Patch and Remediation 8.6

User Guide

ivanti

Endpoint Security

powered by HEAT

Notices

Version Information

Ivanti Endpoint Security User Guide - Ivanti Endpoint Security Version 8.6 - Published: Dec 2020 Document Number: 02_215_8.6_171321400

Copyright Information

Table of Contents

Chapter 1

Ivanti Patch and Remediation Overview

In this chapter:

- Patch and Remediation at a Glance

Ivanti Patch and Remediation (Patch and Remediation) is an Ivanti Endpoint Security module that audits and remediates software and system configuration vulnerabilities within your network. It can also be used for network-wide installation of content non-related to vulnerabilities, such as software or service packs.

To accomplish this task, Patch and Remediation uses two main components: The *Ivanti Endpoint Security Server* and the *Ivanti Endpoint Security Agent*.

Patch and Remediation uses the Ivanti Endpoint Security Server to download content and then deploys it throughout your network. Content includes data that identifies vulnerabilities, patches that remediate them, and various other types of software and service packs. Content is deployed with assistance from the Ivanti Endpoint Security Agent.

The agent scans its host endpoint via a Discover Applicable Updates task, which takes a system inventory of endpoint software, hardware, and system configuration settings. The Discover Applicable Updates results are sent back to the server, which compares these results with a list of known vulnerabilities. Based on these results and administrator input, the server deploys content as needed.

Patch and Remediation at a Glance

Patch and Remediation is a module you can use to install patches and other software on your network endpoints.

Benefits

- Identifies endpoint vulnerabilities and remediates them by installing content (such as software and patches).
- Scans agent-managed endpoints for an inventory of their hardware and software.
- Lets you deploy patches, software, and other types on content to endpoints.
- Lets you establish Mandatory Baselines, which are content standards applied to endpoint groups that monitor endpoints to ensure defined content is always installed.
- Adds new Patch and Remediation-related reports, agent policies, default options, widgets, access rights, and email notifications.

Chapter 2

Getting Started with Patch and Remediation

In this chapter:

Patch and Remediation is a Ivanti Endpoint Security module that remotely installs patches and other software on your managed network endpoints. To get started with Patch and Remediation, you should install the module and then perform several other tasks essential to its operation.

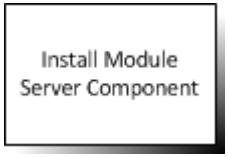
After performing these tasks, you will be able to deploy patches and other content to endpoints in your network, thus remediating potential exploits.

Following completion of these initial tasks, take some time to grow accustomed to the Patch and Remediation. You will continue to perform these tasks, plus many other. Ivanti Endpoint Security contains many features and functions, and by learning the environment, you can secure your network quickly and efficiently.

The Ivanti Patch and Remediation Workflow

To use Ivanti Patch and Remediation (Patch and Remediation), all Ivanti Endpoint Security components must be installed, along with the Patch and Remediation module. After installing all necessary components, review this chart to understand the Patch and Remediation work flow.

Refer to the following flow chart to determine tasks when using the Patch and Remediation module within Ivanti Endpoint Security.



Install the Patch and Remediation module server component. This component is installed after initial Ivanti Endpoint Security installation. For additional information, refer to Installing the Patch and Remediation Module Server Component on page 19.

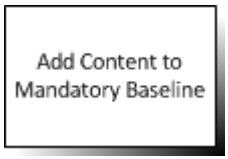
Note: If you purchased a Patch and Remediation license during your initial Ivanti Endpoint Security purchase, Patch and Remediation is installed during the initial Ivanti Endpoint Security installation by default.

Install the Patch and Remediation module endpoint component on agents you want to support Patch and Remediation functions. Each agent you install the endpoint component on consumes a Patch and Remediation license. For additional information, refer to Installing the Patch and Remediation Module for Endpoints on page 20.

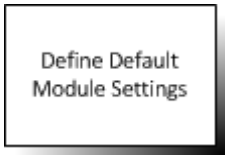
Create *groups* containing Patch and Remediation endpoints in preparation for *deployment*. A group associates similar endpoints for the purpose of deploying content to multiple endpoints. For additional information, refer to Creating New Groups on page 21.

Create new agent policy sets (or edit existing policy set for Patch and Remediation functions) and apply them to Patch and Remediation groups. Agent policy sets are a compilation of values that govern agent behavior. New settings for agent policy sets are added after installing Patch and Remediation. For additional information, refer to Apply Agent Policy Sets on page 22.

View network vulnerabilities and then deploy content, which are patches and other software, to managed endpoints. First, view network vulnerabilities. Agents detect vulnerabilities by scanning endpoints for signatures that indicate a vulnerabilities are present. The, remediate vulnerabilities using a deployment, which triggers the agent to download selected content from the Ivanti Endpoint Security Server. For additional information, refer to Viewing and Remediating Vulnerabilities on page 23.



After initial vulnerabilities are remediated, you can define a Mandatory Baseline. This baseline is a selection of user-defined content that must always be installed on all group endpoints. If an endpoint falls out of compliance, the Mandatory Baseline ensures the endpoint is patched back into compliance via automatic deployment. For additional information, refer to Installing the Patch and Remediation Module for Endpoints on page 20.



Define default Patch and Remediation settings. New default settings are added to Ivanti Endpoint Security after Patch and Remediation is installed. New settings include new access roles, email notifications, and deployment options. For additional information, refer to the following topics:

- Defining Default Deployment Options on page 25
- Editing Email Notifications on page 25
- Editing Custom Roles on page 26

Logging In

Get started with Ivanti Endpoint Security by logging in.

You can access the console from any endpoint within your network.

Note: When accessing the Ivanti Endpoint Security console using a Web browser with high security settings enabled, the following message may display:

```
Scripting must be enabled to display this application properly.
```

In this event, Ivanti recommends adding the Ivanti Endpoint Security Web address as a trusted site in your browser settings to view the Web console.

1. Open your Web browser.
2. In your browser's address bar, type the Ivanti Endpoint Security URL (http[s]://*ServerURL*) and press ENTER.

   Tip: You can also use the server IP address.

   Step Result: A dialog prompting you for credentials opens.
3. Type your user name in the **User name** field.

   When logging in for the first time, type the user name of the Windows user account used to install Ivanti Endpoint Security. You can use additional user names after adding new user profiles to Ivanti Endpoint Security. If logging in using a domain account, type the name in the following format: `DOMAIN\Username`.
4. Type your password in the **Password** field.
5. Click **OK**.

Installing the Patch and Remediation Module Server Component

After logging in to Ivanti Endpoint Security, the first step in implementing Patch and Remediation features and functions is to install the server module

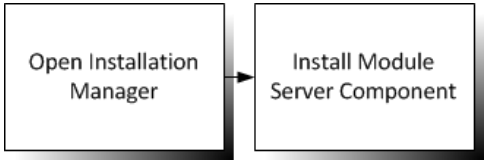


Figure 1: Install Server Module

Install the server module using ***Installation Manager***.

1. Select **Tools** > **Launch Installation Manager**.

   Step Result: Installation Manager opens to the ***New/Update Components*** tab.

2. Select the **Ivanti Patch and Remediation** check box for your version number of Ivanti Endpoint Security.
3. Click **Install**.

   Step Result: The ***Install/Update Components*** dialog opens.
4. Click **Next** to dismiss the **Database backup recommended** notification. Ivanti recommends backing up your database before installing a module.
5. Click **Install**.

   Step Result: A dialog opens, notifying you that installing the module may cause logged in user to lost their work.
6. Click **OK**.

   Step Result: The installation begins.
7. Click **Finish**.

Tip: Select the **Launch Ivanti Endpoint Security** check box to relaunch Ivanti Endpoint Security after clicking **Finish**.

Result: The Patch and Remediation server module is installed.

After Completing This Task:
Continue to Installing the Patch and Remediation Module for Endpoints on page 20.

Installing the Patch and Remediation Module for Endpoints

After installing the Patch and Remediation server module, you must install the Patch and Remediation module for your network endpoints.

Prerequisites:

Complete Installing the Patch and Remediation Module Server Component on page 19.

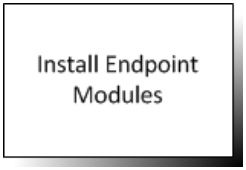


Figure 2: Install Endpoint Module

Install the endpoint component from the ***Endpoints*** page.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the ***All*** tab.

2. From the list, select the endpoints that you want to install the Patch and Remediation endpoint module on.
3. Click **Manage Modules**

   Step Result: The ***Add/Remove Modules*** dialog opens.
4. Select the **Patch** check box for all endpoints you want to install the component on.
5. Click **OK**.

Result: The Patch and Remediation endpoint module is installed on selected endpoints.

After Completing This Task:
Continue to Creating New Groups on page 21.

Creating New Groups

After installing the Patch and Remediation components, create a new group for your Patch and Remediation endpoints. By placing your Patch and Remediation endpoints in a group (or multiple groups), you can manage them collectively. For example, you deploy content to all Patch and Remediation with one deployment by using groups.

Prerequisites:

Complete Installing the Patch and Remediation Module for Endpoints on page 20.

Figure 3: Group Diagram

Create and configure groups from the ***Groups*** page.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **Browser** tree, select **Custom Groups**.

   Groups are arranged within a tree structure. You can place your new group anywhere within the custom group hierarchy.

   Note: The group you create is added as a child group to the group selected within the directory tree.
3. Create a group.
   a) From the **View** list, select **Group Membership**.
   b) Click **Create**.
   c) In the **Name** field that displays, type a group name.
   d) In the **Description** field that displays, type a description.
   e) Click the **Save** icon.
4. Add endpoints to the group.
   a) From the **View** list, select **Endpoint Membership**.
   b) Click **Manage**.

c) Assign endpoints to the group.
For more detailed information, refer to Adding Endpoints to a Group on page 342.
d) Click **OK**.

5. Define the group's settings.
Group settings contain additional group controls.
a) From the **View** list, select **Settings**.
b) Define the settings.
For more detailed information, refer to Editing Group Settings on page 409.
c) Click **Save**.

Result: The group is created.

After Completing This Task:
Continue to Apply Agent Policy Sets on page 22.

Apply Agent Policy Sets

After you create a group, create and assign an agent policy set to govern the group endpoint behavior. Agent policy sets can control endpoint communications, hours or operations, and so on.

Prerequisites:

Complete Creating New Groups on page 21.

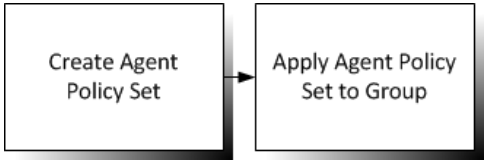


Figure 4: Install Server Module

Create agent policy sets using the ***Agent Policy Sets*** page, and then assign them to a group using the ***Groups page.***

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Click **Create** to create an agent policy set.
For additional information, refer to Creating an Agent Policy Set on page 430.
3. Select **Manage** > **Groups**.
Step Result: The ***Groups*** page opens.
4. From the **View** list, select **Agent Policy Sets**.
Step Result: The ***Agent Policy Sets*** view opens.
5. From the **Browser** tree, select the group you created.

6. Click **Assign** to assign the agent policy set to your created group.
   For additional information, refer to Assigning an Agent Policy Set to a Group on page 385.

Result: The agent policy set is created and assigned.

After Completing This Task:
Continue to Viewing and Remediating Vulnerabilities on page 23.

Viewing and Remediating Vulnerabilities

After installing the Patch and Remediation module server and endpoint components, your network endpoints complete their first Discover Applicable Updates task, which detect vulnerabilities. Following this task, you can then view vulnerabilities in your network and then deploy patches and other content to resolve them.

Prerequisites:

Complete Apply Agent Policy Sets on page 22.

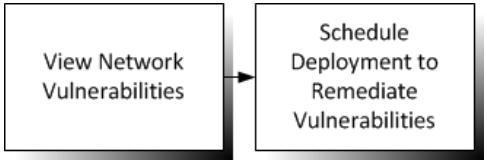


Figure 5: Viewing and Remediating Vulnerabilities

1. View dashboard widgets, vulnerabilities, and reports to identify vulnerabilities in your network.
   Dashboard widgets and reports provide detailed graphs and statistics about the state of your network. Reviewing this information provides insight about the actions required to secure your network. For additional information, refer to the following documentation:
   - To see an overview of how many vulnerabilities are in your network, view *The Dashboard*. View the dashboard by click **Home** from the navigation menu.
   - To view the vulnerabilities on a specific endpoint, view *The Endpoint Details Page*. View the ***Endpoint Details*** page by selecting **Manage** > **Endpoints** and clicking an endpoint link.
   - To view the specific vulnerabilities in your network, view *The Content Pages List*. To view this page, select **Manage** > **Vulnerabilities**.
   - To view a report of vulnerabilities in your network, view *Generating a Report*. To generate reports, select **Reports** > **All Reports**, select a report, and click **Generate Report**.
2. From the **Navigation Menu**, select **Review** > **Vulnerabilities** > **--- All ---** (or any of the other vulnerability options).
3. From the list, select the vulnerabilities you want to deploy.

Tip: Use the page filters to find vulnerabilities applicable to your endpoints.

4. Click **Deploy** to remediate vulnerabilities.

   Remediate network vulnerabilities by deploying content that fix identified vulnerabilities. For additional information, refer to .

Result: The deployment is scheduled and will begin at the scheduled time. Completion time of the deployment varies dependent on size.

After Completing This Task:
Continue to Adding Content to a Mandatory Baseline on page 24.

Adding Content to a Mandatory Baseline

Each group in Ivanti Endpoint Security has a Mandatory Baseline, which is a list of content that must be installed on the group's endpoints at all time. By default, this baseline is empty. However, you can add patches, software, and other content to this baseline. After adding content to the baseline, Ivanti Endpoint Security continually checks groups endpoints for the content's presence. If a group endpoint is found to not have content included in the Mandatory Baseline, Ivanti Endpoint Security automatically deploys that content to the endpoint.

