devices**: View device properties, run scans, and target devices.
- **Remote control**: Remotely control devices and exchange files with them.
- **Distribution**: Distribute software packages, use custom scripts, schedule distributions, and create software distribution tasks.
- **Scripts**: Create and manage scripts.
- **Directory manager**: Locate, access, and manage devices in other directories via LDAP (the Lightweight Directory Access Protocol).
- **Scheduled tasks**: View all tasks that are currently in the scheduled or completed.
- **Alerting**: Configure and schedule alert rulesets to notify you with device monitoring data. For more information on alert rulesets, see Alerts and monitoring overview.
• **Alert log:** View alerts sent to the server. The log is sorted by time with the most recent alert at the top. For more information on logs, see Alert logs.

• **Reports:** Manage predefined service reports.

• **Queries:** Create and modify queries to the database to isolate specific devices that meet your criteria.

• **Preferences:** Create custom inventory attributes and view licensing information.

**Viewing device properties and inventory**

In the **My devices** view, you can quickly view information about a device by clicking the device in the list and selecting **Properties** in the action pane.

More detailed information about the device is available in its inventory data. View inventory data in the **All devices** view by double-clicking the device, or by selecting the **View inventory** tab in the **Properties** pane to open the full **Inventory** window.

**About the Properties tab**

Use the Properties tab to view useful information about the selected device. The screen includes a brief summary of properties and the following buttons:

• **View inventory:** Click this button to display the full inventory of the selected device in a tree view. This data is gathered by the inventory scanner, which stores it in the database. The details view displays all of the possible inventory items available for a device, so some items (which are not enabled on the device you’ve selected) will have no data. Click an item in the view to display details about it for this particular device. To go back to the default view, click the device name at the root of the view.

• **Remote control:** Launches the remote control window, allowing direct access to the selected device from the console.

**Targeting devices [Web console]**

The **Targeted devices** list helps you complete tasks on selected devices, such as deploying agents or scanning for software updates to a select group of devices.

The recommended number of devices that you should add to the list is 250 or fewer. The devices will stay in the list until your console session ends or times out (after 20 minutes of inactivity).

You can target devices by selecting them from any list of devices. If you don’t see the devices you want, use the **Find** button on the toolbar. Search for one particular device, or search for several using the wildcard characters % or *.

With one or more devices in the **Targeted devices** list, you can complete a task such as deploying an agent configuration to each of the targeted devices.
To target devices using the Web console

1. In the My devices or All devices list, click the device you want to target for an action. Select multiple devices by using Shift+click or Ctrl+click.

2. Click the Target button. If it isn’t visible, click the Filter button on the toolbar to hide the Filter options (the Target button is on the far right).

In the action pane the selected devices are listed under the Targeted devices tab. Once they are listed under this tab, you can open a tool (such as Distribution) and schedule a task that can be applied to the targeted devices.

NOTE: Device lists can span multiple pages, and as you select devices you need to click the Target button for each page. You can’t select devices on multiple pages and click the buttons just once for all of the pages.

NOTE: You can click the down arrow below the toolbar on the far right to set how many devices you want to display per page. You can display up to 500 devices per page. To permanently change the number of devices displayed in device lists, click Administration > Preferences > Page settings.

Filtering the display list [Web console]

The Devices lists have a filter option you can use to determine which devices appear in the list. You can filter by one of four types of criteria (device name, IP address, operating system, or login name). Use a wildcard character (% or *) to select a range of items with a similar identifier.

To filter the display list

1. Click My devices and navigate to a group under Devices.

2. If the Filter options are not visible, click the Filter button on the toolbar.

3. In the Filter list, select Device name, IP address, Operating system, or Login name.

4. Set the parameters of the filter by typing in the text box.

   In this box, the following extended characters are not supported: <, >, , , , , .

   For example, if you filter by device name, type the host name or range of computer names. You can enter wildcard characters to find certain computer names (such as *srv).

5. Click Find.
Using groups [Web console]

You can organize devices in groups for easier management. You can create groups to organize devices based on function, geographic location, department, device attribute or any other category that meets your needs. For example, you could create a Web server group for all servers configured as Web servers, or create a group that includes all devices running a specific OS.

The main Devices view contains three groups. Right-click a group to open it, delete it, or target all of the devices it contains for actions such as software distribution or agent deployment.

- **My devices**: Lists groups/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 moving or copying them from the Public devices and All devices groups. All users can create groups under My devices in the Windows console.

- **Public devices**: Lists groups/devices an administrator has added from the All devices group. An administrator (a user with the Administrator right) sees all of the devices in this group, while other users see only the devices allowed by their scope. Only administrators can create groups 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 devices that have been scanned or moved into the core database. Devices configured with the standard management agent automatically appear in the All devices group/folder when they are scanned into the core database by the inventory scanner. Users, including administrators, can't create groups under All devices.

Creating a group of devices [Web console]

Groups help you organize devices in the console's Devices list. You can create groups to organize devices based on function, geographic location, department, attributes 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. You can place groups within groups, such as all devices running a specific OS at a certain location.

Groups are organized as follows:

- **Devices**: To create groups under Devices, you must select My devices or Public devices first.

- **My devices**: My devices can only be seen by the user who created them.

- **Public devices**: Only administrators can create or modify groups under Public devices, but anyone can view the groups.

- **All devices**: There are no subgroups in All devices.
To create a group

1. In the Devices list, click My devices or Public devices.
2. Click the Add group button on the toolbar.
3. Type a name for the new group and click OK.

To delete a group

1. In the console's device view, click the parent of the group you want to delete.
2. In the tool pane, right-click the group you want to delete and click Delete group.

Using the Actions tab [Web console]

Use the Actions tab to execute the following operations on selected and targeted devices:

- Delete devices from the database
- Run inventory scans on selected devices
- Run patch and compliance scans on selected devices

To delete devices from the database

You can either select devices from the current device list, or target a list of devices (which is useful when there are several pages in the device list).

1. In the Web console, click My devices and select or target the devices to delete.
2. Click the Actions tab > Delete devices. Select Delete targeted devices or Delete selected devices as appropriate.
3. Click Delete and confirm that you want to delete the devices.

The delete function can delete single or multiple devices from any default group or user-created group. Once a device has been deleted from a group, it is completely removed from all lists of managed/inventoried devices, including the default All devices group.

To run an inventory scan on selected devices

You can either select devices from the current device list, or target a list of devices (which is useful when there are several pages in the device list).

1. In the Web console, click My devices and select or target the devices to delete.
2. Click the Actions tab > Run inventory scan. Select Scan targeted devices or Scan selected devices as appropriate.
3. Select the type of scan (Hardware only, Hardware and software, or Full sync).
4. Click Scan.

Status notes on the progress of the scan are displayed in the action pane.
To run a patch and compliance scan on selected devices

You can either select devices from the current device list, or target a list of devices (which is useful when there are several pages in the device list).

1. In the Web console, click My devices and select or target the devices to delete.
2. Click the Actions tab > Run patch and compliance scan. Select Scan targeted devices or Scan selected devices as appropriate.
3. Select the type of scan (Security and patch scan, Compliance scan).
4. Click Scan.

Changing page settings [Web console]

Use Page settings to set display preferences for pages listing devices or displaying graphics. This does not include the health dashboard, which contains separate dialog boxes for setting display preferences.

To change Web console page settings

1. In the Web console toolbox, click Administration > Preferences.
2. Click the Page settings tab.
3. In the Graph type list, select the type of graph you want to display in Reports.
4. In the Items/page box, type the maximum number of items you want to display in each page that uses pagination (the maximum allowed value is 500).
5. To show text alongside the buttons on toolbars, select the Show text on toolbars check box.
6. To ensure that the Web session you are running to view the Web console does not time out, select Always keep Web session alive.
7. Click Update.

NOTE: You can show text alongside the buttons on toolbars, thus helping new users with feature identification. If this option is not selected, only icons appear on the toolbars. However, the icons display text when the mouse pointer hovers on them.

To display more devices while viewing a list

1. While viewing any list of devices, click the down arrow at the far right (under the toolbar) to open the Page Settings box.
2. Type a number in the **Items/page** box (maximum 500).

3. To begin the list later than the first record, change the number in the **Start** box.

4. Click **Set**.

Your changes are valid only while you work in the current list. If you change to another device list, the number of devices displayed reverts to the setting in effect on the **Page settings** tab.

**Configuring custom columns [Web console]**

Use **Custom columns** to modify column names and fields. Any column changes you make will not be seen by other users. Custom column changes appear in the **My devices** view.

The Web console includes a default column set with eight columns. You can’t edit the default set, but you can define a custom column set to use as your default.

![Web console interface for configuring custom columns](image)

**NOTE:** It is not advisable to create custom columns in which there can be multiple field names. For example, if you were to create a **Computer.Software.Package.Name** field and a device had multiple packages installed, Endpoint Manager will list only one package name per line, even if the different package names are on the same device. In this situation the **All devices** list will show multiple entries for the same device.

**To create a custom column set**

1. In the Web console toolbox, click **Administration > Preferences**.
2. Click the **Custom columns** tab > **New**.
3. Type a name for the column set.
4. In the top box, navigate through the folders to find the attribute you want for each column heading. Select an attribute and click **Add**.

The box contains a folder structure, starting with **Computer**, that represents all of the inventory data currently in the database. Individual attributes have an attribute icon.

**NOTE:** If you select an attribute in the database that has a 1:* relationship, you will get duplicate entries for the device. When you select attributes with a 1:1 relationship (only one possible attribute, like Computer.System.Asset Tag), you will not receive duplicate entries.

5. To change the order of the columns, select a column heading and click **Move up** or **Move down**.

6. To remove a column, select it and click **Remove**.

7. To change the heading displayed for a column, select the heading, click **Edit**, make your modifications, and press **Enter**. The following extended characters are not supported: <, >, ', " , !.