Prerequisites:

Complete Editing Email Notifications on page 25.

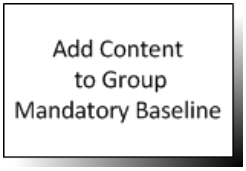


Figure 6: Adding Content to Mandatory Baselines

Add content to a Mandatory Baseline from the ***Groups*** page.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **Browser** tree, select the group you created earlier.
3. From the **View** list, select **Mandatory Baseline**.
4. Click **Manage** to add content.

   For additional information, refer to Adding Content to Mandatory Baselines on page 357.
5. Click **OK**.

Result: Content is added to the group Mandatory Baseline.

After Completing This Task:
Continue to Defining Default Deployment Options on page 25.

Defining Default Deployment Options

After you install Patch and Remediation, a ***Deployments*** tab is added to the ***Options*** page. Configure this tab to define the default values for the ***Deployments Wizard***.

Prerequisites:

Complete Adding Content to a Mandatory Baseline on page 24.

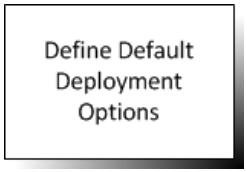


Figure 7: Define Default Deployment Options

Define default deployment options from the ***Options*** page.

1. From the **Navigation Menu**, select **Tools** > **Options**.
2. Select **Tools** > **Options**.
3. Select the ***Deployments*** tab.
4. Define the default deployment options.
   For additional information, refer to Configuring the Deployments Tab on page 91.
5. Click **Save**.

Result: The default deployment options are defined.

After Completing This Task:
Continue to Editing Email Notifications on page 25.

Editing Email Notifications

After installing Patch and Remediation, two new email notification types are added: New Vulnerabilities and Deployment Failure. To use these new notifications, edit your defined email addresses or create new ones.

Prerequisites:

Complete Defining Default Deployment Options on page 25.

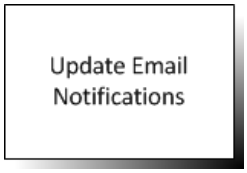


Figure 8: Edit Email Notifications

Edit email notifications from the ***Email Notifications*** page.

1. From the **Navigation Menu**, select **Tools** > **Email Notifications**.
2. For each defined email address, select one or both of the following new notification types available after installation of Patch and Remediation.

Tip: For more information on how to define a new address and email notifications, refer to Creating Email Notifications on page 112.

Notification Type	Description
New Vulnerabilities	Sends the defined address a notification email when new vulnerabilities are available.
Deployment Failure	Sends the defined address a notification email when a scheduled deployment fails.

Tip: Additional options are available for the Ivanti Endpoint Security core features and other modules.

3. Click **Save**.
4. Click **OK**.

Result: The email addresses you edited are configured to receive the new email notifications.

After Completing This Task:
Continue to Editing Custom Roles on page 26.

Editing Custom Roles

After installing Patch and Remediation, new access rights are added for new features. To update custom roles for these features, edit your roles.

Prerequisites:

Complete Editing Email Notifications on page 25.

Edit custom roles from the ***Users and Roles*** page.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. From the page list, click the edit icon for the custom role to which you want to add access rights.

   Step Result: The ***Edit Role*** dialog opens.
4. Select the ***Access Rights*** tab.

5. Define the new Patch and Remediation access rights.

Dashboard Access Rights	Description
View PR Widgets	Access to select and view the Patch and Remediation Dashboard widgets.

Vulnerabilities/Patch Content Access Rights	Description
View Content	Access the vulnerability and other content data.
Manage Content	Enable and disable vulnerabilities and other content.
Export Content	Export vulnerability and other content data list.
View Content Details	Access the detailed information for vulnerabilities and other content.

Endpoint Access Rights	Description
View PR Tab	Access the Patch and Remediation tab.
Manage PR Tab	Install, uninstall, enable, and disable the Patch and Remediation module.
Export PR Tab	Export the Patch and Remediation tab endpoint list.
Scan Now Discover Applicable Updates	Scan endpoints using the DAU Scan Now Dropdown button.
Reboot Endpoints	Reboot endpoints using the **Reboot Now** button.

Inventory Access Rights	Description
View Inventory	View the endpoint inventory.
Export Inventory	Export the endpoint inventory list.

Deployments and Tasks Access Rights	Description
Create Deployments	Ability to create new deployments.
View My Deployments and Tasks	Access the deployments and tasks that this user has created.
View All Deployments	Access the deployments that all users have created.

Deployments and Tasks Access Rights	Description
Manage Deployments and Tasks	Deploy, enable, disable, abort, and delete deployments and tasks that the user has access to.
Export Deployments and Tasks	Export the deployments and tasks in the list that this user has access to.

Packages Access Rights	Description
View Packages	Access the package data.
Manage Packages	Create, edit, and delete packages.
Export Packages	Export the package data list.
Cache Packages	Ability to download packages from the Global Subscription Service onto the Ivanti Endpoint Security server.

Email Notifications Access Rights	Description
Manage PR Email Notifications	Create and edit Patch and Remediation notifications.

6. Click **OK**.

Chapter 3

Using the Ivanti Endpoint Security Console

In this chapter:

Within the Ivanti Endpoint Security console, you can use a number of common functions to navigate and operate the system. After you log in, Ivanti Endpoint Security opens to the ***Home Page***.

Ivanti Endpoint Security performs the following functions:

- Endpoint Detection
- Agent Installation
- Endpoint Management
- Endpoint Grouping
- Agent Policy Set Creation
- User and Role Creation and Management
- Server Module Management
- Report Generation

Ivanti Endpoint Security consists of a browser-based management console, which provides access to system management, configuration, reporting, and deployment options.

Common Functions

Ivanti Endpoint Security uses standard Web browser conventions and unique conventions. Familiarize yourself with these conventions to facilitate efficient product use.

From the **Navigation Menu** and system pages, you can access all features and functions you are authorized for.

Common Conventions

The Web console supports user interface conventions common to most Web applications.

Table 1: Common User Interface Conventions

Screen Feature	Function
Entry Fields	Depending on text, type data into these fields to either: • Retrieve matching criteria • Enter new information
Drop-Down Menus	Display a list of selectable values when clicked.
Command Buttons	Perform specific actions when clicked.
Check Boxes	A check box is selected or cleared to: • Enable or disable a feature • Initiate functions for list items Some lists include a **Select All** check box for selecting all items, including overflow items.
Radio Buttons	Select the button to select an item.
Sort	Data presented in tables can be sorted by clicking column headers. Columns can be sort in the following orders: • Ascending (default) • Descending
Mouseovers	Move your mouse over an item to display a text description.
Auto Refresh	Some pages feature an **Auto Refresh** check box. Select the check box to automatically refresh the page every 15 seconds.
Scrollbars	Drag scrollbars to see additional data.
Tabs	Select different tabs to display hidden information.
Bread Crumb	Displays the path to the page you are viewing. The breadcrumb lists: • The page you are viewing • Its parent page (if applicable) • The **Navigation Menu** item used to open the page If the breadcrumb contains a link, you can click it to retrace your steps.

Tip: Most pages support right-click.

The Navigation Menu

This menu appears on all Ivanti Endpoint Security pages. Use this menu to navigate through the console.

This menu organizes product features based on functionality. When you select a menu item, a new page, dialog, wizard, or window opens. You can access all system features from this menu (that your access rights authorize).

Note: The menu items available change based on modules you install.

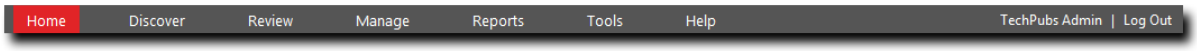


Figure 9: Navigation Menu

Table 2: Navigation Menus

Menu	Description
Home	Opens the ***Home*** page. This link contains no menu items.
Discover	Contains menu items related to running discovery scan jobs and virus and malware scans.
Review	Contains menu items related to reviewing security content, application event logs, virus and malware events, and discovery scan jobs.
Manage	Contains menu items related to managing system features.
Reports	Contains menu items related to creating reports.
Tools	Contains menu items related to system administration.
Help	Contains menu items related to help systems.

Mobile Device Management adds new **Navigation Menu** items.

Most navigation menus contain items. The following table lists each menu item in the **Discover** menu and the actions that occur when they are selected.

Table 3: Discover Menu Items

Menu Item	Description
Assets...	The ***Discover Assets*** dialog.
Assets and Install Agents...	The ***Install Agents*** dialog.
Assets and Uninstall Agents...	The ***Uninstall Agents*** dialog.

Menu Item	Description
Scan Now - Virus and Malware Scan	The ***Virus and Malware Scan*** dialog.

The following table lists each menu item in the **Review** menu and the actions that occur when they are selected.

Table 4: Review Menu Items

Menu Item	Description	
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.	
	Create Custom Patch List	The ***Create Custom Patch List*** dialog.
	Custom Patch List	The **Custom Patch Lists** sub-menu lists the last five custom patch lists that you have edited.
	All Lists	If you have created more than five custom patch lists, the navigation menu lists an **All Lists** item, which will open the ***Patch Content*** page with all custom patch lists displayed.
My Default View	The ***All Content*** page with your saved filters.	
Vulnerabilities	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show only critical vulnerabilities.
	Critical Vulnerabilities	The ***Patch Content*** page, filtered to show only critical vulnerabilities that are not superseded.
	New Vulnerabilities	The ***Patch Content*** page, filtered to show only critical but not superseded vulnerabilities released in the last 30 days.
	Top Vulnerabilities	The ***Patch Content*** page, filtered to show only critical but not superseded vulnerabilities sorted by the greatest number of applicable endpoints that are not patched.

Menu Item	Description	
Software	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show all software.
	Service Packs	The ***Patch Content*** page, filtered to show only service packs.
	Software Installers	The ***Patch Content*** page, filtered to show only software installers.
	Updates	The ***Patch Content*** page, filtered to show only software updates.
Other	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show all non-critical content.
	Detection Only	The ***Patch Content*** page, filtered to display **Detection Only** content.
	Informational	The ***Patch Content*** page, filtered to display only **Information** content.
	Packages	The ***Patch Content*** page, filtered to display only **Packages** content.
	Policies	The ***Patch Content*** page, filtered to display only **Policies** content.
	Recommended	The ***Patch Content*** page, filtered to display only **Recommended** content.
	System Management	The ***Patch Content*** page, filtered to display only **System Management** content.
	Tasks	The ***Patch Content*** page, filtered to display only **Task** content.
	Virus Removal	The ***Patch Content*** page, filtered to display only **Virus Removal** content.
Asset Discovery Job Results	Opens the ***Job Results*** page, which is filtered to display discovery job results.	
Agent Management Job Results	Opens the ***Job Results*** page, which is filtered to display Agent Management Job results.	

Menu Item	Description
Virus and Malware Event Alerts	Opens the ***Virus and Malware Event Alerts*** page.
Application Control Log Queries	Opens the ***Application Control Log Queries*** page, which allows users to create log queries that extract information on application activity.
Device Event Log Queries (Device Control only)	Opens the ***Device Event Log Queries*** page, which you can use to create, edit, or review device event log queries.

The following table lists each menu item in the **Manage** menu and the actions that occur when they are selected.

Table 5: Manage Menu Items

Menu Item	Description	
Endpoints	Opens the ***Endpoints*** page.	
Mobile Endpoints	Opens the ***Mobile Endpoints*** page.	
Inventory	Opens the ***Inventory*** page.	
Groups	Opens the ***Groups*** page.	
Users	Opens the ***Users*** page.	
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.	
	Create Custom Patch List	The ***Create Custom Patch List*** dialog.
	Custom Patch List	The **Custom Patch Lists** sub-menu lists the last five custom patch lists that you have edited.
	All Lists	If you have created more than five custom patch lists, the navigation menu lists an **All Lists** item, which will open the ***Patch Content*** page with all custom patch lists displayed.
Deployments and Tasks	Opens the ***Deployments and Tasks*** page.	
Agent Policy Sets	Opens the ***Agent Policy Sets*** page.	
Mobile Policies	Opens the ***Mobile Policies*** page.	
Antivirus Policies	Opens the ***Antivirus Policies*** page.	

Menu Item	Description	
Application Control Policies	Opens the ***Application Control Policies*** page, which contains the following tabs:	
	Managed Policies	Managed policies include Easy Auditor, Easy Lockdown, Denied Applications Policy, and Supplemental Easy Lockdown/ Auditor Policy. This tab is selected by default.
	Trusted Change	Trusted change policies include Trusted Publisher, Trusted Path, Trusted Updater, and Local Authorization.
	Memory Injection Policies	Memory Injection Policies.
Device Control: Policies (Device Control only)	Opens the ***Device Control Policies*** page, which you use to create, edit, or review Device Control policies.	
Policy Wizards	Opens a sub-menu. The sub-menu contains the following items:	
	Easy Auditor...	The ***Easy Auditor*** wizard.
	Easy Lockdown...	The ***Easy Lockdown*** wizard.
Application Library (Application Control only)	Opens the ***Application Library*** page, which lists the applications and files on your network endpoints.	
Device Library (Device Control only)	Opens the ***Device Library*** page, which lists all devices on your network endpoints.	

The following table lists each menu item in the **Reports** menu and the actions that occur when they are selected.

Table 6: Reports Menu Items

Menu Item	Description
All Reports	Opens the ***All Reports*** page.
AntiVirus	Opens the ***All Reports*** page with antivirus reports expanded.
Configuration	Opens the ***All Reports*** page with configuration reports expanded.
Deployments	Opens the ***All Reports*** page with deployments reports expanded.

Menu Item	Description
Device Control (Device Control only)	Opens the ***All Reports*** page with Device Control reports expanded.
Inventory	Opens the ***All Reports*** page with inventory reports expanded.
Management/Status	Opens the ***All Reports*** page with management/status reports expanded.
Policy and Compliance	Opens the ***All Reports*** page with policy and compliance reports expanded.
Power Management (Power Management only)	Opens the ***All Reports*** page with Power Management reports expanded.
Risks	Opens the ***All Reports*** page with risks reports expanded.
Vulnerabilities/Patch Content	Opens the ***All Reports*** page with vulnerabilities/patch content reports expanded.
Enhanced Reports	Opens a custom, user-defined URL. This URL is usually used to open a third-party reporting Web page.

The following table lists each menu item in the **Tools** menu and the actions that occur when they are selected.

Table 7: Tools Menu Items

Menu Item	Description
Users and Roles	Opens the ***Users and Roles*** page.
Change My Password...	Opens the ***Change My Password*** dialog.
Download Agent Installer...	Opens the ***Download Agent Installer*** dialog opens over the currently selected page.
Wake on LAN	Opens the ***Wake on LAN*** page.
Power Management (Power Management only)	Opens the ***Power Management*** page.
Directory Sync Schedule	Opens the ***Directory Sync Schedule*** page.

Menu Item	Description	
Device Control Device Control only)	Opens the **Device Control** submenu. The submenu includes the following items:	
	Recover Password	Opens the ***Recover Password*** dialog, which you can use to help network users recover forgotten passwords for encrypted devices.
	Grant Temporary Permissions	Opens the ***Grant Temporary Permissions*** dialog, which you can use to extend network users temporary access to certain network devices.
Launch Installation Manager...	Opens the ***Installation Manager*** in a new window.	
Subscription Updates	Opens the ***Subscription Updates*** page.	
Mobile Management Setup	Opens the ***Mobile Management Setup*** page.	
Mobile Endpoint Registration	Opens the ***Mobile Endpoint Registration*** dialog.	
Email Notifications	Opens the ***Email Notifications*** page.	
Options	Opens the ***Options*** page.	

The following table lists each menu item in the **Help** menu and the actions that occur when they are selected.

Table 8: Help Menu Items

Menu Item	Description
Help Topics...	Opens the ***Help*** page.
Knowledge Base...	Opens the Ivanti knowledge base.
New Users Start Here...	Opens the ***New Users Start Here*** page.
Technical Support	Opens the ***Technical Support*** page.
Product Licensing	Opens the ***Product Licensing*** page.

Menu Item	Description
About...	Opens the ***About*** dialog.

Note: Any unavailable or absent menus, menu items, or sub-menu items are due to restricted access rights or unavailable modules. Contact your network administrator if you require access to unavailable features.

The Page Banner

A page banner displays when the page is added for a new module. Use this banner to identify the module that the page belongs to.

Figure 10: Page Banner

For example, pages for Ivanti Patch and Remediation display a Patch and Remediation page banner. Page banners are color-coded by module.

List Pages

Most pages feature lists of selectable items. These items represent different product features that can be edited using menus and buttons.

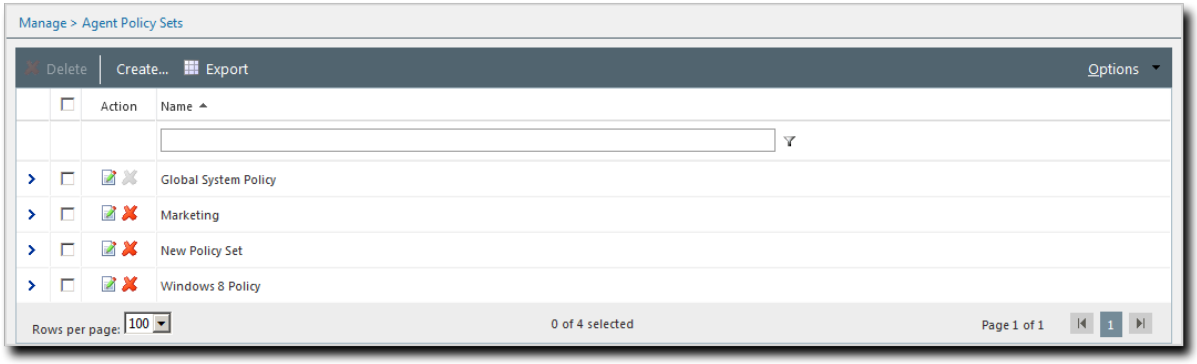


Figure 11: List Page

To select a single list item:

- Select a check box.
- Click a list row.

To select multiple list items:

- Select the **Select All** check box.
- Select multiple, concurrent items by using `SHIFT+Click` and mousing over list rows.

Toolbars

Toolbars appear on most Web console pages. They contain menus and buttons you can use to initiate page features.

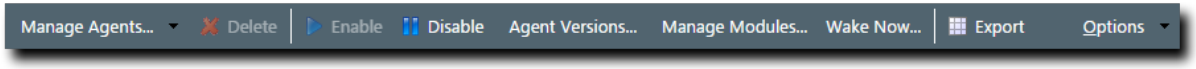


Figure 12: Toolbar

- The menus and buttons displayed vary according to page.
- Click the available menus and buttons to use them.
- User roles determine which buttons are available.

The Options Menu

Toolbars feature an **Options** menu. You can use these options to change how the page displays information.

Table 9: Options Menu Items

Option	Description
Show results on page load	Toggles automatic page results on and off. • When enabled, the page list automatically populates with results. • When disabled, you must define page filters and click **Update View** before results populate. For more information, see Filters on page 40.
Save as default view	Saves the current page settings as the default view.
Clear default view	Resets the saved view to the system default.
Show Filter Row[1]	Toggles the **Filter Row** on and off. For additional information, refer to Using Filter Rows on page 42
Show Group By Row[2]	Toggles the **Show Group By Row** on and off. For additional information, refer to Group By on page 44.
Enable Copy to Clipboard[3]	Toggles the ability to select text for clipboard copy.

1. This option title changes to **Hide Filter Row** when toggled.
2. This option title changes to **Hide Group By Row** when toggled.
3. Selecting this option disables other features, such as right-click context menus and list item dragging.

Filters

Filters appear on most list pages. You can use them to search pages for specific data.

Depending on which page you are viewing, you can filter pages using one of the following features. Only one feature appears per page.

- Filters
- Filter Row

Filters appear above page lists. They feature different fields, lists, and check boxes used for filtering. Filters vary according to page.

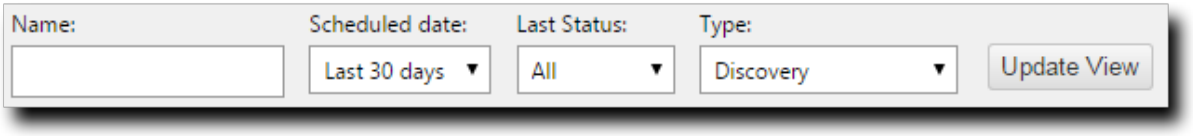


Figure 13: Filters

You can save frequently used filter settings as your default view. To save your settings, select **Options** > **Save as default view** from the toolbar. The toolbar **Options** menu contains the following options for filtering.

Table 10: Filter Options

Option	Function
Show results on page load	Automatically retrieves and displays results when selected.

Save as default view	Saves the active filter and sort criteria as the default view for the page.
	• The default view displays each time the page is accessed, including the following events:
	  • Browsing to a different page.
	  • Logging out of the Web console.
	• The default view is saved until you save a new one or you clear it.

Clear default view	Resets a saved default view to the system default view.

Filter Rows

Filter rows appear in the lists themselves. Rows feature a field for each column.

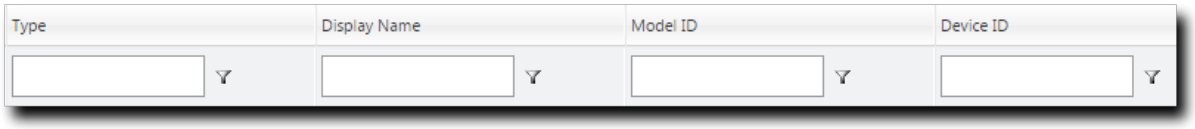


Figure 14: Filter Row

- Filters are not case sensitive.
- Columns can be filtered using a variety of data types. For example, you can use a **Contains** filter or a **StartsWith** filter.
- Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.

Supported Wildcards
When searching for or filtering vulnerabilities, you can use wildcards to make search results more specific and efficient.

Wildcards can be used anywhere within the search string. The following table lists the supported operators and wildcards in Ivanti Endpoint Security. Type any wildcards that you intend to use in the **Name or CVE-ID** field.

Table 11: Supported Wildcards

Wildcard	Description	Example
%	Any string. The string can be empty or contain any number of characters.	Typing `Microsoft%Server` in the **Name or CVE-ID** field returns any vulnerability with the words *Microsoft* and *Server* in any part of the name, such as: • MS12-043 Security Update for **Microsoft** Office SharePoint **Server** 2007 32-Bit Edition (KB2687497) • The 2007 **Microsoft** Office **Server**s Service Pack 3 (SP3), 32-bit Edition (KB2526299)
_ (underscore)	An underscore can be used as a Wildcard placeholder for any single character.	Typing `_itrix` or `Citri_` in the **Name or CVE-ID** field returns any vulnerabilities with *Citrix* in the name.
[ ]	Any single character within the brackets. You can also type a range ([a-f]) or set ([acegik]).	Typing `[m]ic` in the **Name or CVE-ID** field returns vulnerabilities with the string *mic* within the name (*Microsoft* and *Dynamic*). Typing `200[78]` in the **Name or CVE-ID** field returns vulnerabilities with 2007 or 2008 within the name.

Wildcard	Description	Example
[^]	Any single character **not** specified within the brackets. You can also type a range ([^a-f]) or set ([^acegik]).	Typing `M[^i]cro` in the **Name or CVE-ID** field returns results that: • Replace *i* with all remaining alphanumeric and symbolic characters (a, $, and so on). • Include all other characters remaining in the string (m, c, r, o). Results would include Macro, Mecro, M$cro, and so on. If a vulnerability contains Micro and a valid combination like Macro in its name (e.g. `MS99-999 Microsoft Word 2010 Vulnerability Could Enable Macros to Run Automatically`), it will be returned in the results.

Using Filters
When list pages are overpopulated with items, use filters to search for specific list items. Use this feature to filter list pages by criteria specific to the page.

Filters are available on most list pages.

1. Select a list page. For additional information, refer to List Pages on page 38.
2. Ensure filters are displayed.
   If filters are not displayed, click **Show Filters**.
3. Define filter criteria.

   Note: Available filters differ by page.

   - In filter fields, type the desired criteria.
   - From filter lists, select the desired list item.
4. If applicable, select the **Include sub-groups** check box.

   Note: This check box only appears on list pages related to groups.
5. Click **Update View**.

   Step Result: The list is filtered according to the filter criteria.
6. [Optional] Save the filter criteria by selecting **Options** > **Save as default view** from the toolbar.

Using Filter Rows
Some list pages use filter rows rather than filters. Use these rows, which are the first row of applicable lists, to filter column results. Filter column results to search for specific list items.

These rows appear on several list pages.

1. Select a page featuring the filter row.
2. Ensure the filter row is displayed.
   a) If the filter row is not displayed, select **Options** > **Show Filter Row** from the toolbar.
3. Type criteria in a filter row field.
4. Apply a filter type.
   a) Click the **Filter** icon.

      Step Result: A menu opens.

   b) Select a filter type.

      The following table describes each filter type.

      Table 12: Data Filtering Types

Type	Description
NoFilter	Removes previously applied filtering.
Contains	Returns results that contain the value applied to the filter.
DoesNotContain	Returns results that do not contain the value applied to the filter.
StartsWith	Returns results that start with the value applied to the filter.
EndsWith	Returns results that end with the value applied to the filter
EqualTo	Returns results equal to the value applied to the filter.
NotEqualTo	Returns results that are not equal to the value applied to the filter.
Greater Than	Returns results that are greater than the value applied to the filter.
Less Than	Returns results that are less than the value applied to the filter.
GreaterThanOrEqualTo	Returns results that are greater than or equal to the value applied to the filter.
LessThanOrEqualTo	Returns results that are less than or equal to the value applied to the filter.
Between	Returns results that are between two values. Place a space between the two values.
NotBetween	Returns results that are not between two values. Place a space between the values.
IsEmpty	Returns results that are empty.
NotIsEmpty	Returns results that are not empty.
IsNull	Returns results that have no value.

Type	Description
NotIsNull	Returns results that have a value.

Note:

- Filters are not case sensitive.
- Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.
- The availability of filtering options depends on the type of data displayed in the column. For example, filtering options that can only apply to numeric data are available in columns that contain text data.

Result: The list column is filtered according to the criteria. If desired, repeat the process to filter additional columns.

Using a Custom Date Range Filter

Use the Custom Date Range filter on Virus and Malware Event pages and tabs to display events that have occurred over a specific time period.

Prerequisites:

You must have launched the **Custom Date Range** dialog from the **Last Date Detected** filter field of a Virus and Malware Event page or tab.

1. Enter Start and End dates and times that cover the period you want to view alerts for, then click **OK**.

   Calendar and Time View popups can be opened to facilitate the entry of dates and times. Times that can be selected are provided in 30-minute intervals.

   Note: Your Start date should be less than 90 days from the current date, as event alerts raised outside that range are removed from view.

2. Click **Update View** to display the filtered results.

Result: The list is filtered according to the custom date range criteria you entered. Last Detected Dates are always displayed using server time.

Tip: As Malware and Virus Event alerts can be removed from view, the results list may not display all alerts that occurred within your custom date range. However, removed alerts are not deleted from the database and can therefore be viewed by generating an appropriate report.

Group By

The **Group By** row lets you sort list items into groups based on column headers. Use this feature to see which list items share similarities.

To use the **Group By** row, ensure **Options** > **Show Group By Row** is selected from the toolbar, and then drag a column header into the row. You may drag multiple columns to the row, but you may only drag one column into the row at a time.

To ungroup the list, right-click on the row and select **Cancel All Groupings**. To hide the **Group By** row, select **Options** > **Hide Group By Row**.