8. Click **OK** to save the column set.

9. To use the custom column set when you view any device list, select it and click **Set as current column set** on the toolbar.

**NOTE:** If you’re using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, and so on).

**To edit a custom column set**

1. In the Web console toolbox, click **Administration > Preferences**.
2. Click the **Custom columns** tab.
3. Select the custom column set and click **Edit**.
4. Follow the instructions in steps 4-8 above to make changes.
5. Click **OK** to save your changes.

**Troubleshooting tips [Web console]**

The following troubleshooting tips are for issues that most frequently occur with the Web console.

**I don’t know the URL to the Web console.**
Contact the person who installed the core server, most likely the network administrator for your site. However, typically the URL is http://core server machine name/remote.

**Who am I logged in as?**
Look at the title bar; the user who is logged in is listed next to **Connected as**.
What machine am I logged in to?
Look at the title bar; the name of the core server is listed next to Connected to.

I don't see some of the toolbar links.
This occurs because your network administrator is using the role-based administration or feature-level security option that limits you to performing certain tasks that you have the rights to do.

I get an invalid session when viewing the console.
It's possible the browser session has timed out. Use your browser's Refresh button to start a new session.

An ASP.NET error appears when I try to start the Web console.
If you see an ASP.NET error message when attempting to log in to the Web console, ASP and the ASP directory permissions may not be configured correctly. Reset the ASP.NET configuration by running the following command:

```
ASPNET_REGIIS.EXE -i
```

The number of items per page is different from the number I specified.
When you specify how many items to display per page, that setting is stored in the Web browser's cookies directory and expires when the console session times out.

The console times out too frequently.
You can change the default session timeout for the console's Web pages. The IIS default is 20 minutes of inactivity before a login expires. To change the IIS session timeout:

1. On the Web server, click Start > Administrative Tools > Internet Information Services (IIS Manager.)
2. Expand Default Web Site.
3. Right-click the LDMS folder, then click Properties.
4. Under the Virtual Directory tab, click Configuration.
5. Click the Application Options tab, then change the session timeout to the value you want.

**NOTE:** Endpoint Manager is a session-based product. Do not disable the session state.

I can’t view the Remote control page in the Web console.
In order to view the Remote control page, you must enable ActiveX controls. Some browsers have ActiveX controls disabled by default. If the Remote control page does not load correctly, enable ActiveX controls on your browser by changing the security settings.
I completed the new distribution package wizard, but the console did not create a package.
The console uses the IUSR and IWAM accounts on the console server. These accounts are originally created based on the computer name. If you have ever changed the computer name, you must follow the steps below in order to successfully create software distribution packages.

1. If you have .Net Framework installed, uninstall it.
2. Uninstall IIS.
3. Reinstall IIS.
4. Reinstall the .Net Framework if you uninstalled it.

A scheduled software distribution job did not run.
If you schedule a software distribution job and it does not start, verify that the Intel Local Scheduler Service is running on the device.

Also, take into consideration that the scheduling of the job is based on the core server's time. If the job was scheduled on a console that resides in another time zone, the job will start based on the core server's time, which may be different than expected.

Report charts don't display properly.
In order to view the interactive bar and pie charts displayed in many reports, you must have the Adobe Flash Player installed. Verify that Flash is installed, then run the report again.

Why am I seeing two instances of the same device in my database?
Have you deleted a device from the core database and reinstalled it using UninstallWinClient.exe?

UninstallWinClient.exe is in the LDMain share, which is the main ManagementSuite program folder. Only administrators have access to this share. This program uninstalls Ivanti 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. You may see two instances of the device in the database you just deleted. One of these instances would contain historical data only, while the other would contain data going forward.

I added a S.M.A.R.T. drive on a device, but I don't see S.M.A.R.T. drive monitoring in the inventory list for that device.
Hardware monitoring is dependent on the capabilities of the hardware installed on a device, as well as on the correct configuration of the hardware. 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, monitoring data will not be available, and resulting alerts will not be generated.
In PXE-based OS provisioning DOS scripts, some parts after a comma are truncated.
In any line of a script, all characters after a comma are truncated; therefore, any commands after the comma are not executed. To avoid this, use double quotes around the whole command, like this:

\[
\text{REMEXEC1}=%\texttt{QUOTE}\texttt{echo }\texttt{"hi, good morning"}\texttt{QUOTE}\]

Single quotes will not work, as they are stripped out in the .INI file reading.

When attempting to install Remote Control from the web console in a different subnet, the RC viewer cannot be installed.
If you connect to a web console that’s being hosted by a core in a different domain, and right-click a computer in the My Devices list and select Remote Control, you will get an error saying that the RC viewer hasn’t been installed properly.

To solve, the URL for the CAB is obtained by reading the tag named "CabUrl" from web.config. The tag CabUrl must contain the core’s fully-qualified domain name instead of just the machine name. You need to open web.config and put the fully-qualified domain name in the CabUrl tag.

A USB disk device is not listed in the Inventory list until an inventory scan has been run.
When a disk device is connected with a USB cable to a managed device, it is not immediately listed under Hard drives in the device’s inventory. It is listed under Logical drives after being connected to the device. However, it will not appear under Hard drives until an inventory scan has been run on the device.

On managed Linux devices, a USB disk device must be mounted in order to be listed in inventory. If it is mounted but an inventory scan has not been run, it will appear under Logical drives; after the inventory scan it will also be listed under Hard drives. When the device is disconnected it should be dismounted from the system. On some Linux systems running an older kernel, the device may also stay in the inventory list even after it has been disconnected and dismounted. In this case the managed device needs to be rebooted before the device will be removed from the inventory list.

The same IP address appears twice in the All devices list
For Linux devices on a different segment than the core, you may get a multiple entries using the same IP address in the My devices list for the device. For nodes on the same network segment as the core, the discovery gets a node’s MAC address from the Ethernet from the ICMP packet. For nodes not on the same network segment as the core, the discovery gets the MAC address from an NETBIOS query. Since Linux nodes do not respond to a NETBIOS query, a MAC address cannot be obtained from a standard network scan discovery for Linux nodes on a different network segment than the core. When a client is deployed to a node, the MAC address in the scan file is used to find the inventory record to update (after trying the deviceID). Records that have no MAC address and no DeviceID cannot be found, so a new record is created. You can delete the duplicate entry in the Discovered devices list.
Using the health dashboard [Web console]

The health dashboard is a simple, high-level, uncluttered view of your devices. It represents each device with an icon that shows the device's current health. The devices viewed in the health dashboard are based on scopes and roles. The health dashboard is movable and configurable. The health dashboard displays the overall health of all the devices in the view, listing the number of devices by state (X number of devices in Critical state, X number of devices in Normal state, and so on). You can view a graph and device list or undock the graph and view that by itself on your workstation or a group monitor.

When you right-click a device's icon, you can select basic troubleshooting items, such as ping, trace route and remote control (if the device is managed). You can also select View details, which opens the Real-time Inventory and Monitoring console.

- To open the health dashboard
- To view the Real-time Inventory and Monitoring console
- To view device properties
- To perform basic troubleshooting tasks
- To sort devices by name or health status
- To dock the health dashboard graph
- To view devices by status category
- To refresh the health dashboard

**To open the health dashboard**

1. In the Ivanti Management console, click **Tools > Reporting/Monitoring > Health Dashboard**.

   The health dashboard opens in a Web browser. It displays the devices listed in the **All devices** group. If devices are listed multiple times in **All devices**, they are listed multiple times in the health dashboard.

2. To avoid listing devices multiple times:
   - Configure options for duplicate device name handling in Configure Ivanti Software Services (in the Ivanti® Endpoint Manager powered by Landesk, click **Configure > Services**).
   - When customizing columns in the device view, avoid choosing an attribute that results in listing a device multiple times. For example, selecting software applications can list a device multiple times because it is listed once for each unique software application installed.

   **NOTE:** For dialogs and windows to display properly, the Endpoint Manager Web server must be added to
the allowed list of the browser's popup blocker.

**To view the Real-time Inventory and Monitoring console**

- In the health dashboard, double-click a device.

The Real-time Inventory and Monitoring console lists basic inventory and system information, as well as a remote control option, monitoring and performance alert settings, and power options.

For more information see "Viewing the Real-time Inventory and Monitoring console [Web console]" (1027)

**To view device properties**

- In the health dashboard, right-click a device, then click Properties.

You can view the device name, IP address, the percentage of CPU and memory usage, and the amount of hard disk space remaining. Viewing Properties connects to that device to gather real-time information on key metrics such as storage space and memory used.

If the device is offline (or unable to communicate on the network), the Properties dialog box reports an error.

**NOTE:** If the Real-time Inventory and Monitoring option is not installed with the Ivanti agent on a device, the Properties option does not display when you right-click the device.

**To perform basic troubleshooting tasks**

The health dashboard provides basic troubleshooting functionality, such as pinging the device, remote control (if the device is managed), and access to a device's device information console.

1. To remote-control a device, right-click the device and select Remote control.
2. To ping a device, right-click the device and select Ping device.
3. To send a trace route command to a device, right-click the device and select Tracert device.

**To sort devices by name or health status**

1. In the health dashboard toolbar, click the Sort By drop-down list.
2. Select either Name or Health.

**To dock the health dashboard graph**

1. In the health dashboard toolbar, click Dock graph.

A dockable window opens, which displays the graph and basic status information.

2. To return the graph to the main health dashboard window, click the Dock graph button again.
To view devices by status category

1. In the health dashboard toolbar, click the View drop-down list.
2. Select a health status option (Normal, Warning, Critical, or Critical/Warning).

NOTE: You can also click a bar (or pie section) on the graph to view only devices matching that status.