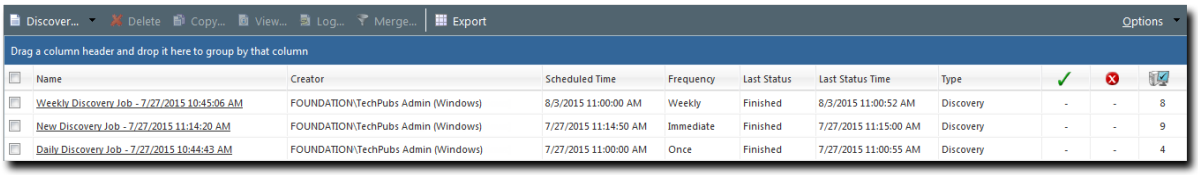


Figure 15: Group By Row

Expanding and Collapsing Structures

Certain structures in the Web console are expandable and collapsible. Expand structures to view additional information or options. Collapse them to conserve screen space.

Click available **Plus** icons (+), **Minus** icons (-), and **Rotating Chevron** icons (>) to expand or collapse a structure.

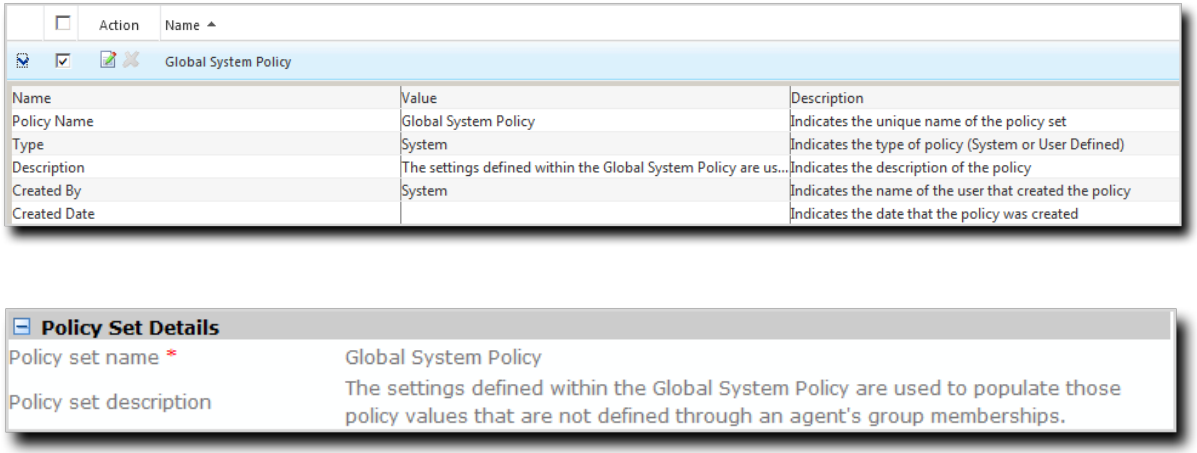


Figure 16: Expandable Structure Examples

Advancing Through Pages

When a list page contains an overflow of items, pagination links are created to manage the overflow. Click these links to advance through list items.

The number of list items and the page you are viewing determines the number of pagination links.

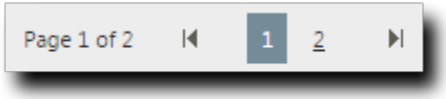


Figure 17: Pagination Feature

Table 13: Pagination Feature Functions

Icon or Link	Title	Function
	**Final Page Link**	Advances to the final page of list items.
	**First Page Link**	Returns to the first page of list items.
...	**Next Ten/Previous Ten Pages Link**	Displays the next ten or previous ten page links available. Fewer page links will display if the remaining list items cannot populate ten pages.
1 2 3 4 5	**Pagination Links**	Advances or returns to the selected pagination link.

Each page also features a **Rows Per Page Drop-Down List**. This list modifies the number of list items displayed on a single page (25, 50, 100, 200, 500).

Help

Ivanti Endpoint Security contains context-sensitive HTML help that includes feature explanations, step-by-step procedures, and reference materials.

Accessing Help differs according to context.

- From a page, select **Help** > **Help Topics**.
- From a dialog, click the **Question Mark** icon (**?**).

Use the following features to navigate through Help:

- From the ***Content*** tab, expand the bookmarks and click links to display Help topics.
- From the ***Search*** tab, type criteria in the **Keywords** field and click **Search** to display Help topics related to your search.

Exporting Data

On many system pages, you can export the listed data to a comma-separated value file (`.csv`) available for use outside of the Web console. Use this exported data for management purposes (reporting, noting trends, and so on).

You can export data from a variety of pages.

Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

1. Open a system page or dialog that you can export information from.
2. [Optional] Use the page filters to refine the items listed.
3. Click **Export**.

   Step Result: The ***File Download*** dialog opens.
4. Use the browser controls to complete the data export.

Result: The data is exported. All data results export, including data on overflow pages.

The Home Page

The entry point to Ivanti Endpoint Security is the ***Home Page***. From this page you can view the dashboard, which features drag-gable widgets that display information about Ivanti Endpoint Security and agent-managed endpoints.

Some widgets display general information about the system, others provide links to documentation, and still others summarize activity for Ivanti Endpoint Security modules you are licensed for.

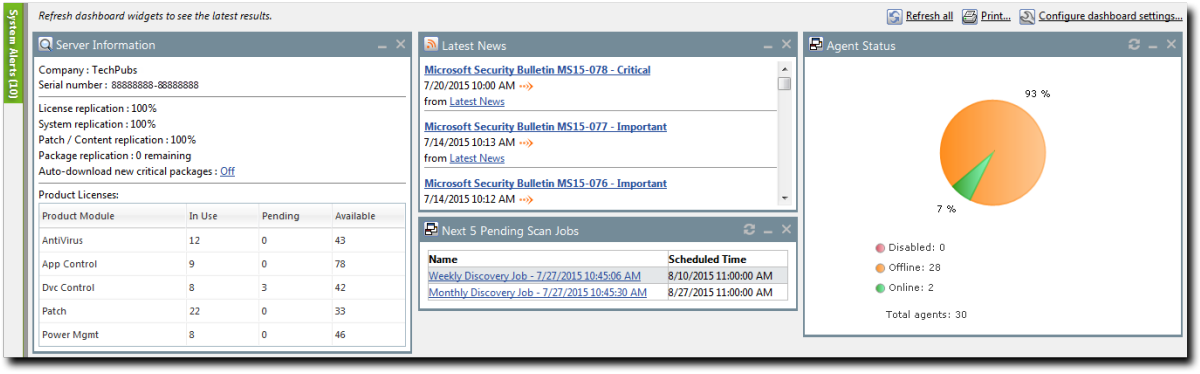


Figure 18: The Home Page

The Dashboard

The **dashboard** displays widgets depicting the activity on your protected network. Located on the ***Home*** page, the dashboard provides convenient information you can use to ensure your network protection is up to standard. Additionally, you can customize the dashboard to display the widgets most applicable to your network environment.

Widget graphs are generated based on the latest data and statistics available from endpoints, groups, module-specific data, and so on.

The following ***Dashboard*** widgets are available:

The Agent Module Installation Status Widget

This widget displays the installation and licensing stats of each agent module.

A graph bar displays for each installed module. The following table describes the widget graph.

Table 14: Graph Bar Color Descriptions

Bar Color	Description
Blue	The number of endpoints with the module pending install or uninstall.
Green	The number of endpoints with the module installed.
Red	The number of endpoints without the module installed.

Tip: Click the graph to open the ***Endpoints*** page.

Note: Endpoints with an agent version that does not support a module are not counted.

The Agent Status Widget

This widget displays all agents grouped by agent status.

Table 15: Agent Status Widget Fields

Field	Description
Online	The number of agents that are online.
Offline	The number of agents that are offline. **Tip:** Offline status is determined by the amount of time since the agent last communicated as determined on the ***Options*** page.
Disabled	The number of agents that are disabled.
Total Agents	The total number of agents in your environment.

Tip: Click the graph to open the ***Endpoints*** page. The page is filtered to display all agents.

The Applicable Content Updates Widget

This widget displays applicable content updates grouped by content type. View this widget when determining what content is applicable to endpoints in your network.

Table 16: Applicable Content Updates Widget Graph Bars

Bar	Description
Critical	The number of critical content items that are applicable to the your endpoints.

Bar	Description
Recommended	The number of recommended content items that are applicable to your endpoints.
Optional	The number of optional software, informational, and virus removal content items that are applicable to your endpoints.

Tip: Click the widget graph to open the ***Content*** page, which is filtered to display all applicable non-patched content.

Table 17: Applicable Content Updates Widget Fields

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.
Endpoints	The total number of endpoints with applicable updates.

Note:

- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.
- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Critical Patch Status by Endpoint Widget
This widget depicts the patch status of all managed endpoints. Each bar indicates the number of managed endpoints with applicable vulnerabilities within a given release date range.

The following table describes the **Critical Patch Status By Endpoint** widget. Green bars indicate endpoints that are patched for critical vulnerabilities, while red bars indicate endpoints that are not patched for critical vulnerabilities.

Table 19: Critical Patch Status By Endpoint Bars

Graph Bar	Description
<30 days	The number of endpoints with applicable critical vulnerabilities fewer than 30 days old.
30 - 120 days	The number of endpoints with applicable critical vulnerabilities between 30 to 120 days old.
>120 days	The number of endpoints with applicable critical vulnerabilities greater than 120 days old.

The following table describes the widget fields.

Table 20: Critical Patch Status By Endpoint Fields

Field	Description
Endpoints	The total number of endpoints with applicable critical vulnerabilities.
Critical vulnerabilities	The total number of critical vulnerabilities applicable to your environment.

Tip: Click the graph to open the ***Critical Vulnerabilities*** content page.

Note:

- If an endpoint is marked as *Do Not Patch* for a critical vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved critical vulnerabilities.
- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the **Critical vulnerabilities** count.

The Discovery Scan Results: Agents Widget
This widget displays the number of endpoints capable of hosting agents discovered in the latest Discovery Scan Job. The endpoints are classified in to two groups: endpoints with agents and endpoints without agents.

Table 21: Discovery Scan Results: Agents Widget Fields

Field	Description
As of	The name of the Discovery Scan Job used to generate the widget graph and statistics. This job is the job most recently run.
Endpoints with agents	The number of agent-compatible endpoints discovered that have agents installed.
Endpoints without agents	The number of agent-compatible endpoints discovered that have no agents installed.
Endpoints	The total number of agent-compatible endpoints discovered.

Tip: Click the widget to open the ***Results*** page for the most recently run Discovery Scan Job.

The Endpoints with Unresolved Updates Widget
This widget displays all endpoints with unapplied applicable content updates, grouped by content type. View this widget when determining if an endpoint requires deployment.

An unresolved update is an occurrence of an endpoint that has not had an applicable content item installed.

Bar	Description
Critical	The number of endpoints that have unresolved critical content updates.
Recommended	The number of endpoints that have unresolved recommended content updates.
Optional	The number of endpoints that have unresolved software, informational, and virus removal content updates.

Tip: Click a widget graph bar to open the ***Content*** page, which is filtered to display all unapplied applicable content.

Field	Description
Endpoints	The number of endpoints with applicable updates within your network.

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.

Note:

- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved updates.
- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.

The Incomplete Deployments Widget

This widget displays all deployments with elapsed start dates and a status of *not started* or *in progress*.

Table 22: Incomplete Deployment Widget Fields

Field	Description
<25%	The number of deployments that are less than 25 percent complete. This field includes deployments that have not started.
25% - 49%	The number of deployments that are 25 to 49 percent complete.
50% - 69%	The number of deployments that are 50 to 69 percent complete.
70% - 79%	The number of deployments that are 70 to 79 percent complete.
80% - 89%	The number of deployments that are 80 to 89 percent complete.
>90%	The number of deployments that are more than 90 percent complete.
Total	The total number of deployments that have a status of *in progress* or *not started* with an elapsed start time.
Total affected endpoints	The total number of endpoints receiving pending or in-progress deployments.

The Last 5 Completed Scan Jobs Widget

This widget contains information about the last five completed discovery scan jobs. Each job name is a link to the associated ***Result*** page.

Table 23: Last 5 Completed Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the name to open the ***Results*** page for the job.

Column	Description
Completed Date	The date and time the job completed on the server.
Status	The status of the completed job.

The Latest News Widget
This widget displays important announcements and other information in Ivanti Endpoint Security.

Click a link to view additional details about an announcement.

The Mandatory Baseline Compliance Widget
This widget displays the Mandatory Baseline status for all endpoints that have the Patch and Remediation module installed.

Table 24: Mandatory Baseline Compliance Widget Fields

Field	Description
Compliant	The number of endpoints with all Mandatory Baseline content installed. **Note:** Endpoints that don't have Mandatory Baseline content installed that's marked *Do Not Patch* are considered compliant.
In process	The number of endpoints currently downloading Mandatory Baseline content.
No baseline	The number of endpoints with no content assigned to their Mandatory Baselines.
Non compliant	The number of endpoints that do not have all content in their Mandatory Baselines installed.
Total number of endpoints	The number of endpoints with an agent installed.

The Mobile Endpoint Last Check In Widget
This widget displays your mobile endpoints, which are grouped by the duration or their last check in.

The total number of mobile endpoints is grouped into six different time categories. Click the graph to open the ***Mobile Endpoints*** page, which will be sorted by date with the oldest endpoints listed on top.

Graph Bar	Description
1 day (Green)	The number of mobile endpoints that last checked in one day ago.
2 days (Light Green)	The number of mobile endpoints that last checked in two days ago.
3 days (Blue)	The number of mobile endpoints that last checked in three days ago.
4-7 days (Yellow)	The number of mobile endpoints that last checked in four to seven days ago.

Graph Bar	Description
8-14 days (Orange)	The number of mobile endpoints that last checked in 8 to 14 days ago.
14+ days (Red)	The number of mobile endpoints that last checked in 14 days ago or more.

The Mobile Endpoint Status Widget
This widget shows the last known status of all registered mobile endpoints. A pie chart displays the percentage of endpoints in each status.

Status	Description
Online	The number of endpoints that have checked in within the set communication interval without issue.
Online Jailbroken	The number of jailbroken iOS endpoints that have checked in within the set communication interval.
Online Rooted	The number of rooted Android endpoints that have checked in within the set communication interval.
Offline	The number of endpoints that have not checked in within the set communication interval.
Disabled	The number of disabled mobile endpoints.
Unmanaged	The number of mobile endpoints that have their profile removed or the app uninstalled.
Expired	The number of endpoints issued an expired license.
Wiped	The number of endpoints that have been sent a command to revert to factory settings.
Total mobile endpoints	The total number of mobile endpoints registered with Ivanti Endpoint Security.

Tip: Click an endpoint status to open the ***Mobile Endpoints*** page, which is filtered to display the clicked endpoint status.

The Mobile Endpoints with Policy Widget
This chart displays all mobile endpoints and their policy assignment status.

This table describes each widget bar.

Bar	Description
No Policy	The number of mobile endpoints that have no policy assignments.

Bar	Description
Blocked	The number of mobile endpoints that have policy assignments that are not being enforced because the endpoint has a status of **Unmanaged**, **Offline**, or **Expired**.
Pending	The number of mobile endpoints that have had a policy assignment that has not yet been applied.
Applied	The number of mobile endpoints that have a policy assignment applied successfully.

The Next 5 Pending Scan Jobs Widget
This widget displays information about the next five pending discovery scan jobs.

Table 25: Next 5 Pending Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the link to view the ***Discovery Scan Jobs*** page ***Scheduled*** tab.
Scheduled Time	The date and time the job is scheduled for on the server.

Tip: Click a job name link to view the ***Discovery Scan Jobs*** page ***Scheduled*** tab.

The Offline Patch Endpoints Widget
This widget displays all offline Patch and Remediation endpoints. These endpoints are grouped by time ranges since they last checked in.

Table 26: Offline Agents Widget Fields

Field	Description
< 48 hours	The number of Patch and Remediation endpoints offline fewer than 48 hours.
48 - 72 hours	The number of Patch and Remediation endpoints offline 48 to 72 hours.
> 72	The number of Patch and Remediation endpoints offline greater than 72 hours.
Total number of offline agents	The number of Patch and Remediation endpoints that are offline (since their last scheduled Discover Applicable Updates task).

Tip: Clicking the **Offline Patch Endpoints** widget pie chart opens the ***Endpoints*** page ***Patch and Remediation*** tab, which is filtered to display offline patch endpoints.

The Patch Agent Module Status Widget

This widget displays all endpoints with the Patch and Remediation module installed, which are grouped by Patch and Remediation status.

Table 27: Patch Agent Module Status Widget Fields

Field	Description
Working	The number of Patch and Remediation endpoints that are working on a deployment task.
Idle	The number of Patch and Remediation endpoints that are idle.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Sleeping	The number of Patch and Remediation endpoints that are sleeping.
Offline	The number of Patch and Remediation endpoints that are offline.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Agents with PR module installed.	The number of endpoints with the Patch and Remediation module installed.
Total Agents	The total number of Patch and Remediation endpoints in your network.

Tip: Click the graph to open the ***Endpoints*** page ***Ivanti Patch and Remediation*** tab.

The Scheduled Deployments Widget

This widget displays endpoints that have not-yet installed applicable content. These endpoints are divided in to two categories: endpoints with deployments scheduled and endpoints with deployments not scheduled. These categories are further divided into three categories: endpoints with not-yet applied critical content, endpoints with not-yet applied recommended content, and endpoints with not-yet applied optional content.

Orange graph bars indicate endpoints that are not scheduled to receive applicable content, while blue graph bars indicate endpoints that are scheduled to receive applicable content.

Table 28: Scheduled Deployments Widget Graph Bars

Graph Bar	Description
Critical	The number of endpoints scheduled or not scheduled to receive deployments for critical content.
Recommended	The number of endpoints scheduled or not scheduled to receive deployments for recommended content.

Graph Bar	Description
Optional	The number of endpoints scheduled or not scheduled to receive deployments for optional content.

Tip: Clicking the **Scheduled Deployments** widget opens the ***Deployments and Tasks*** page, which is filtered to display scheduled deployments.

Table 29: Scheduled Deployments Widget Field

Field	Description
Endpoint with unresolved updates	The number of endpoints with unresolved updates.

The Server Information Widget

This widget lists your serial number, number of licenses available, number of licenses in use, and information about current license usage and availability.

Table 30: Server Information Widget Fields

Field Name	Description
Company	The company your server is registered to as defined during installation.
Serial Number	The license number (serial number) assigned to your server.
License Replication	The subscription status between your server and the Global Subscription Service (GSS).
System Replication	The system replication status between your server and the GSS.
Patch / Content Replication	The replication status between your server and the GSS.
Package Replication	The number of packages remaining for replication.
Auto-download New Critical Packages	The indication of whether your automatically downloads packages for critical vulnerabilities. Click the link to open the ***Subscription Service Configuration*** dialog. For additional information refer to Configuring the Service Tab on page 139.

Table 31: Product Licenses Table Columns

Column	Description
Product Module	The module for which you purchased licenses.
In Use	The number of module licenses in use.

Column	Description
Pending	The number of licenses pending use or pending removal. Licenses pending removal become available upon removal completion.
Available	The number of licenses available.

Note: A license expiration notice displays if all available licenses are expired.

The Time Since Last DAU Scan Widget
This widget displays all active agents (not including *disabled* or *offline*) grouped by the amount of time since their last Discover Applicable Updates task.

Table 32: Time Since Last Agent Scan Widget Fields

Field	Description
< 24 hours	The number of agents that last performed a Discover Applicable Updates (DAU) task and checked in fewer than 24 hours ago.
24 - 47 hours	The number of agents that last performed a DAU task and checked in 24 to 47 hours ago.
48 - 72 hours	The number of agents that last performed a DAU task and checked in 48 to 72 hours ago.
> 72 hours	The number of agents that performed a DAU task and last checked in greater than 72 hours ago.
Never checked in	The number of agents that have registered yet have not completed a DAU task.
Total active agents	The total number of active agents.

Tip: Click the **Time Since Last Agent Scan** widget graph to open the ***Endpoints*** page, which is filtered to display enabled endpoints.

The Un-remediated Critical Vulnerabilities Widget
This widget displays the total number of unremediated critical vulnerabilities that are applicable to your environment grouped by age.

Table 33: Un-remediated Critical Vulnerabilities Widget Graph

Graph Bar	Description
<30 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network fewer than 30 days old.

Graph Bar	Description
30 - 120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network that are 30 to 120 days old.
>120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network greater than 120 days old.

Tip: Click the graph to open the ***Vulnerabilities*** page, which is filtered to display critical but not superseded applicable vulnerabilities.

Table 34: Un-remediated Critical Vulnerabilities Widget Fields

Field	Description
Critical Vulnerabilities	The number of critical but not superseded vulnerabilities applicable in your network.
Endpoints	The number of endpoints with critical but not superseded applicable vulnerabilities.

Note:

- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Critical vulnerabilities** count.
- If an endpoint is marked as *Do Not Patch* for an applicable vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Endpoints with Unresolved AV Alerts Widget

This widget displays the number of endpoints with unresolved antivirus event alerts.

There are two types of unresolved antivirus event alerts, *not cleaned* and *quarantined*. If an endpoint has multiple not cleaned event alerts, it is counted only once in the **Not Cleaned** column. Likewise, if it has multiple quarantined event alerts, it is counted only once in the **Quarantined** column. However,

if an endpoint has both not cleaned and quarantined event alerts, it is counted twice (once in each column).

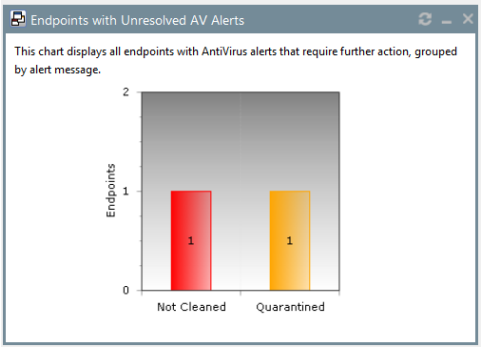


Figure 20: Endpoints with Unresolved AV Alerts Widget

The following table describes each graph bar.

Bar	Description
Not Cleaned	The number of endpoints with not cleaned event alerts.
Quarantined	The number of endpoints with quarantined event alerts.
Tip: Clicking a widget graph bar opens the ***Virus and Malware Event Alerts*** page, which is filtered on the endpoint name.	

The Top 10 Infected Endpoints Widget
This widget displays the 10 endpoints which have received the most event alerts in the last 10 days, and a breakdown of each endpoint's alert status.

The widget lists all event alert types, including cleaned, not cleaned, deleted, and quarantined.

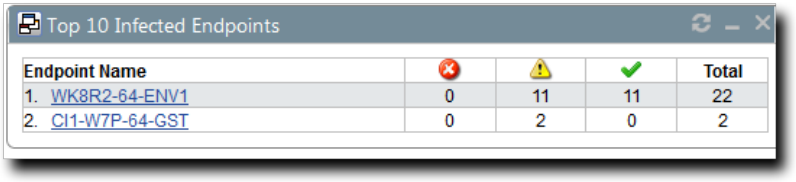


Figure 21: Top 10 Infected Endpoints Widget

The following table describes each column in the widget.

Column	Description
Endpoint Name	The name of the endpoint, with a link to its ***Details*** page.
Not Cleaned	The number of alerts on the endpoint where it was not possible to clean a suspect file.

Column	Description
Quarantined	The number of alerts on the endpoint where the file was moved to quarantine.
Cleaned	The number of alerts on the endpoint where a file was successfully cleaned.
Deleted	The number of alerts on the endpoint where a suspect file was deleted.
Total	The total number of all alerts on the endpoint. This is the number on which the ranking of the list is based.

The Top 10 Virus/Malware Threats Widget

This widget displays the 10 types of virus or malware that have generated the most event alerts in the last 10 days.

The malware types are listed from the top down in descending order of frequency, and the number of endpoints affected is displayed along the bottom of the widget.

Note: The display is based on the number of event alerts generated by each virus/malware type, regardless of how the event was handled (cleaned, not cleaned, deleted, or quarantined).

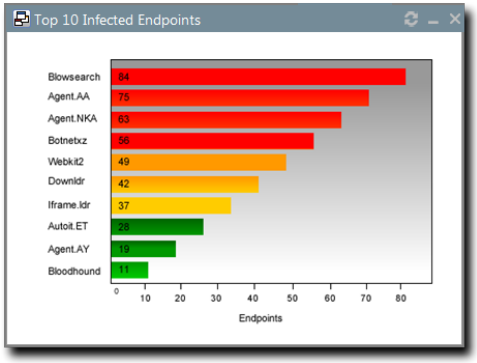


Figure 22: Top 10 Virus/Malware Threats

Clicking on any virus/malware bar will bring you to its ***Virus/Malware Details*** page.

The Estimated Energy Savings: Daily Widget

This widget displays the energy savings for the previous day. This calculation is based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 35: Estimated Energy Savings: Daily Widget Fields

Field	Description
Results for the day of	The date for which the widget displays the results.
Desktop count	The number of monitored desktops.

Field	Description
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Weekly Widget
This widget displays the energy savings of the past seven days based on your endpoints' actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 36: Estimated Energy Savings: Weekly Widget Fields

Field	Description
Results for the week from	The dates for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Monthly Widget

This widget displays the energy savings of the past 30 days based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

The following table describes the fields in the **Estimated Energy Savings: Monthly** widget.

Table 37: Estimated Energy Savings: Monthly Widget Fields

Field	Description
Results for the month from	The month for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Device Control Denied Actions Widget

This widget displays the users with the highest number of actions blocked by device control policies. View this widget when determining the lists of users for whom action block occurred due to the device control policies.

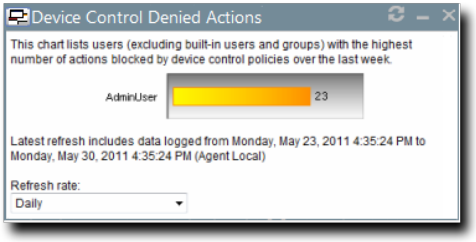


Figure 23: Device Control Denied Actions Widget

The chart displays the users with the highest number of actions blocked by device control policies. The widget can displays five users with the highest number of actions blocked by device control policies.The count on the bar displays the number of times the user actions were blocked by the device control policies.

The Devices Connected to Endpoints Widget

This widget displays the number of peripheral device classes that were connected to endpoints. View this widget when determining which devices were connected to endpoints over the last week.

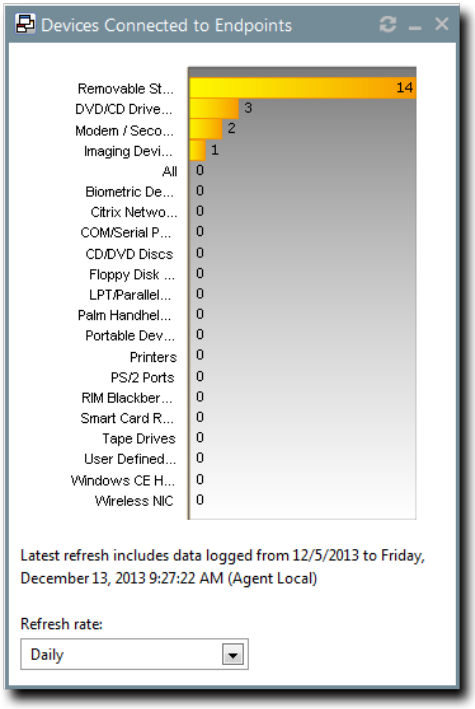


Figure 24: Devices Connected to Endpoints Widget

The chart displays the number of devices in each device class connected to the endpoints. The count on the bar displays the number of devices in a particular device class that were connected to the endpoints.