To refresh the health dashboard

After you add new devices to the My devices list, you must manually refresh the health dashboard to view any of these new devices. To do this, click the Refresh button on the health dashboard toolbar.

This adds and removes devices from the list, and updates the status of each device. You don’t need to manually refresh the health dashboard to view current device health. When the health of any monitored device changes, the health dashboard automatically refreshes its device icons to reflect current device health.

Configuring health dashboard options [Web console]

To configure how the health dashboard displays data

1. On the health dashboard toolbar, click the Options button.
2. Type a number (in seconds) in the Update every box to set how often you want the health dashboard to check for health status updates.
3. Select the graph type you want to display from the Graph type list (3D bar, 3D pie, 2D bar, 2D pie).
4. From the View list, select the status category you want to display. You can display all devices, or display devices by status type (Normal, Warning, Critical, Critical/Warning).
5. Select how you want the devices sorted (by Name or Health).
6. Select Large icons to display the health dashboard view with large icons.
7. Select List view to list the devices with the same columns as the main console. Large icons don’t display in this view.
8. Click OK.

The health status is updated according to the frequency you specify in this dialog. If you want to update status immediately, you can click the Refresh button on the toolbar.

Using remote control [Web console]

Remote control lets you diagnose and troubleshoot device problems. During a remote session, you can do anything on the remote computer that a user sitting at it could do, while using the keyboard layout of your computer. All of your actions happen in real time on that computer. Remote control allows you to:
Fix software and identify hardware problems quickly by allowing authorized users to check and take control of a computer remotely

- Access remote files
- Transfer files in either direction
- Execute remote applications
- Remote reboot

Set remote control access to users through the Role-based administration tool. If you have integrated or certificate-based security, the remote control right can be set to exclude days of the week and/or hours of the day. If a user is remote-controlling a machine, and this user has a time constraint added to the remote control right, the session will no longer work after the ending time of the constraint is reached.

**Prerequisites for using remote control**

- To use remote control from the console, you must first install the remote control viewer. You need administrative privileges on the local computer to install the viewer, which you are prompted to download the first time you access the remote control page. If necessary, you can uninstall the remote control viewer using the Windows Control Panel's Add/Remove Programs applet. Look for *IvantiEndpoint Manager Remote Control Console* in the program list.

- To be remote-controlled, Windows devices must have the product remote control agent installed and loaded. This agent is installed by one of the following actions:
  
  - Create an agent configuration task in the console and schedule a deployment to the device
  - Map a drive from the device to the core server and run the appropriate agent configuration

This agent may be loaded as a resident service in order to provide immediate access to the machine, or (if you have certificate-based security) it may be installed as an on-demand agent that loads only when needed.

- Additionally, you can install the remote control mirror driver to improve the performance of detecting, capturing, and compressing screen changes if the device CPU is slower (< 2.0 GHz) or the network is fast (> 100 MBps). Note that remote control doesn’t support DOS graphics or full-screen DOS windows. The command prompt window may not display initially when using the mirror driver. If this occurs, minimize the window, then maximize it.

**Using remote control**

**To remote control a device using the Web console**

1. In any **My devices** list, right-click the icon of the device you want to connect to and select **Remote control**.
You can also select the device and, in the action pane, click **Properties > Remote Control**.

This action opens the Ivanti Remote Control Viewer. Other remote options include KVM remote control for Intel vPro devices and a browser-based HTML 5 remote control.

2. If you prefer to use another type of remote control, click **Remote access > Remote control** in the Web console toolbox. Select **Direct, KVM, or Browser-based**, and then specify the device name or IP address of the device you want to control.

You can also remote control more than one computer at a time. After starting one session, return to the Web console and select another computer.

For information about Linux device remote control, see "Accessing remote Linux devices [Web console]" (1012).

**Controlling remote Windows devices [Web console]**

**To start remote control**

1. In a Web console device list, select the device you want to control.
2. In the action pane, click the **Properties tab > Remote control**.

You can also right-click the device and select **Remote control**.

The Ivanti Remote Control Viewer opens.

Once you’ve taken control of a remote device, its monitor appears in the main window of the viewer. If the remote control agent is loaded, the **Connection messages** pane in the viewer provides status information.

**Using hot keys in remote control**

**To use hot keys in the remote control viewer**

You must be actively remote controlling a device to use hot keys.

1. With the focus on the viewer window, press the hot key combination for any one of the available actions.
2. To quickly access hot keys, click the **Send a special key sequence** button on the toolbar and select a command.

To view commonly used hot keys and change their key sequence, click **Tools > Options > Hot key settings** tab in the remote control viewer.

---

**NOTE:** If you find that the hot keys don’t work, the focus isn’t on the Viewer window. If the border is
Sending Ctrl+Alt+Delete Windows 7 and newer devices

The default local security policy on Windows 7 and newer won’t allow Ctrl+Alt+Delete from a remote control viewer. To change this, do the following.

**To allow Ctrl+Alt+Delete on Windows 7 and newer 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 **Options** list click either **Services** or **Services and Ease of Access applications**.
5. Click **OK**.

Navigating in the remote device screen

By default the Autoscroll option is enabled. When Autoscroll is enabled and you are remote controlling a device, place your cursor along the yellow/black border of the viewer window and scroll up, down, or side to side. The closer your cursor gets to the border, the faster the scrolling will occur.

You can disable Autoscroll. When you do this, the yellow/black border is replaced by window scroll bars if any part of the remote device’s screen is obscured.

**To disable Autoscroll in the remote control viewer**

1. Click **Tools > Options** and clear the **Allow autoscroll** check box.
2. Click **OK**.
3. Use the horizontal and vertical scroll bars to move the remote device's screen.

Drawing on the remote device screen

You can using basic draw tools to highlight an area of the screen on the remote device. The remote user sees what you draw, which can be helpful if you’re showing something to the user to help them solve a problem.

**To highlight part of the remote screen with draw tools**

1. In the remote control viewer, click the **Highlight an area on the remote screen** button.
2. Use the options on the floating toolbar and draw on the remote screen.
Using a chat session with the remote user

As you run a remote control session, you can open a chat window with the remote device’s user. This is useful when you’re helping someone solve a problem or showing them how to perform a task.

To open a chat window with the remote user

1. In the remote control viewer, click the Start/Stop a chat session button.
2. Type a message in the box and click Send.
3. To end the chat session, click Stop or click the toolbar button again.

The exchange of messages is displayed in the chat window. You can save the chat session to keep for future reference.

Viewing connection messages

The viewer window’s Connection messages pane displays status messages sent to the status bar (such as remote control agent package exchanges). Messages remain in the list so you can:

- View the history of the remote session
- Diagnose problems with the session
- Check whether the remote control agent is loaded
- Check the status of the remote control agent

To view connection messages from the console

- If the Connection messages pane isn’t displayed, click View > Connection messages.

Saving connection messages

While you’re in a remote control session, you have the option of saving the connection messages. These messages may be useful as an audit trail or if you need to troubleshoot any issues related to your remote control session.

To save connection messages

1. In the viewer window, click File > Save connection messages.
2. In the Save As dialog box, type a file name and save as a text file. The connection messages are saved to the My Documents folder by default.

If the remote control agent is loaded, the Connection messages window tells you that the agent is found and what protocol it’s using. In the Web console device list, you will also see a magnifying glass icon appear on the device you selected when the session is established.

Executing programs remotely

In the viewer window, you can start any program on a remote device to diagnose issues.
To execute programs remotely

1. In the toolbar’s Run box, enter the path for the program you want to run. If you need to find the program, select Browse from the list.
2. To run the program on the remote device, click the Remote execute button on the toolbar.

Transferring files to remote devices

You can use the remote control viewer window to transfer files between your machine and the remote device. 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 currently remote controlling a device as long as the connection has been created. The Run each Explorer window in a separate process option doesn’t work with file transfer.

To transfer files to a device

1. On the remote control viewer toolbar, click the Transfer files to the remote computer button.
2. Select a file to transfer by clicking the filename. Right-click the file and select Copy, or select to drag and drop.
3. Scroll down the Windows Explorer tree to Ivanti Remote Control. Below this, click the name of the remote device you’re controlling.
4. On the remote device, open a folder to paste the file to, then right-click and select Paste.

Similarly, you can also transfer files from a remote device to your device.

Shutting down and rebooting remote devices

You can remotely shut down or reboot devices. When you do, a message box appears on the remote device with a warning that the system will shut down in X seconds. If someone is currently at that machine they can click a Shutdown or Cancel button.

If no action is taken the reboot will happen when the countdown reaches 0.

If the device has applications open with unsaved data, those applications will probably interrupt the shutdown when they prompt for the user to save. You may have to remote control the device and save/close applications for the shutdown or reboot to work.

To reboot a remote device

1. In the remote control viewer, click the Reboot the remote computer button on the toolbar.
2. Enter a time for displaying a message box on the remote computer (maximum 300 seconds).
3. Type a prompt to the user that will appear in the message box.
4. To maintain the remote connection after the reboot, select the Continue session after reboot
check box.
5. To keep the settings you have entered as a default, select the **Save these settings** check box.

**Configuring session options**

There are several settings you can change to improve your use of the remote control viewer, such as changing display options, optimizing performance for your network, and changing key mappings for hot keys on the remote computer.

**To configure remote session options**

1. In the remote control viewer, click **Tools > Options**.
2. Make changes on the three pages of the dialog box as described below.
3. When you have finished, click **OK**.