Dashboard Setting and Behavior Icons

Setting and behavior icons are UI controls used to manage the dashboard. Click these icons to maximize, minimize, hide, and refresh the dashboard and widgets.

The following table describes each icon action.

Table 38: Widget Setting and Behavior Icons

Icon	Action
	Opens the ***Dashboard Settings*** dialog.
	Opens the dashboard in print preview mode.

Icon	Action
	Collapses the associated widget.
	Expands the associated collapsed widget.
	Hides the associated widget.
	Refreshes the associated widget (or the entire dashboard).

Note: Not all widgets contain **Refresh** icons.

Previewing and Printing the Dashboard

When viewing the dashboard, you can reformat it for printing. This reformat omits the Web site header and footer, reorganizing the dashboard to display only the selected widgets, making it ideal for printing.

1. From the **Navigation Menu**, select **Home**.
2. Click  .

   Step Result: The dashboard print preview opens in a new Web browser window.
3. [Optional] Use your Web browser controls to print the dashboard.

Editing the Dashboard

You can customize how widgets are arranged and prioritized. Edit the dashboard to display only the widgets useful in your environment.

Edit the dashboard from the ***Dashboard Settings*** dialog.

1. From the **Navigation Menu**, select **Home**.
2. Click  .

   Step Result: The ***Dashboard Settings*** dialog opens.
3. Choose which widgets you want to display on the dashboard.
   - Select widget check boxes to display them.
   - Clear widget check boxes to hide them.
4. Prioritize the widgets in the desired order.
   - Click  to increase a widget priority.
   - Click  to decrease a widget priority.

   Highly prioritized widgets are more prominently placed.

5. Display or hide widget descriptions.
   - Click to display descriptions.
   - Click to hide descriptions.
6. Choose a widget layout.
   - Click to display widgets in two columns.
   - Click to display widgets in three columns.
7. Click **OK**.

Result: Your dashboard settings are saved. The ***Home*** page displays the selected widgets in the priority you defined.

The System Alert Pane

The ***System Alert*** pane displays information about changing conditions in your environment. This pane alerts you to required actions and links to related help topics.

The **System Alert** pane displays in the dashboard and shows the number of alerts that require your attention.

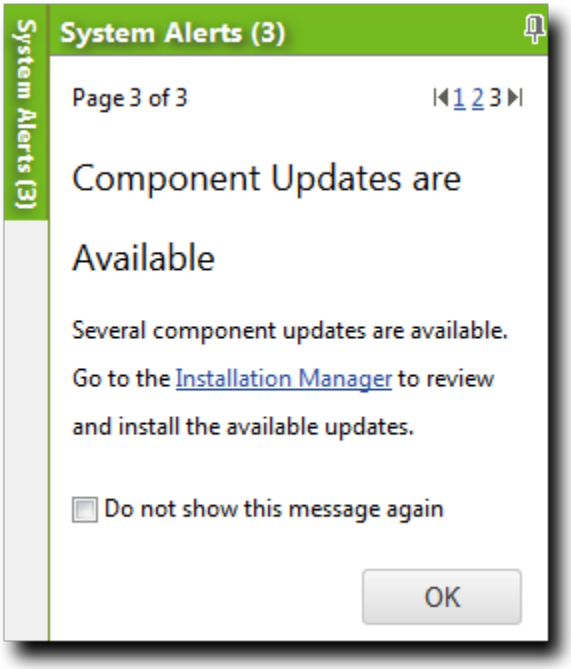


Figure 25: The System Alert Pane

The following functions can be found in the ***System Alert*** pane.

Table 39: Options Menu Items

Option	Description
Pin (icon)	Docks the ***System Alert*** pane. Clicking this icon again collapses it.
Pagination Links	Allows you to navigate between alerts. For more information, see Advancing Through Pages on page 46.
Action Link	Opens the appropriate application page, external Web page, or context-sensitive help topic, depending on the action specified in the alert.
Don't show this again (check box)	Collapses the ***System Alert*** pane. The alert shown in the ***System Alert*** pane when this check box is selected will no longer be shown.
OK (button)	Collapses the ***System Alert*** pane.

Note:

- Dismissing a notification only dismisses the notification for logged in user. The notification still displays for others.
- The system automatically dismisses alerts as you complete their related actions, regardless of whether you dismiss the alerts.

License Expiration

When licensing for a module expires, the module behavior changes. All functionality is restored when the licensing is renewed.

Note: When a subscription expires, the module history and configuration is retained. No work is lost when the module is renewed.

Table 40: License Expiration Scenario and Events

Scenario	Event(s)
Server Module Expiration	• Endpoint module functionality is partially disabled. • The module cannot be installed on additional endpoints. • The ***Endpoints*** page list the module status as `Expired`. • The ***Home*** page lists the **Available** license count as `Expired`.
Endpoint Module Expiration	• Endpoint module functionality is partially disabled. • The module cannot be installed on additional endpoints. • The ***Endpoints*** page list the module status as `Expired`. • The ***Home*** page lists the **Available** license count as `Expired`. • The Patch and Remediation endpoint module component continues to inventory its host, but no longer enforces Patch and Remediation policies or downloads deployments. • The AntiVirus endpoint module continues enforcing policies and completing scans, but no longer downloads new virus definitions. • The Application Control endpoint component stops enforcing all policies, no longer blocking or logging applications. • The Device Control endpoint component allows all actions and stop logging activity.

Table 41: License Expiration Scenario and Events for Mobile Endpoints

Scenario	Event

Mobile Endpoint Module Expiration	• The ***Mobile Endpoints*** page list the module status as `Expired`.
	  • Endpoints with the oldest check ins expire first.
	  • Endpoints that attempt to register when your license count is depleted are listed with a status of `Expired`.
	  • Endpoints cannot be issued commands with the exception of **Delete**.
	  • Any push notifications available on expired endpoints are removed.
	  • Any policy events queued or issued to expired endpoints have display a status of `Expired`.
	• Endpoints cease communications with the server and the cloud.
	• The ***Home*** page lists the available license count as `0`.

	Note: Endpoints in an `Offline` or `Wiped` status hold their license until deleted.

To reactivate your licenses following renewal, open the ***Subscription Updates*** page and click **Update Now**. Your server replicates updated subscription information. The page refreshes when the update completes, and all previous module functionality is restored.

Note: For more information about renewing or adding licenses, contact Ivanti Sales Support (sales@ivanti.com) .

Chapter 4

Configuring Options

In this chapter:

You can customize your system to use options and settings that you select.

Ivanti Endpoint Security contains general options and agent options. More options are added when you install new modules.

After installing the Patch and Remediation, new options are added for agents and deployments.

The Options Page

You can control a number of default settings from the ***Options*** page: user interface options, agent options, and so on. Use these options to customize default settings and values.

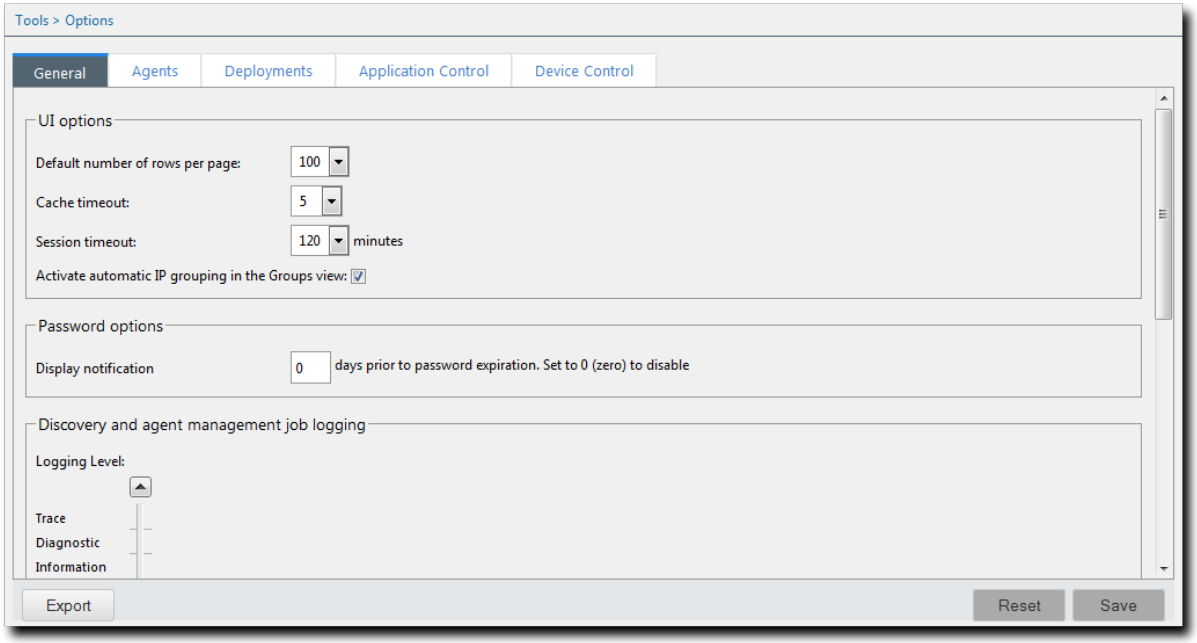


Figure 26: Options Page

The ***Options*** page contains the following tabs, which contain options related to their labels:

- The General Tab on page 76
- The Agents Tab on page 79

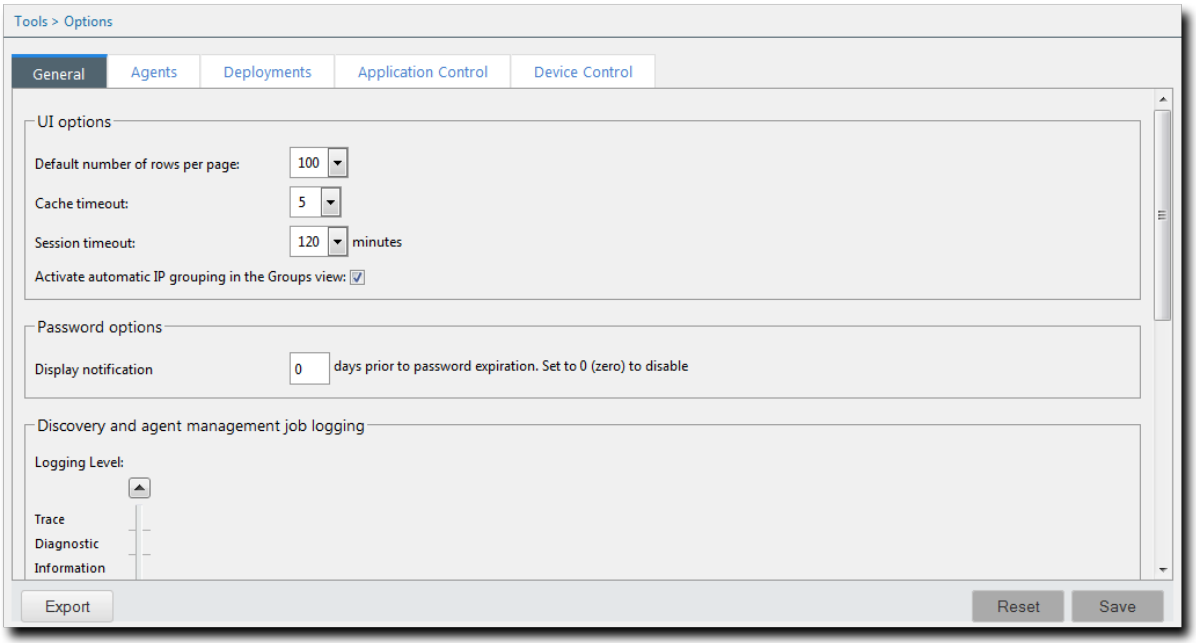


Figure 27: Options Page

- Patch and Remediation adds the new ***Deployments*** tab. It features options for configuring the default values in the ***Deployment Wizard***. For additional information, refer to The Deployments Tab on page 85.
- Several new options are also added to the ***Agents*** tab. For additional information, refer to The Agents Tab on page 79.

The Options Page Buttons

The ***Options*** page contains several buttons that are common to each of its tabs. These buttons share similar functions to buttons commonly seen on page toolbars.

The following table describes the ***Option*** page button functions.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Reset	Cancels any edits made to the options since the tab was loaded.
Save	Saves the tab option settings (if any edits were made). You must click this button to implement your edits.

Viewing the Options Page

Navigate to the ***Options*** page to edit default system settings.

You can reach this page from the **Navigation Menu**.

1. From the **Navigation Menu**, select **Tools** > **Options**.
2. Select a tab.
3. [Optional] Complete a task listed in Working with Options on page 87.

The General Tab

Default settings for user interface options, password options, security configuration management options, and report and display options are controlled from the ***General*** tab. The options available on this page are generalized and are not closely related.

UI Options

With these options, you can control user interface features according to your preferences.

Select from lists and check boxes to configure **UI options**.

Table 42: UI Options

Option	Description
Default number of rows per page	Defines the default number of rows that display in list pages (**25**, **50**, **100**, **200**, **500**).
Cache timeout	Defines the maximum number of minutes data is held in the memory before it needs to be reloaded from the database (**5**, **10**, **15**, **20**, **30**).
Session timeout	Defines the number of minutes before a repeat login is required due to inactivity (**20**, **40**, **60**, **80**, **100**, **120**).

Option	Description
Activate automatic IP grouping in the Groups view	Creates groups organized by IP address in the ***Groups*** page **Browser** named **IP Collection**.
Enhanced Reports URL	Defines the URL that is opened when **Reports** > **Enhanced Reports** is selected from the **Navigation Menu**. This feature is intended to open a third-party reporting solution, but you can use it to open any URL you want.

Password Options
This option defines the number of days before an upcoming password expiration that a warning appears that notifies you of the upcoming expiration.

Complete the field to configure the options.

The following table describes the available **Password option**.

Table 43: Password Options

Option	Description
Display notification *x* days prior to password expiration.	Defines the number of days prior to a required password change (as controlled by Windows) that a notification displays. A value of `0` disables the notification.

Note: User that do not have password expirations are unaffected by this option.

Discovery and Agent Management Job Logging
During Discovery Scan or Agent Management Jobs, a log of events is saved on your server. The **Discovery and Agent Management Job Logging** options lets you configure the information that is logged during job activity.

Table 44: Discovery and Agent Management Job Logging Options

Option	Description
Logging Level	Defines the information recorded in the job during Discovery Scan Jobs and Agent Management Jobs. Options include: • **Trace** • **Diagnostic** • **Information** • **Warning** • **Error** • **Critical**

Option	Description
Include common troubleshooting information for	Defines whether the log include common troubleshooting information for a given part of a job. Options include: • **Agent Management** • **Discover** • **SOAP**

Note: By default, Discovery Scan and Agent Management Job logs are saved to `%Installation Directory%\HEAT Software\EMSS\Web\Services\ScanEngine\Engine\engine.log` on the server.

Report and Display Options
These options control date, time, and paper formatting for reports. Modify date and time settings according to your locale. Modify paper settings according the paper types your enterprises uses for printing.

Note: These options apply only to reports in a PDF format.

Table 45: Report and Display Options

Option	Description
Date format	Defines the date format displayed in text-based and graphical reports. Select from the following options: • **Default** (mm/dd/yyyy) • **MM/dd/yyyy** • **dd/MM/yyyy** • **yyyy-MM-dd** • **dd.MM.yyyy** • **dd-MM-yyyy** • **yyyy/MM/dd**
Time separator	Defines the character used to separate hours, minutes, and seconds in reports. Select from the following options: • **Default** (the current character in use) • **Colon** (**:**) • **Period** (**.**) This option also defines the time format used in reports. Select from the following options: • **12 Hour** • **24 Hour**

Option	Description
Time format	Displays the selected **Date Format** punctuated by the selected **Time Separator**. This field refreshes as you select different **Report and display options**.
Paper size for reports	Defines how reports are formatted for printing. Select from the following options: • **Default** (the currently saved formatting style) • **Letter** • **A4**

Security Configuration Management (SCM)
This option lets you remove and delete Ivanti Security Configuration Management benchmarks when they are no longer needed.

The following table describes each option.

Table 46: Security Configuration Management (SCM)

Option	Description
Manage Benchmarks	Opens the ***Configuration Policy Manager***. For additional information, refer to Using the Configuration Policy Manager.
Note: Ivanti Security Configuration Management options operate independently of the ***General*** tab. Therefore, clicking **Save** is not necessary when editing these options.	

The Agents Tab

This tab contains default options related to the agent.

Default option sections include:

- Agent Installation on page 80
- Communication on page 81
- Absentee Agent Deletion on page 82
- Agent Versions on page 83

Patch and Remediation adds the following option sections:

- Discover Applicable Updates Options on page 81
- ISAPI Communication on page 82

Patch and Remediation also adds new options to existing sections:

- Communication on page 81
- Agent Versions on page 83

Agent Installation
These options define default installation values for Agent Management Jobs. Adjusting these settings can help save on effort using an Agent Management Job.

Use **Agent Installation** options to define the default settings for the ***Agent Settings*** page in the ***Schedule Agent Management Job Wizard***. Complete the field and select from the lists to define the options.

Note: When configuring an Agent Management Job, the following options can be changed.

Table 47: Agent Installation Options

Agent Installation Option	Description
Timeout (drop-down list)	Defines the default number of minutes before an agent installation job terminates due to non-responsive status (0-30).
Number of retries (drop-down list)	Defines the default number of attempts an agent installation will retry if initial and subsequent installations fails (1-10).
Number of simultaneous installs (drop-down list)	Defines the default maximum number of agents that can be installed or un-installed simultaneously during an Agent Management Job (1-25). A setting of `1` indicates that serial install/uninstalls should occur.
Server identity (field)	Defines the default text entered in the **Server Identity** field during agent installation jobs. **Server Identity** is the name agents list as their Ivanti Endpoint Security server.
Scan method for pre-selected targets (radio buttons)	Defines how endpoints pre-selected from a page list are added to a job's **targets** list (discovery scan or agent management) after launching a job configuration dialog. The options are: **IP Address** — Adds the selected endpoint to a job's target list using its IP address. **Computer Name** — Adds the selected endpoint to a job's target list using its endpoint name.

Communication
This section contains default options for agent communications with the server.

Patch and Remediation adds a new option.

Table 48: Communication Options

Option	Description	
Agents should be shown offline when inactive for	Defines the time period (in minutes, hours, or days) before an agent is considered offline because it has not checked. A value of *0* disables this option. **Tip:** Disabled and uninstalled agents are not considered offline.	
Stand alone Patch agent uniqueness based on	Defines how the server identifies Patch Agents during communication.	
	Endpoint name	Configures the server to identify Patch Agents using the NetBIOS name of the endpoint. Select this option in smaller networks where endpoints are unlike to share a NetBIOS name, as it reduces administrative maintenance in the event that an endpoint needs to be re-imaged. This option is selected by default.
	Instance	Configures the server to identify Patch Agents using a unique number. Select this option in larger network environments where multiple instances of a single NetBIOS name may exist. This option prevents communication errors related to multiple agents sharing a name.

Discover Applicable Updates Options
You can select the default events that schedule a **Discover Applicable Updates** task for Patch and Remediation Patch and Remediation endpoints. These options are added after Patch and Remediation is installed.

Table 49: Discover Applicable Updates Options

Option	Description
DAU should be run after subscription replication	Determines a DAU task is scheduled for all endpoints following a subscription replication.

Option	Description
DAU should be run after inventory change	Determines a DAU task is scheduled for an endpoint after if detects an inventory change.

Absentee Agent Deletion
Sporadically, an endpoints will cease communication with the server. Configure the **Absentee Agent Deletion** option to determine the amount of time before the agent is removed from your server database.

Table 50: Absentee Agent Deletion Option

Option	Description
Delete absentee agent after *x* days.	Removes an uncommunicative agent after the defined time period (days). A value of *0* disables this function.

Note: Absentee agents records are only deleted from the database, leaving no history of them in the Web console. However, the agent software is not deleted from its host endpoint.

ISAPI Communication
Using these options, you can limit connections between the server and Patch and Remediation endpoints. Limiting server and endpoint communications ensures the server can handle all incoming agent communications. These options are added after Patch and Remediation is installed.

Ivanti Endpoint Security supports the Internet server application programming interface (ISAPI) communication settings for Internet Information Services (IIS).

Table 51: ISAPI Communication Options

Option	Description	
Concurrent agent limit	Defines the maximum number of threads used by the server. Select from the following options:	
	SQL default (64 threads)	Enables the default thread count for a SQL Server implementation.
	Custom setting (5 to 256 threads)	Enables a custom thread count.

Option	Description	
Connection timeout	Defines the number of seconds before an ISAPI thread times out. Select from the following options:	
	Default (30 seconds)	Sets the connection timeout to the default value.
	Custom setting (5 to 300 seconds)	Sets the connection timeout to a custom value.
Command timeout	Defines the number of seconds before an ISAPI command times out. Select from the following options:	
	Default (60 seconds)	Sets the command timeout to the default value.
	Custom setting (5 to 900 seconds)	Sets the command timeout to a custom value.

Agent Versions

There are multiple versions of the agent. By defining **Agent Version** options, you can limit which versions are available for installation.

After Patch and Remediation is installed, an **Agent Version** list for Linux, Unix, & Mac is added.

Table 52: Agent Version Options

Option	Description
Windows 7 and newer agent version	Defines which agent versions are available for installation on endpoints running Windows operating systems when working with the following system dialogs: • The ***Manage Agent Versions*** Dialog • The ***Download Agent Installers*** Dialog • The ***Install Agents Wizard***
	Note: Windows XP and Windows Server 2003 are only supported on Agent Version 8.3.0.10. For additional information, see Knowledge Base Article 1752.

Option	Description
Linux, Unix, & Mac agent version (Patch and Remediation only)	Defines which agent versions are available for installation on endpoints running Unix-based operating systems when working with the following system dialogs: • The ***Manage Agent Versions*** Dialog • The ***Download Agent Installers*** Dialog

Note:

When selecting agent version options, remember the following information:

- **Newest Available** means only the latest agent version is available for installation.
- ***Agent Version* only** list items mean only that agent version is available for installation.
- ***Agent Version* +** list items mean that agent version and all versions that supersede it are available for installation.

The Agent Version Detail Dialog

This dialog describes the various agent versions. It also lists system requirements, applicable notes, and recent changes.

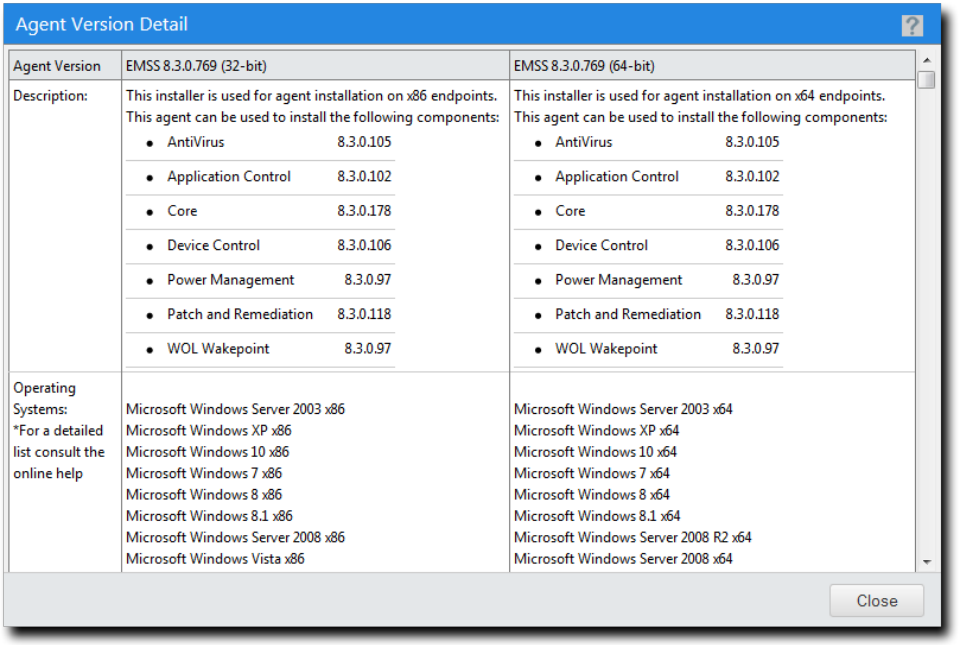


Figure 28: Agent Version Detail Dialog

To access this dialog, click the **What is different about each version?** link on the ***Agents*** tab.

Field	Description
Agent Version	The agent name and version number.
Description	A description of the agent. This field also lists the components that are installed with the agent.
Operating Systems	The operating systems that are supported by the agent.
System Requirements	The system requirements to install the agent on a endpoint.
Installation Notes	The information notes pertaining to installation of the agent.
Changes	The changes made to the agent since its previous release.

The Deployments Tab

This tab, added after installing Patch and Remediation, lets you configure default values related to deployments.

This tab includes options for:

- **Deployment defaults**, which you can use to configure the number of deployment-related tasks that can run at one time.
- **Notification defaults**, which you can use to set the default text that displays when users are notified of their deployments.
- **User interface**, which controls whether the deployments you schedule are listed in the Web console using agent local time or UTC time.

Deployment Defaults

These options let you define how many endpoints can perform actions simultaneously. Defining higher values lets you perform more deployment-related actions simultaneously. However, multiple agents performing actions simultaneously may strain network resources.

Table 53: Deployment Default Options

Option	Description
Maximum number of deployments that can run simultaneously	The number of endpoints that can simultaneously run deployments.
Maximum number of simultaneous Discover Applicable Updates (DAU) tasks	The number of enddpoints that can simultaneously run the DAU task.
Maximum number of reboot tasks that can run simultaneously	The number of endpoints that can simultaneously receive a deployment requiring a reboot.
Maximum number of simultaneous mandatory baseline deployments	The number of endpoints that can simultaneously receive Mandatory Baseline deployments.

Option	Description
Maximum number of times a deployment will be consecutively attempted	The number of failed deployment attempts permitted before the server disables it. This option does not apply to Mandatory Baseline deployments. This option also disables the deployment for endpoints that have not started it.

Notification Defaults
When using the ***Deployment Wizard***, you can configure a deployment to notify recipients. By using **Notification defaults**, you can create default notification for the ***Deployment Wizard***.

These notifications, which are pop-up dialogs, alert endpoint users that a deployment is about to occur. Default notification settings can be overridden when completing the ***Deployment Wizard***.

Table 54: Notification Defaults Options

Option	Description
User notification windows should always be on top	Defines the default selection for the **Deployment Notification Options** and **Reboot Notification Options** when completing the ***Deployment Wizard***.
Manual Installation	Defines the default message that displays when the deployment recipient receives a package requiring manual installation.
May Reboot	Defines the default message that displays when the deployment recipient receives a package that may require the recipient to reboot.
Default deployment message	Defines the default message that displays with a deployment notification.
Default reboot message	Defines the default message that displays with a deployment reboot notification .

Note: All notifications may contain a maximum of 1000 characters.

User Interface
When using the ***Deployment Wizard***, you can configure a deployment times in the Web console to display as endpoint local time or endpoint Coordinated Universal Time (UTC). This option also affects what start time option is selected by default when completing the ***Deployment Wizard***.

Table 55: User Interface Option Descriptions

Option	Description
Agent Local Time (Deploy at local time for each individual node)	Defines **Agent Local Time** as the deployment start time in the Web console and the ***Deployment Wizard***.

Option	Description
Agent UTC Time (Deploy at UTC time for each individual node)	Defines **Agent UTC Time** as the deployment start time in the Web console and the ***Deployment Wizard***.

Working with Options

From each ***Options*** page tab, you can define default behavior for different Ivanti Endpoint Security features.