**Change settings tab**

- **Allow autoscroll**: Enables the viewer window to scroll as you move the cursor closer to the yellow/black window border. When this option is cleared, the remote device window has horizontal and vertical scroll bars if part of the window is obscured.
- **Lock out the remote keyboard and mouse**: Locks the device's keyboard and mouse so that only the user running the viewer window can control the remote device. Note that special key combinations in Windows such as "Ctrl+Alt+Delete" or the "Windows Key+L" aren't locked out.
- **Synchronize clipboards**: Synchronizes the clipboards between the viewer console and the remote device so you can paste information between the two machines.
- **Hide the remote computer screen**: Makes the remote device's screen blank so only the user running the viewer can see the display on the remote device.
- **Always ask to clear remote computer's screen**: Rather than automatically clear the remote device's screen, this option displays a message box for the remote user to accept that the screen is cleared.
- **Lock the remote computer when the session ends**: Locks the remote device when the session ends, so anyone at that device must provide credentials in order to use it again.
- **Auto keyboard mapping**: Enables the keyboard layout of the viewer console to be used on the remote device.
- **Enable old agent compatibility**: If you want to remote control a device with an Ivanti agent older than version 8.5, select this check box to enable the connection.
- **Use alternate names**: Enables the use of alternate names for the person using the remote control viewer so that the actual login and computer names do not appear on the remote device. If you select this option, type the alternate names in the text boxes below.

**Optimize performance tab**

- **Optimize performance for**: Select Modem, Broadband, LAN, or Custom as appropriate for your network environment. (These options are also available on the **Optimize performance for**
**connection speed** toolbar button.)

- **Use mirror driver on remote computer**: Loads the mirror driver for enhanced performance on slower machines. This driver can reduce the amount of time required to see the target machine's desktop and increase the visual quality of the targeted desktop's image. It can be useful if the remote control agent is to be downloaded over the Internet or installed on machines by users who do not have administrative rights.

- **Suppress remote wallpaper**: Speeds up the viewing rate by not displaying the remote device's background wallpaper. Some wallpapers can substantially slow down a remote control session.

- **Reduce the color depth**: If you're connecting via a slow link or dial-up networking connection, this option reduces the amount of transferred color information. The closer you move the slider to full reduction, the more color artifacts (distortion) you might see.

**Hot key settings tab**

This page of the dialog box lists eleven hot key combinations that are used by the person running the remote control session to send commands to the remote computer. These hot keys are different than standard Windows key combinations because entering the standard keystrokes would initiate the command on the computer running the remote control viewer, not the remote computer.

To change a hot key, click in the box and press the key combination you want to use. The key combination (for example, Ctrl+Shift+T) is entered for you in the box.

**Accessing remote Linux devices [Web console]**

You can establish an SSH session with a Linux device that has the standard Ivanti agent.

**To access a remote Linux device**

1. Select the device in a Web console device list.
2. In the action pane, click the **Properties** tab.
3. Click the **SSH** button.

When you select SSH access, a window opens with an SSH session on the remote device. You must provide a username and password to access the device. When you have authenticated, a secure shell session opens on the remote device.

**Software distribution overview [Web console]**

The software distribution tool gives you the ability to distribute software packages to target devices. The tool supports many different types of packages.

Software distribution features include:

- 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
• Full-featured package builder to build complete software packages
• Ability to distribute any package type, including MSI, setup.exe, and other installers

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, RPM files (Linux), and so on. In most cases, the software package needs to contain everything necessary to install the application you’re distributing. Put the package on your distribution package delivery server.

2. **Create a distribution package.** 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 switches, and so on. Once you create a distribution package, the information is stored in the database and can be used in multiple tasks.

3. **Create a push delivery method.** The push delivery method defines how a package will be sent to devices. These options aren’t associated with a specific distribution package. 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.** Here you specify the distribution package, the delivery method, the devices that need to receive the distribution package, and when the task should run.

When the scheduled time occurs, the scheduler service will start the scheduled task handler which contacts the software distribution agent on each device and informs it that the package is ready for installation.

The software distribution agent then obtains the package from the delivery server and processes it on the device by installing or removing the packaged files.

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. You can create delivery method templates that are independent of a particular package. 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 work independently from package deliverers. You can create custom groups and subgroups of packages in which you can group related packages for concurrent distribution.

**Prerequisites for software distribution**

Devices receiving the software distribution packages must have the following product agents installed:

• Standard Ivanti agent
• Software distribution agent (Windows only)
If you don’t have an existing package to deploy, you can use Ivanti package-building technology to create a standalone executable program for the required software installation. A Web server or network server can be configured as a “delivery server” to store distribution packages. Through the console, you can schedule the distribution task. 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 previously deployed 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).

**Using the Start command in a batch file package**

The batch file distribution package has been designed to run as if it were issued from the Run command in the Windows Start Menu. When a batch file is executed using the Run command, it closes upon completion. A program that is required to run in an open command window will close prematurely when run through a batch file distribution package.

The program can be configured to continue running by using the `start` command in the batch file. The `start` command will actually spawn a new command window that remains open after the batch file has completed and closed the initial command window.

Here is an example of a batch file that uses the "start" command to spawn a new command window running the Sample.exe program.

```
start "Title" /D "c:\program files\ManagementSuite\ldclient\sdmcache\swd\alerttest" Sample.exe
```

The first parameter ("Title") is the name of the command window that will be displayed in the title bar. Note that the title is mandatory because the path to the executable will be misinterpreted as the title if it is omitted. If the path to the executable includes a space, it must be in quotes. If the title were not present, the quoted path to the file would be mistaken for the title, even though the /D switch indicates the path is present.

This single line batch file runs Sample.exe in a new command window titled "Title." For more help on the Start command, type the command with either the /h or /? switch at a command prompt.

**Distributing software to Linux devices [Web console]**

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 management agent to communicate with the Linux device 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 management 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 server, 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 lower-case.
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, associate it with the delivery method you want, and schedule the delivery.

**About Distribution packages [Web console]**

The Distribution packages view shows the available distribution types and any packages you’ve created for each distribution type. When you select a distribution package you’ve created, you can view the properties for it, delete it, clone it, place it in a group with other packages, or reset the package hash.

To create a new distribution package, select a distribution package type in the left pane and click New.

**Understanding the distribution 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 box.

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.

Macintosh

Any Macintosh file can be downloaded, though Endpoint Manager 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, Endpoint Manager will decompress the file before returning.

**NOTE:** 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.

Windows Script Host Package (WSH)

Windows Script Host Packages (WSH) are a Microsoft alternative to batch files but are often used to automate similar tasks such as mapping drives, copying files, or modifying registry keys. WSH files are most commonly used with Jscript (.js) and VBScript (.vbs) files. One 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 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 Endpoint Manager, Ivanti continues 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.

**Linux**

Software distribution supports Red Hat Enterprise Linux Advanced Platform 5 and SUSE Linux Enterprise Server 10/11. RPM deployment is supported. Scripting is not supported. Additional files need to be in a location where Linux can reach them. A Web share or an anonymous HTTP site can be used to store RPMs. Linux does not support mapped drives.

**Package Groups**

- **My packages**: Distribution packages that the current user has created. Users with Administrator rights can also see these packages.
- **Public packages**: Distribution packages that users have marked public. Anyone who schedules a package from this group will become the owner of the associated task. The task remains in the Public tasks group and will also be visible in the User tasks group for that user.
- **All distribution packages**: Both the current user’s distribution packages and distribution packages marked public.
- **User distribution packages**: (Administrator users only) List of all distribution packages sorted by owner/creator (not including public packages).

**Custom groups**

You can create custom groups in the My packages, Public packages, and User distribution packages groups. Only an administrator can make changes to User distribution packages. With custom groups, you can group related packages such as Microsoft Office 2007 MSI package with a Microsoft Office 2007 executable package. To create custom groups for public distribution packages, you must have the Public distribution configuration right.

**To create a custom group**

1. In the Web console toolbox, click Distribution > Distribution.
2. Click one of the distribution package groups.
3. Click the New group button on the toolbar.
4. Type a name in the Group name box and click OK.
5. To move a package or another group into the new group, select the package or group from a list and click the Move/copy button on the toolbar.

You can move/copy packages or other groups from all package groups except User distribution packages.
Resetting package hashes

The software distribution agent uses the MD5 hash algorithm to verify that the package and additional files are downloaded correctly. When a distribution package is first scheduled, the product 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 the agent computed on the target device, the download isn’t considered valid. If you make any changes to the package outside of this product, 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. In the Web console toolbox, click **Distribution > Distribution**.
2. Find the package in the distribution package groups.
3. Select the package and click the **Reset package hash** button on the toolbar.

Moving/copying packages

You can move or copy distribution package definitions, such as a package that delivers an executable to a set of targeted devices.

To move or copy a distribution package

1. In the Web console toolbox, click **Distribution > Distribution**.
2. Find the package in the distribution package groups.
3. Select the package and click the **Move/copy** button on the toolbar.
4. Select the group in which you want the new package to be saved, and click **Move** or **Copy**.

Moving or copying a distribution package only moves or copies the distribution package settings, not the actual files you are distributing.

Scheduling a distribution task [Web console]

When you have created a distribution package and delivery method, you can schedule the package to be deployed to devices you manage. You can schedule items for one-time delivery or schedule a recurring task.

Before you can schedule tasks for a device, it must have the Standard Ivanti agent and be in the inventory database. Ivanti Server configurations are an exception. You can distribute to a server that doesn’t have the standard management agent.
To schedule a distribution task

1. In the Web console toolbox, click Distribution > Distribution.
2. Find the package in the distribution package groups.
3. Select the package and click the Schedule button on the toolbar.
4. Configure the task by setting options on the five pages of the dialog box.
5. When you have finished, click Save.

For details about individual options in the Scheduled task properties dialog box, see "Scheduling tasks [Web console]" (1023).

NOTE: When you click the Schedule button, a task is created. It has no targeted devices, and it is unscheduled. If you cancel this Scheduled task procedure, be aware that the task will still appear in the Task list.

Creating a delivery method [Web console]

You can create and edit delivery methods in the Web console. The Delivery methods tab displays all publicly available delivery methods and any delivery methods that you've created.

Delivery method groups

Delivery methods are saved in the following groups:

- **My delivery methods**: Delivery methods that the current user has created. The administrative users can also see these delivery methods.
- **Public delivery methods**: Delivery methods that have an owner type of Public or Public user. Anyone who schedules a delivery method from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group for that user.
- **All delivery methods**: Both the current user's delivery methods and delivery methods marked public.
- **User delivery methods**: (administrative users only) List of all delivery methods sorted by owner/creator (not including public delivery methods).

Within each group, delivery methods are organized by type (Policy-supported, Push, Policy, and Multicast).

For more information on how delivery methods are used in software distribution, see "Software distribution overview."
To create a new delivery method

1. In the Web console toolbox, click **Distribution > Distribution**.
2. In the action pane, click the **Delivery methods** tab, select a delivery method type from one of the groups, and click **New** on the toolbar.
3. Type a name for the method in the **Name** text box.
4. Add information on all of the pages of the dialog box, as described below.
5. When you have finished, click **Save**.

**About the Description page**

- **Owner**: Set an individual owner or select **Public** or **Public user** to allow other users to share methods.
- **Description**: 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 names.
- **Number of devices for simultaneous distribution**: Specify the maximum number of devices to which a distribution task can be applied. This can help to limit network traffic as the task is being distributed.

**About the Network usage pages**

Use these pages to manage network usage while tasks are being distributed.

- **Network usage page**: Select file transfer and download options, including preferred server, peer download, and Targeted Multicast™.
- **Bandwidth page**: Specify bandwidth limits and select network connection options.
- **Bandwidth usage page**: Specify maximum percentages of bandwidth to be used in WAN and local distribution settings.
- **Multicast domain page**: Select options for how to implement multicast distributions.
- **Multicast limits page**: Set limits related to multicast delivery and file caching.

**About the Reboot page**

Use this page to configure whether the computer is rebooted after the software has been installed or removed. These options are supported on Windows devices but are not supported on Linux.

- **Reboot only if needed**: Devices will reboot it the package requires it.
- **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.
- **Always reboot**: Devices will reboot regardless of whether the package requires it or not.
About the Feedback and timing pages

Use these pages to determine how users are notified about distribution tasks, and how they can delay or cancel tasks.

- **Feedback and timing**: Select whether to hide or display feedback from the user, and whether to allow the user to delay running the package or cancel it.
- **More deferral options**: Set limits on how many times the user can delay a package and whether to wait for user response or start packages immediately. You must have selected **Display progress to user** on the Feedback and timing page for these options to be available.
- **Custom message**: Select to use either an HTML page or a text-based message box when the user is notified of a package distribution.

About the Type and frequency of policy page

Only available for policy distributions. Select whether the policy is required, recommended, or optional, and select how often the policy is applied (one time, as desired, or on a regular interval).

About the Downgrade page

Use this page to specify whether a distribution package should have its functionality downgraded to the level of the OS and agent on a target device, or whether the package should fail if the OS or agent can’t handle the default functionality of the page.

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 page lets you configure how the service contacts devices.

- **UDP**: Selecting UDP uses a Ping Discovery Service (PDS) ping via UDP. Most device components depend on PDS, so your managed devices should have PDS on them. PDS is part of the standard management agent. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping retries and timeout. UDP discovery is not supported by Linux.
- **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 enabled.
- **Number of retries**: The number of attempts discovery makes to contact devices.
- **Discovery timeout**: The number of milliseconds before discovery retries will timeout.
Timeout for subnet broadcasts: The number of milliseconds before subnet broadcast retries will timeout.

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.

Disable DNS/WINS lookup: When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

Troubleshooting distribution failures [Web console]

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, a task can cause problems on thousands of devices at once. When planning a deployment using software distribution, take care to not create an overwhelming number of problems.

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, test the system 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 rollouts occur should be based upon how much device variety the enterprise has and how much of a load you can handle in troubleshooting problems on target devices.

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 to make sure it is configured to use ICMP and not PDS.

Scheduling tasks [Web console]

The Scheduled tasks tool lists distribution tasks you have run from both the Ivanti Management console and the Web console. Tasks can include Agent configuration, Patch Manager, Software distribution, Provisioning, Scripts, and Device discovery.

In the Web console, you can schedule packages and scripts, policies, and alert rulesets. The tasks are displayed in the action pane for each feature. For example, if you open the Distribution tool, you’ll see a Scheduled tasks tab in the action pane that lists your package distribution tasks. Tasks for all these tools are also listed in the Scheduled tasks tool window.

NOTE: While you can run inventory, patch, and compliance scans from the My devices tool, these tasks are not listed in the Scheduled tasks tool. Status messages for these scans are displayed in the action pane only.

The Scheduled tasks tool window shows these task groups:

- **My tasks**: Tasks that you have scheduled. Only you and administrative users can see these tasks.
- **Public tasks**: Tasks that users have marked as public. Anyone who edits or schedules a task from this group will become the owner of that task. The task remains in the Public tasks group and will also be visible in the User tasks group for that user.
- **All tasks**: Both your tasks and tasks marked as public.
- **All policies**: Your policy-based tasks and those marked as public.
- **User tasks**: (Administrator users only) List of all tasks sorted by owner/creator (not including public tasks).

When you click **My tasks**, **Public tasks**, or **All tasks**, the task list shows information in these columns:

- **Task**: The task names.
- **Start on**: When the task is scheduled to run. Click a task name and click **Edit** to edit the start time or to reschedule it.
- **Status**: The overall task status, which can be Working, All Completed, None Completed, Not Scheduled, Available for Download, or Failed.
- **Distribution package**: The package name the task distributes. This field applies only to distribution packages.
- **Delivery method**: The delivery method the task uses. This field applies only to distribution packages.
- **Owner**: The name of the person who scheduled the task.
- **Task ID**: A sequential number assigned to tasks in the database.

When you double-click a scheduled task, the tool pane shows this progress information:

- **Name**: The task state name.
- **Quantity**: The number of devices in each task state.
- **Percentage**: The percentage of devices in each task state.

Before you can schedule a task for a device, it must have the appropriate agent and be in the inventory database. Server configurations are an exception. They can target a device that doesn’t have the standard management agent.

Tasks can be rescheduled, edited, or deleted either from the Scheduled tasks tool or from the action pane for the specific tool. To edit any task, select it and click the **Edit** button on the toolbar.

### Creating custom task groups

You can create custom groups for the task types **My tasks** and **Public tasks**. With custom groups, you can group related tasks such as scanning for vulnerabilities and running a script.

**To create a custom task group**

1. In the Web console toolbox, click **Distribution > Scheduled tasks**.
2. Select the task group in which you want to create a custom group.
3. Click the **New group** button on the toolbar.
4. Type a name for the group and click **OK**.
5. To move tasks or other groups into the group, select them from a list and click the **Move** button on the toolbar. Select your custom group and click **OK**.

### Moving tasks

Use the **Move** toolbar button to move a task from one task group to another, thus making the task visible to users who can view the task group you are moving the task to.

1. In the **Scheduled tasks** tool or the tasks tab for a Web console tool, select a task from one of the groups (My tasks, Public tasks, All tasks, All policies, or User tasks).
2. Click the **Move** button on the toolbar.
3. Select the task group you want to move the task to, then click **OK**.
Task scheduler help

The Scheduled task - properties dialog box contains these pages:

- Overview page
- Custom scripts page
- Target devices page
- Schedule task page

About the Overview page

- **Owner:** lists the current owner of the task. You can select another user as the owner, or select Public or Public user to save the task in the Public tasks group.
- **Currently selected item:** displays the name of the item being scheduled. Click **Change** to open the Custom page and select a different item.
- **Currently selected targets:** displays the devices that are targeted for the task. Click **Change** to open the Target devices page and change the targets.
- **Scheduled time:** displays when the task is scheduled. Click **Change** to open the Schedule task page and change the time.

About the Custom scripts page

- **Currently selected custom script:** Select the script you want to schedule.

About the Target devices page

Use this page to add device targets for the task you’re configuring. You can also see the targeted devices, queries, and device groups for the task on this tab.

Three drop-down lists contain queries, LDAP queries, and groups that you have created in the Endpoint Manager network view.

- **Add target list:** Add the devices you added to the target list from **My devices**. (See Targeting devices for instructions.)
- **Add LDAP list:** Select an LDAP object that you added to the target list from the Directory manager tree.
- **Add query:** Select a query from the first list and click this button to add the results of the query to the target list.
- **Add LDAP query:** Select an LDAP query from the second list and click this button to add the results of an LDAP query to the target list.
- **Add group:** Select a group from the third list and click this button to add the contents of the group to the target list.
- **Wake up devices:** Select this check box if you want to wake up targeted devices (that are powered down or in a sleep or hibernate state) when the task is started.
- **Remove:** Select a target item and click this button to remove those targeted devices.
NOTE: In the Web console, device groups are not targeted as groups. Instead, if you select a group and target it, the individual devices in the group are added to the targeted devices list.

About the Schedule task page

- **Leave unscheduled**: (default) Leaves the task in the Task list for future scheduling.
- **Start now**: Runs the task as soon as possible. It may take up to a minute for the task to start, depending on other settings.
- **Start at scheduled time**: Starts the task at the time you specify. Specify the following options:
  - **Date**: The date you want the task to start.
  - **Time**: The time you want the task to start.
  - **Repeat every**: If you want the task to repeat, select the period (Hour, Day, Week, or Month). If you pick **Month** and the date doesn’t exist in all months (for example, 31), the task will only run in months that have that date.
- **Schedule these devices**: The first time a task runs, leave the default of **All**. For subsequent runs, choose from one of the following.
  - **Devices that did not succeed**: Select this if you want the task to run only on 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.
  - **Waiting or currently working**: Select this if you want the task to run on devices that are waiting to be processed or are currently being processed.
  - **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 did not try to run the task**: Select this if you want the task to run only 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.
  - **Retry task on failed devices**: If a task fails on a device, allows the task to be retried. Specify the number of retries allowed on a device.

About the Distribution package

For information on the options in the **Distribution package - properties** dialog box, see **Software Distribution help**.
Viewing the Real-time Inventory and Monitoring console [Web console]

Use the Real-time Inventory and Monitoring console to view top-level summary information about a device, view system information like CPU or fan information, monitor the health status and thresholds of key components of a device, manage vulnerabilities, and power on, power off, or reboot a device.

The Real-time Inventory and Monitoring console includes the following tools:

- **System information**
- **Remote session**
- **Monitoring**
- **Rulesets**
- **Power options**
- **Hardware configuration**

NOTE: In order to view the Real-time Inventory and Monitoring console for a device, you must first deploy the Ivanti management agent, with the Real-time Inventory and Monitoring components selected, on that device. Also, the device must be rebooted after the agent is installed for the server information console to function correctly. This reboot is required when you install the agent on the core server as well as on managed devices.

To view the real-time inventory console

1. In the Ivanti Management console, right-click a managed device and select **Real-time inventory and monitoring**.

   You can also click **Tools > Reporting/Monitoring > Health dashboard** and double-click a device in the list of devices.

   The console opens in a new browser window and shows the **Health summary** page by default.

2. Click the health summary buttons to view details about device health information.

3. Click items in the toolbox to use the available tools.

**System information**

**System information** contains summary data about the health of the device, as well as information about hardware and software, system logs, and other data such as asset and network information.
Health summary

The **Health summary** page provides a quick overview of system health for this device. You can see at a glance whether selected hardware elements are functioning correctly and whether there are potential problems that may need to be addressed.

When any of the health elements are in a warning or critical state, the corresponding button contains a yellow (warning) or red (critical) icon indicating that a problem exists. Click the button to view a description of the event that caused the warning or critical alert.

System summary

Use the **System summary** page to view important information about the selected device. The information listed on the page can include the following, depending on the type of hardware and software configured on the device.

- **Health**: The overall health of the device as defined by the conditions and parameters you set.
- **Type**: The type of the device, such as print, application, or database.
- **Manufacturer**: The maker of the device.
- **Model**: The model of the device.
- **BIOS version**: The version of the device's BIOS.
- **Operating system**: The device's operating system.
- **OS version**: The version number of the operating system.
- **CPU**: The manufacturer, model, and speed of the device's processor.
- **IPMI type, IPMI version**: The type and version number of IPMI the device is using.
- **BMC version**: For Intel AMT and vPro devices, the version number of the baseboard management controller.
- **SDR version**: The version of the Sensor Data Record in the device's BMC.
- **Vulnerability scanner**: The version of the vulnerability scanner.
- **Remote control**: The version of the remote control agent.
- **Software distribution**: The version of the software distribution agent.
- **Inventory scanner**: The version of the inventory scanner.
- **Kernel**: For Linux devices, the version number of the kernel installed.
- **Monitoring**: The version number of the monitoring agent on the device.
- **CPU usage**: The percentage of the processor currently being used.
- **Physical memory used**: The percentage of total physical memory used on the device.
- **Virtual memory used**: The percentage of total virtual memory used on the device.
- **Last reboot**: The date and time the device was last rebooted (in the time zone of the database).
- **Drive**: The drives on the device with the total size of the drive and percentage of space used.
This information is taken from the registry in Windows or from configuration files in Linux.

*This information appears after an agent has been installed on the device.

**Hardware**

Use the **Hardware** page to view details about the device's hardware configuration. Items in the **Hardware** list are grouped in the following categories. Note that not all categories appear for all devices. For example, if the device does not have fan and temperature sensors, the **Cooling** category does not appear in this list.

- **CPU**: Processors and cache
- **Storage**: Logical drives, physical drives, removable media, and storage adapters
- **Memory**: Usage information and memory modules
- **Chassis**: The server's chassis; view whether the case is open or closed
- **Input devices**: Keyboard, mouse, and other devices
- **Motherboard**: Motherboard, expansion slots, and BIOS
- **Cooling**: Fans and temperature sensors
- **FRUs**: Field-replaceable units
- **Power**: Power supplies
- **Voltage**: Voltages
- **IPMI sensors**: Discrete and numeric sensors
- **Dell DRAC**: Dell DRAC data. Click buttons to launch Dell DRAC Utility and Dell DRAC server administrator.

**Setting alerting thresholds for hardware items**

Some items in the **Hardware** list represent data from sensors in the device, such as temperature sensors. If a managed device contains components with supported sensors, you can change the sensor readings that will trigger an alert. For example, a CPU temperature sensor can have lower and upper temperature readings that trigger warning and critical alerts. Thresholds are generally based on manufacturer’s recommended settings, but you can change the upper and lower settings using the **Thresholds** dialog box.

1. In the Real-time Inventory and Monitoring toolbox, click **System information**.
2. Expand the **Hardware** folder to find the hardware element you want (such as **Cooling > Temperatures**).
3. In the list of sensors, double-click the sensor you want to set thresholds for.
4. Type values in the lower and/or upper threshold text boxes, or drag the sliders on the trackbar to the left or right to change the values.
5. Click **Update** to save your changes.
6. To return to the original values for the thresholds, click **Restore defaults**.
Logs

The Logs page displays local system logs, the System Events Log (SEL) for IPMI devices, and an alert log.

Local logs, such as the Application, Security, and System logs, have a Refresh button to display the most current data, and a Clear button to remove all items from the list.

If this device’s BIOS has the ability to clear the BIOS log, click the Clear button to remove all log entries. This button is unavailable if the BIOS does not support this action.

The Alert log displays all current alerts for the device. You can filter by name, state, or instance to reduce the number of alerts in the list, and you can enable date filtering to show only alerts from a specified range of dates.

The Hardware events log displays real-time data, or archived items. You can delete individual items, purge all items in the list, or refresh the list to show most recent log items.

The Provisioning history page displays the provisioning history of the device, including the date of the provisioning action, its status, and the template used.

Software

The Software page shows summary information about processes, services, and packages on this device, as well as a list of current environment variables.

- **Processes**: Displays processes that are running; right-click a process and select Kill process to terminate it
- **Services**: Displays services available on the device and their status; right-click a service and select Stop, Start, or Restart to make changes
- **Packages**: Lists installed packages with version numbers and vendor name
- **Environment**: Lists the environment variables currently set on the device

Other

The Other page shows asset information and a summary of network hardware and connections.

- **Asset information**: View and edit asset management information. Click Contact information to enter details such as the name and position of the person using the device, as well as location, department, and the asset tag number on the device. Click System information to view system information such as serial number, manufacturer, and chassis type
- **Network information**: View a list of network hardware installed, statistics of network activity, a configuration summary (including IP address, default gateway address, and WINS, DHCP, and DNS server information), and a list of current network connections (mapped drives)
Remote session

Use Remote session to start a remote control session with the selected device. If the device is a Windows server, standard product remote control launches. For Linux servers, you can choose between SSH and SFTP remote sessions.

In the Real-time Inventory and Monitoring toolbox, click Remote session and then click Launch to initiate the remote control session.

Monitoring

Use Monitoring to view performance counters and to set thresholds for device components. Performance counters are used with the Performance monitor alert to monitor specific performance-related events on a device. You must have deployed an alert ruleset to the device that includes the Performance monitor alert rule in order to receive alerts based on performance counters.

To select a performance counter to monitor

1. In the Real-time Inventory and Monitoring toolbox, click Monitoring.
2. Click the Performance counter settings tab.
3. From the Objects column, select the object you want to monitor.
4. From the Instances column, select the instance of the object you want to monitor, if applicable.
5. From the Counters column, select the specific counter you want to monitor.
6. Specify the polling frequency and the number of days to keep the counter history.
7. In the Alert after counter is out of range text box, specify the number of times the counter will be allowed to cross the thresholds before an alert is generated.
8. Specify upper and/or lower thresholds.
9. Click Apply.

To view a performance graph for a monitored counter

1. Click the Active performance counters tab.
2. In the Counters list, select the counter for which you want to see a performance graph.
3. Select View real-time data to display a graph of current performance, or select View historical data to display a graph showing performance over the period you specified (using the Keep history option when you selected the counter.)

On the performance graph, the horizontal axis represents time that has passed. The vertical axis represents the units you are measuring, such as bytes per second (when monitoring file transfers, for example), percentage (when monitoring percentage of the CPU that is in use), or bytes available (when monitoring hard drive space).
## Rulesets

Use the **Rulesets** tool to view a list of the alert ruleset configurations assigned to the selected device, and to view the details of each alert.

**To view alert rulesets**

1. In the Real-time Inventory and Monitoring toolbox, click **Rulesets**.
2. Select a ruleset name from the drop-down list to view details of that ruleset.

The columns for each alert are described below.

- **Alert type**: A description of the alert event that is monitored.
- **State**: When an alert event reaches the severity state in this column, an alert will be generated. Multiple states can be selected for an event.
- **Action**: The action that occurs when the alert is generated, as defined in the alert ruleset.
- **Contribute to health**: If the alert event reaches the specified state, the health status of the device changes in the All devices list or the health dashboard.

## Power options

**Power options** lets you power off, reboot and, in the case of managed IPMI and Intel vPro devices, power on remote devices. In the case of non-IPMI devices, the device must have the Ivanti agent deployed to it in order to execute the reboot and power off functions.

With IPMI and Intel vPro devices, you must have configured the correct credentials to execute the power on/power off and reboot features. If IPMI or Intel vPro devices have the Ivanti agent deployed, then you can execute the power off and reboot features without the IPMI or Intel vPro credentials. To configure BMC credentials for IPMI devices, use Configure Services.

**To use power options on the selected device**

1. In the Real-time Inventory and Monitoring toolbox, click **Power options**.
2. Select **Reboot**, **Power off**, or **Power on**, then click **Submit**.

**NOTE:** If you have multiple core servers, you can use power options only from the core server that you first log in to. If you switch to another core and then attempt to use power options, the power command will not be successful.

## Hardware configuration

The **Hardware configuration** tool lets you configure options for devices with IPMI, Intel vPro, and Dell DRAC capabilities. This tool and any options are only displayed on devices with the corresponding hardware (for example, IPMI options are displayed only if the device is recognized as an IPMI device).
Viewing the alert log [Web console]

Use the global Alert log page to view alerts sent to the core server. The log is sorted by time (GMT) with the most recent alert at the top.

To view the global alert log

1. In the Web console toolbox, click Monitoring > Alert log.
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 alert name, state, instance, device name, or IP address, select the criteria in the Filter 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 filter text box. To search by date, select Enable date filtering and enter a start date and end date. When you have added filter criteria, click the Find button.
5. To clear the health status of an alert, select the alert in the Alert name column and click the Acknowledge alert button on the toolbar, and then click OK.
6. To delete a log entry, right-click the alert and select Delete entry.
7. To delete all entries in the log, right-click any line in the Alert name column and select Purge log.

NOTE: 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.

Click here for descriptions of alert log columns.

- **Alert name**: The name associated with the alert, as defined in the Alert configurations page.
- **Time**: The date and time the alert was generated (GMT).
- **State**: 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.
- **Instance**: Provides more detailed information as to the situation in which the alert was generated.
- **Device name**: The name of the device on which the alert was generated. This should be a fully qualified domain name.
IP address: The IP address of the device on which the alert was generated.

Using queries [Web console]

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

For example, you can create and run a query that returns only devices with a processor clock speed of less than 2 GHz, or with less than 4 GB of RAM, or with a hard drive of less than 80 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.

In Endpoint Manager you can create database queries for devices in your core database, and you can create LDAP queries for devices located in other directories.

In the Web console, you can create core database queries using the Queries tool. You create LDAP queries with the Directory manager tool.

Viewing available queries

The Custom queries page displays a list of queries that you have created, either in the Endpoint Manager network view or in the Web console.

To view available queries

1. In the Web console toolbox, click Reporting > Queries.
2. Expand the groups (My queries, Public queries, or All queries) to find a query.
3. Right-click a query to edit, delete, or run it.

Running queries in the Web console

To run a query

1. In the Web console toolbox, click Reporting > Queries.
2. Expand the groups (My queries, Public queries, or All queries) to find a query.
3. Select the query and click the Run button on the toolbar.
   The query results are displayed in the tool pane.
4. To print the query results, click the Print view button on the toolbar. The complete query results are listed in a table format. Use your browser’s Print feature to print the list.
5. To save the query results to a CSV (comma-separated value) file, click the Save as CSV button on the toolbar and specify a location to save the file.
6. To view a brief inventory summary of a device in the query results, right-click the device and click View computer.

NOTE: If the query list spans multiple pages, use the arrows at the top right of the page to navigate between pages. Enter the number of items to display per page and click Set.

Creating custom queries [Web console]

Custom queries are useful when you want inventory details about hardware and software installed on your devices. Use a custom query to build a list of devices with similar inventory. For example, if you want to upgrade all devices to at least a 2 GHz processor, you can query for all devices in your database with processor speeds of less than 2 GHz. Custom queries are also used to define groups and scopes.

You can query on any of the inventory items (known as "attributes") that the inventory scanner stores in the database.

Managing queries

Manage queries in the Queries tool pane. Use this tool to create, edit, or delete queries:

- To run an existing query, select it and click Run.
- To create a new query, click New. Once you have created and saved that query, its name will appear in the list on this page.
- To edit a query in the list, double-click it. The Edit query page appears with query parameters you can edit.
- To edit the most recent query, click Edit current.
- To delete a query, select the query and click Delete.
- To clear the query parameters from the Edit query page, click the Clear toolbar button. If the query has already been saved, it's cleared from this page but remains in the Custom queries list.

Creating a query is a four-step process:

1. **Create a search condition:** Specify a set of inventory attributes that will be the basis of your query.
2. **Select attributes to display:** Refine or "filter" the query so that the results display the attributes most useful to you, such as IP addresses or computer device names.
3. **Sort results by attributes:** Specify how you want the query results sorted. (This option applies only if, in step 2, you chose to display more than one type of attribute in the query results.)
4. **Run the query:** Run the query you just created. You can also save it for later use, or clear all of the query information to begin again.
Step 1: Creating a search condition [Web console]

A search condition is a set of inventory attributes and associated values that you query for. You can use one search condition or group several together to form the basis of a query.

The following steps take place on the Edit query page. From the Custom queries view, click New, or select an existing query and click Edit.

To create a search condition

1. In the Web console toolbox, click Reporting > Queries.
2. On the toolbar, click New, or select an existing query and click Edit.
3. Under Step 1, click Edit. A window appears showing a list that represents all of the inventory data currently in the database.
4. Drill down this list to select the attributes that will be your search condition. For example, to locate all clients running a particular type of software, you would select Computer.Software.Package.Name.
5. After selecting the attributes, you'll see a series of fields in the right side of the window. From these fields, select an operator and value to complete the search condition. For example, to locate all clients running Internet Explorer 7.0, select the attributes "Computer.Software.Package.Name", the operator "," and the value "Internet Explorer". Select the Boolean operator AND, then click Add. Select the attributes "Computer.Software.Package.Version", the operator "LIKE", and the value "8", and click Add.
6. You can continue to refine the query by creating another search condition, then adding it to the first with a boolean operator (AND or OR). Also use the buttons to add, delete, replace, group, or ungroup the conditions you create.
7. When you’re finished, click OK.

NOTE: To run and store a query on the health status of servers (Computer.Health.State), you should be aware that the state in the database is represented by a number. Use the table below to create search conditions. For example, to create a search condition for machines with "Unknown" health, use the operator "NOT EXIST".

<table>
<thead>
<tr>
<th>Health condition</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>NOT EXIST</td>
</tr>
<tr>
<td>Normal</td>
<td>2</td>
</tr>
<tr>
<td>Warning</td>
<td>3</td>
</tr>
<tr>
<td>Critical</td>
<td>4</td>
</tr>
</tbody>
</table>
Step 2: Selecting attributes to display [Web console]

For Step 2, select the attributes that will be most useful for identifying computers returned in the query results. For example, if you want results that help you physically locate each computer matching the search condition set in Step 1, you would specify attributes such as each computer’s display name (Computer.DisplayName) or IP address (Computer.Network.TCPIP.Address).

To select attributes to display

1. On the Edit query page, under Step 2, click Edit. A window appears showing a list that represents all of the inventory data currently in the database.
2. Drill down this list to select an attribute to display in the query results list. Remember to select attributes that will help you identify the clients returned in the query.

   NOTE: If you’re using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, Computer.DisplayName, Computer.DeviceName, Computer.Device ID, Computer>Login Name, and so on).

3. After you’ve selected an attribute, click Add to move it into the box on the bottom half of the window.
4. If you want to enumerate your query results list, select Include count.
5. Repeat the process to add more attributes. Use the arrow buttons to add or remove attributes, and click Move up or Move down to change the order of attributes.
6. To enable the results of the query to be targetable for any actions you specify, select Make results targetable.
7. When you’re finished, click OK.

You can also edit the column headings in your query results list.

To change column headings

1. Under Step 2, click Edit.
2. In the bottom box, click a column heading and click Edit. Edit the heading and press Enter. Repeat as necessary.
3. Click OK.

At this point, you may want to save your query. The next procedure in creating a query is optional and applies only to query results that contain two or more columns. To save your query, click the Save button on the toolbar. Type a name in the Save query dialog box, select a group, and then click Save.

Step 3: Sorting results by attribute [Web console]

This step is necessary only if you defined more than one attribute and column heading in Step 2 and now want to sort the results alphabetically or numerically within one of those columns.
For example, if you specified two different attributes to display in the query results (the IP address and the processor type), you could sort alphabetically by processor type in the results.

If you skip this step, the query will automatically sort by the first attribute selected in Step 2.

**To sort results by attribute**

1. On the **Edit query** page, under **Step 3**, click **Edit**. A window appears showing the attributes you selected in **Step 2**.
2. Select which attribute you want to sort by, then click >> to move it over to the **Selected attributes** box.
3. Click **OK**.

For more information, see "Welcome to Ivanti SmartVue" (629).

**Step 4: Running the query [Web console]**

After creating your query, you can run it, save it, or clear it to start over.

**To save the query for future use**

1. On the **Edit query** page, click the **Save** toolbar button. The query now appears in the list on the **Custom queries** page.
2. If your query is a modified version of another one, click the **Save as** toolbar button to give it a new name.

By default, saved queries are only visible by the person who saved them. If you select **Public query** before saving, the saved query will be visible to all users. Only administrators with the public query management right can make a query public.

**To view the results of a query**

- Click the **Run** toolbar button.

**NOTE:** Query statements are executed in the order shown. If no groupings are made, the query statements 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.

**Viewing query results [Web console]**

Query results match the search criteria you specified in the query-building process. If the results aren’t what you expected, go back to the **Edit query** page and refine the information.

**To view inventory information about a device in the query results**

- Right-click the device name and select **View computer**.
To print the results of a query

1. Click the Print view button on the toolbar. The complete query results are listed in a table format.
2. Use your browser’s Print feature to print the list.

To save query results as a CSV file

1. Click the Save as CSV toolbar button.
2. Specify the location where you want to save the file.

Exporting query results to a CSV file [Web console]

To view your query results data in a spreadsheet or other application, export the data as a comma-separated value (CSV) file.

To save query results as a CSV file

1. On the Query results page, click the Save as CSV toolbar button.
2. Specify a location to save the file to.

Exporting and importing queries [Web console]

You can export and import any queries you create. All queries export as XML files.

The export and import features are useful in two scenarios:

- If you need to reinstall your database, use the export/import features to save your existing queries for use in a new database.

  For example, you could export the queries and move them to a directory unaffected by a database reinstall. After reinstalling the database, you could move the queries back into the queries directory on your Web server, then import them into the new database.

- You can use the export/import features to copy queries to other databases.

  For example, you could export a query to a queries directory on your Web server, then send it to another Ivanti administrator. That person could then place the queries into the queries directory on another Web server and import them into a different database.

To export a query

Complete these steps while connected to a database that has a query you want to export.

1. In the Web console toolbox, click Reporting > Queries.
2. On the Custom queries page, click the query name you want to export. Click the Edit button on the toolbar.
3. On the **Edit query** page, click the **Export** toolbar button. The **Query exported** page is displayed.
4. To view the XML document for the query, click the XML document link.
5. To save the XML document, right-click the link and select **Save target as.** Specify a location to save the file.

**To import a query**

Complete these steps while connected to a database to which you want to import a query.

To import a query back into a database, the query must be in the queries directory recognized by the Web server. By default this directory is `c:\inetpub\wwwroot\LANDesk\LDMS\queries`.

1. In the Web console toolbox, click **Reporting > Queries.**
2. On the **Custom queries** page, click the **New** toolbar button.
3. On the **Edit query** page, click the **Import** toolbar button.
4. Select the query you want to import. If you want to verify the parameters of this query before importing it, click the **View** toolbar button.
5. Click **Import** to import the query. If you want to import all the queries in the list, click **Import all**.

**Creating LDAP queries using Directory manager [Web console]**

In addition to the ability to query the core database with database queries, you can also use the **Directory manager** tool to locate, access, and target 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.

**Adding an LDAP directory**

To manage an LDAP directory, you need to add it to the Directory manager list. To do so, you’ll need to know the location of the directory on your network and a set of credentials to access the directory.

**To add an LDAP directory to Directory manager**

1. In the Web console toolbox, click **Distribution > Directory manager.**
2. Click the **New directory** button on the toolbar.
3. Type the URL to access the directory. You don’t need to type the initial "LDAP://" in the URL.
4. Type a user name and password to access the directory.
5. Click **OK**.

The directory is listed with a tree icon in the Directory manager tool pane. You can also select the directory and click the **Edit** button on the toolbar to view its properties.
Viewing LDAP directories

When you have added at least one directory, you can view items in the directory in the Directory manager tree view, which displays all registered directories and users.

There are two tabs in the action pane, LDAP target list and LDAP queries. Click these to view LDAP objects that you have targeted and LDAP queries you have defined.

Targeting LDAP objects

You can select objects in the Directory manager tree and target them. The devices contained in those LDAP objects can be selected as targets for an action you want to apply to them, such as software distribution or patch and compliance scans.

To target LDAP objects

1. In the Web console toolbox, click Distribution > Directory manager.
2. Browse the Directory manager tree and select an object in the LDAP directory.
3. Select one or more items in the Directory resources list and click the LDAP targets button on the toolbar.
4. Select the tool you want to apply to the targeted devices. The items you’ve targeted are displayed in the Target list option for the tool.

Creating LDAP directory queries

You can create a query that returns results for a directory object, such as a root organization (o), domain component (dc), or organizational unit (ou).

To create an LDAP query

1. In the Web console toolbox, click Distribution > Directory manager.
2. Browse the Directory manager tree and select an object in the LDAP directory. The query that you’re creating will return results from this point in the tree down.
3. Click the New LDAP query toolbar button.
4. Type a descriptive name for the query.
5. Select an LDAP attribute that will be a criterion for the query.
6. Click a comparison operator for the query (=, <=, >=) and a value for the attribute. If you select Contains or Exists, no value is needed.
7. If the query is complex, select AND or OR to join the statement to the next statement.
8. Click Insert to add the statement.
9. Create additional statements by repeating steps 5-8.
10. To negate a statement, select it and click NOT. To delete a statement, select it and click Delete.
11. When the query is complete, click Test to check that the query returns results.
12. If you want to edit the query and use freeform LDAP syntax, click Advanced. The query opens in an editing window that lets you use any syntax options.

13. When you've finished, click Save. The saved query will appear on the LDAP queries tab in the action pane of Directory manager.

**About the Advanced LDAP query dialog**

From the Basic LDAP query dialog box, click Advanced to open the Advanced LDAP query dialog box. The Advanced LDAP query dialog box also opens when you edit a query that has already been created.

- **Name:** The name of the LDAP query. Edit the name to create a copy of an existing query.
- **LDAP query root:** Displays the 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:** Create an LDAP query in a freeform manner.
- **Test:** Click to execute a test of the query you have created.

**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.

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>`
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.

**Managing inventory [Web console]**

You can use inventory scanning to view hardware and software data for managed devices. Inventory data is stored in the core database. This includes hardware, device driver, software, memory, and environment information. Use this inventory data to help manage and configure devices, and to quickly identify system problems.

You can view, print, and export inventory data. You can also use it to define queries, group devices together, and generate specialized reports.

**Inventory scanning overview**

When you configure a device with a Ivanti management agent, the inventory scanner is one of the components that gets installed on the device. When you create an agent configuration, you can specify when the inventory scanner runs on the device.

The inventory scanner runs automatically when the device is initially configured. The scanner executable is named `ldiscn32.exe` for Windows devices and `ldiscn` for Linux devices. The inventory scanner collects hardware and software data and enters it into the core database. After that, the hardware scan runs at the interval you specify (by default it runs once a day).

After the initial scan, the inventory scanner can be run from the console as a scheduled task. The standard management agent must be running on remote devices to schedule an inventory scan to them.
NOTE: A device added to the core database using the Unmanaged device discovery tool 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 All devices list 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
- Keep track of hardware and software changes on devices, and generate alerts or log file entries when such changes occur

Delta scanning

After the initial full scan is run on a Windows device, subsequent running of the inventory scanner only captures delta changes and sends them to the core database. Use the scanner option /RSS to gather software information from the Windows registry. (This option does not apply to Linux devices.)

Forcing a full scan

If you want to force a full scan of a Windows device's hardware and software data, you can delete the existing delta scan file and change a setting in Configure Services. (This option does not apply to Linux devices.)

1. Delete the invdelta.dat file from the device. 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 > Ivanti, right-click the Inventory Scan shortcut icon, select Properties > Shortcut, then edit the Target path.
3. At the core server, click Start > All Programs > Ivanti > Ivanti 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 (ldiscn32.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 compression is not used on Linux devices.)
Scan encryption

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

1. At the core server, click Start > All Programs > Ivanti > Ivanti 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.

Viewing inventory data

Once a device has been scanned by the inventory scanner, you can view its system information in the following ways:

- Viewing summary inventory
- Viewing full inventory
- Viewing attribute properties
- Viewing system information

You can also view inventory data in reports that you generate.

Viewing summary inventory from the real-time inventory console

Summary inventory is found on the Summary page in the server information console and provides a quick look at the device's basic OS configuration and system information.

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 server for the summary inventory feature to complete successfully.

To view summary inventory

1. In the Endpoint Manager console's network view, in a Devices group, right-click a device and select Real-time inventory and monitoring.
2. In the toolbox, click System information > System Summary.

Summary data

This information appears when you view summary inventory for a managed device.

- Health: The current health state of the device.
- Type: The type of device.
- Manufacturer: The manufacturer of the device.
- **Model**: The device's model type.
- **BIOS version**: The version of the ROM BIOS.
- **Operating system**: Windows or Linux OS running on the device.
- **OS Version**: Version number of the OS running on the device.
- **CPU**: Type of processor or processors running on the device.
- **Vulnerability scanner**: The version of the agent installed.
- **Remote control**: The version of the agent installed.
- **Software distribution**: The version of the agent installed.
- **Inventory scanner**: The version of the agent installed.
- **Monitoring**: The version of the monitoring scanner installed.
- **Last reboot**: The last time the device was rebooted.
- **CPU usage**: The percentage of the processor currently in use.
- **Physical memory used**: Amount of RAM available on the device.
- **Virtual memory used**: Amount of memory available to the device, including RAM and swap file memory.
- **Drive space used**: The percentage of drive space currently used. If you have more than one hard drive, each drive will be listed.

Devices that are IPMI-enabled display additional IPMI-specific data. Linux devices also display similar information in the **Summary** view.

**Viewing 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 Endpoint Manager console's network view, in a **Devices** group, double-click a device.
2. In the Web console's **My devices** tool, select a group (such as My devices) and click a device. In the action pane, click the **Properties** tab, and then click **View inventory**.

**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**

1. In the full inventory list, click the attribute in the left pane. You may need to expand items to find the attribute you want.
2. To print the information, use your browser's **Print** feature.
Viewing system information

From the Real-time Inventory and Monitoring console, you can view and modify the device's system information. Information in the Hardware, Logs, Software and Other categories is either stored data or real-time data. When you click an information link you can view detailed information about the selected component and, in appropriate cases, set thresholds and enter information.

1. In the Web console's All devices view, double-click a device.
2. In the toolbox, click System information.
3. Expand the group and click the information link you want to view.
Ivanti Inventory Manager

Ivanti Inventory Manager is a version of Ivanti® Endpoint Manager powered by Landesk 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 Endpoint Manager 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 Endpoint Manager 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 Endpoint Manager features like software distribution and remote control that aren’t part of Inventory Manager.