- Configuring the General Tab on page 87
- Configuring the Agents Tab on page 89
- Configuring the Deployments Tab on page 91
- Exporting Option Data on page 92

Configuring the General Tab

Configure this tab to define how user interface, password, and report display options behave.

Configure the ***General*** tab from the ***Options*** page.

1. From the **Navigation Menu**, select **Tools** > **Options**.
2. Ensure the ***General*** tab is selected.
3. Define the **UI options**.

   These options define general user interface behavior.

   a) Select a value from the **Default number of rows page** list (**25**, **50**, **100**, **200**, **500**).

   This option defines the default number of rows that display in list pages.

   b) Select a value from the **Cache timeout** list (**5**, **10**, **15**, **20**, **30**).

   This option defines the maximum number of minutes data is held in the memory before it needs to be reloaded from the database.

   c) Select a value from the **Session timout** list (**20**, **40**, **60**, **80**, **100**).

   This option defines the number of minutes before a repeat login is required due to inactivity.

   d) Select or clear the **Activate automatic IP grouping in the Groups view** check box.

   This option creates groups organized by IP address in the ***Groups*** page **Browser** named **IP Collection**.

   e) Define an **Enhanced Reports Url**.

   This option is used to define the URL of your custom reports Web page, if one is used in your environment. However, you can enter any URL you want. This URL can be opened by selecting **Reports** > **Enhanced Reports** from the **Navigation Menu**.

4. Define the **Password options**.

   This option defines the number of days prior to a required password change (as controlled by Windows) that a notification displays. Type a value in the **Display notification *x* days prior to password expiration** field. A value of `0` disables password expiration.

5. Define the **Discovery and Agent Management Job logging** options.

   These option control what information is recorded during Discovery Scan Jobs and Agent Management Jobs. Complete the following substeps:

   a) Select a **Logging Level**.

      Logging levels include:

      - **Trace**
      - **Diagnostic**
      - **Information**
      - **Warning**
      - **Error**
      - **Critical**

   b) Select the check boxes for the desired **Include common troubleshooting information for** options.

      Option include:

      - **Agent Management**
      - **Discovery**
      - **SOAP**

6. Define the **Report and display options**.

   These options control formatting options for PDF reports. Perform the step(s) required to define each option.

   Tip: The **Default** item available in each **Report and display options** returns the applicable option to the last saved value.

   a) Select a value from the **Date format** list.

      This option defines the date format displayed in text-based and graphical reports.

   b) Select a value from the two **Time separator** options.

      This option defines the character used to separate hours, minutes, and seconds in reports. This option also defines the time notation used in reports.

      Tip: The **Time format** field previews your **Time separator** selections.

   c) Select a value from the **Paper size for reports** list.

      This option defines how reports are formatted for printing.

7. Define **Security Configuration Management (SCM)** options.

   Click the **Modify** button adjacent to **Manage Benchmarks**. For additional information, refer to Using the Configuration Policy Manager.

8. Click **Save**.

Result: The ***General*** tab configuration is saved.

Configuring the Agents Tab

Configure this tab to define default agent behavior. Settings include agent installation settings, communication settings, and agent version settings.

Configure the ***Agents*** tab from the ***Options*** page. After installing Patch and Remediation, configure the new communication, DAU, ISAPI, and agent version options that are added.

1. Select **Tools** > **Options**.

   Step Result: The ***Options*** page opens.

2. Select the ***Agents*** tab.
3. Define the **Agent Installation** options.

   These options define the default values for Agent Management Jobs.

   a) Select a value from the **Timeout** list (**1**-**30** minutes).

   This option defines the number of minutes before a job times out because the endpoint does not respond.

   b) Select a value from the **Number of retries** list (**1**-**10**).

   This option defines the number of attempts a job retries if initial and subsequent installations fail.

   c) Select a value from the **Number of simultaneous installs** list (**1-25**).

   This option defines the number of agents that can be installed or uninstalled simultaneously during a job. A value of **1** configures jobs for serial installations.

   d) Type a value in the **Server identity** field.

   This field defines the default text entered in the **Server Identity** field during jobs. Identity is the name endpoints list as their server. Type identity in one of the following formats:

   - `computername.domainname.com`
   - `computername`
   - `10.10.10.10`

   e) Select a **Scan method for pre-selected targets** option:

   These buttons define how endpoints select from a page list are added to the job **Targets** list. The options include:

   - **IP Address**
   - **Computer Name**

4. Define the **Communication** options.

   To define these options, complete the following substeps.

   a) Type a value in the **Agents should be shown offline when inactive for** field (**0**-**9999**).

      This option defines the time period (in minutes, hours, or days) before an endpoint status changed to offline because it has not checked in with your sever. Disabled and un-installed agents are not considered offline. A value of *0* disables this option.

   b) Select a value from the **Agents should be shown offline when inactive for** list.

      Select from the following values:

      - **Minute(s)**
      - **Hour(s)**
      - **Day(s)**

   c) Select a **Stand alone Patch agent uniqueness based on** option.

      These options define how the server identifies patch agents during communication (Patch and Remediation only). Select from the following options:

      - **Endpoint name**
      - **Instance**

5. Define the **Discover Applicable Updates (DAU) Options**.

   These options determine whether endpoints perform a DAU task following system actions. Select or clear the following options:

   - **DAU should be run after subscription replication**
   - **DAU should be run after inventory change**

6. Define the **Absentee agent deletion** option.

   This option defines when an uncommunicative endpoints are removed the Web console and system database. Type a value in the **Delete absentee agent after *x* Days** field (**0**-**999**) Days. A value of 0 disables the option.

7. Define the **ISAPI communication** options.

   a) Select a **Concurrent agent limit** option. If you select **Custom setting**, type the number of threads you want to simultaneously allow to your database (5-256).

   b) Select a **Connection timeout** option. If you select **Custom setting**, type the number of seconds that you want to consider an ISAPI thread considered timed out (5-300).

   c) Select a **Command timeout** option. If you select **Custom setting**, type the number of seconds that you want an ISAPI command considered timed out (5-900).

8. Define the **Agent Versions** options.

   These options define the agent versions that are available for installation during when working with the following system dialogs:

   - The ***Manage Agent Versions*** Dialog
   - The ***Download Agent Installers*** Dialog
   - The ***Install Agents Wizard***

   a) Select a value from the **Windows 7 and newer agent version**.
   b) Select a value from the **Linux, Unix, & Mac agent version** (Patch and Remediation only).

   Because the agent is updated regularly, **Agent Versions** option list values change frequently. Additionally, when selecting agent version options, remember the following information:

   - **Newest Available** means only the latest agent version is available for installation.

     Note: This option only defines which agent version is available when working with the ***Manage Agent Versions*** dialog, the ***Download Agent Installers*** dialog, or the ***Install Agents Wizard***. It does not automatically install newly released agent versions on network endpoints. To ensure the newest agent version is installed on network endpoints, you must manually define the latest version. For additional information, refer to Upgrading Endpoints on page 179.

   - ***Agent Version* only** list items mean only that agent version is available for installation.
   - ***Agent Version* +** list items mean that agent version and all version that supersede it are available for installation.

9. Click **Save**.

Result: The ***Agents*** tab configuration is saved.

Configuring the Deployments Tab

Configuring this tab defines default setting for the ***Deployment Wizard***. Selecting frequently used values from this tab leads to faster completion of the ***Deployment Wizard*** when deploying content.

Configure the ***Deployments*** tab from the ***Options*** page.

1. From the **Navigation Menu**, select **Tools** > **Options**.
2. Select the ***Deployments*** tab.
3. Define the **Deployments defaults** options.

   Complete the following substeps.

   a) Type a value in the **Maximum number of deployments that can run simultaneously** field.

      This option defines the number of endpoint that can simultaneously download deployments.
   b) Type a value in the **Maximum number of simultaneous Discover Applicable Updates (DAU) task** field.

      This option defines the number of endpoint that can simultaneously run the DAU task.

c) Type a value in the **Maximum number of reboot tasks that can run simultaneously** field.

This option defines the number of endpoints that can simultaneously run the reboot task.

d) Type a value in the **Maximum number of simultaneously mandatory baseline deployments** field.

This option defines the number of endpoints that can simultaneously download Mandatory Baseline deployments.

e) Type a value in the **Maximum number of times a deployment will be consecutively attempted** field.

This option defines the number of failed deployment attempts allowed before the deployment is disabled. This option does not apply to Mandatory Baseline deployments. This option also disables the deployment for endpoints yet to retrieve.

4. Define the **Notifications defaults** options.

Complete the following substeps.

Tip: You can type a maximum of 1000 characters in each field.

a) Select or clear the **User notification should always be on top** check box.

This option forces all notification dialogs to display on top of other windows.

b) Type the desired message in the **Manual installation** field.

This option defines the default message that displays when an endpoint receives a package requiring manual installation.

c) Type the desired message in the **May reboot** field.

This option defines the default message that displays when an endpoint receives a package that may require the recipient to reboot.

d) Type the desired message in the **Default deployment message** field.

This option defines the default message that displays with a deployment notification.

e) Type the desired message in the **Default reboot message** field.

This option defines the default message that displays with a reboot notification.

5. Define the **User Interface** option.

Select a **How should Deployment Wizard Start Times be displayed?** option.

- Agent Local Time (Deploy at local time for each individual node)
- Agent UTC Time (Deploy at UTC time for each individual node)

6. Click **Save**.

Result: The ***Deployments*** tab configuration is saved.

Exporting Option Data

To export the options settings that are listed on any ***Options*** page tab to a comma separated value (.csv) file, click the **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

Defining Access Rights

After Patch and Remediation is installed, new access right are added to the system. When creating new roles or editing existing ones, you can assign these new Patch and Remediation access rights.

To edit your roles, open the ***Users and Roles*** page (**Tools** > **Users and Roles**), select the ***Roles*** tab, and create a new role or edit an existing one.

Note: New access rights are added when you install new modules.

Access Right	Description	Access
All		
Dashboard		
View Dashboard	Access to view the home page dashboard.	
View Current Status	Access to view the status of the server.	
View AV Widgets	Access to select and view the AntiVirus Dashboard widgets.	
View LAC Widgets	Access to select and view the Application Control Dashboard widgets.	
View PR Widgets	Access to select and view the Patch and Remediation Dashboard widgets.	
View DC Widgets	Access to select and view the Device Control Dashboard widgets.	
View MDM Widgets	Access to select and view the Mobile Device Management Dashboard widgets.	
Jobs		
View Discovery Scan Jobs	Access to view discovery scan jobs.	
Create Discovery Scan Jobs	Access to create and copy discovery scan jobs	
View Agent Management Jobs	Access to view agent management jobs.	
Create Agent Management Jobs	Access to create and copy agent management jobs.	

Access Right	Description	Access
Manage Modules via Jobs	Access to install or uninstall agent modules using agent management jobs.	
Manage Jobs	Cancel, pause, resume, delete or merge all jobs the user has access to.	
Export Jobs	Export the jobs list.	
Vulnerabilities/Patch Content		
View Content	Access to vulnerability and other content data.	
Manage Content	Enable and disable vulnerabilities and other content.	
Export Content	Export vulnerability and other content data list.	
View Content Details	Access the detailed information for vulnerabilities and other content data.	
View My Custom Patch Lists	Access to view custom patch lists that this user has created.	
View All Custom Patch Lists	Access to view custom patch lists that all users have created.	
Manage Custom Patch Lists	Edit, delete or copy custom patch lists that this user has access to.	
Logs		
View Application Control Event Logs	Access to view reports containing application execution content.	
Manage Application Control Event Logs	Access to create reports containing application execution content.	
Export Application Control Event Logs	Access to export reports containing application execution content.	
View Dev Ctl Event Logs	Access to view logs containing device usage events.	
Manage Dev Ctl Event Log Queries	Access to create, edit, and delete device control log queries.	
Export Dev Ctl Event Logs	Access to export logs containing device usage events.	

Access Right	Description	Access
View Device Control Audit Logs	Access to view reports containing device control audit events.	
Manage Device Control Audit Logs	Access to manage reports containing device control audit events.	
Export Device Control Audit Logs	Access to export reports containing device control audit events.	
Alerts & Centralized Quarantine		
View AV alerts	Access to view AntiVirus Virus and Malware Event Alerts page.	
Manage AV alerts	Access to delete AntiVirus alerts.	
Export AV alerts	Access to export AntiVirus alerts.	
View AV Centralized Quarantine	Access to view AntiVirus Centralized Quarantine page	
Manage AV Centralized Quarantine	Access to delete and restore files from Centralized Quarantine	
Endpoints		
View Endpoints	Access the manage endpoints all tab.	
Manage All Tab	Enable and disable agents, delete endpoints, manage agent modules, and wake endpoints.	
Export All Tab	Export the all tab endpoints list.	
Manage Remotely	Access the remote management options available.	
View AV Tab	Access the AntiVirus tab.	
Manage AV Tab	Install, uninstall, enable and disable the AntiVirus module.	
Export AV Tab	Export the AntiVirus tab endpoints list.	
View LAC Tab	Access the Application Control tab.	
Manage LAC Tab	Install, uninstall, enable and disable the Application Control module.	
Export LAC Tab	Export the Application Control tab endpoints list.	

Access Right	Description	Access
View PR Tab	Access the Patch and Remediation tab.	
Manage PR Tab	Install, uninstall, enable and disable the Patch and Remediation module.	
Export PR Tab	Export the Patch and Remediation tab endpoints list.	
View DC Tab	Access the Device Control tab.	
Manage DC Tab	Install, uninstall, enable and disable the Device Control module.	
Export DC Tab	Export the Device Control tab endpoints list.	
Download Agent Installers	Access to the Download Agent Installers page.	
Manage Agent Version	Access to the Manage Agent Version dialog.	
Scan Now Discover Applicable Updates	Scan endpoints using the DAU Scan Now Dropdown/button.	
Scan Now Virus and Malware Scan	Scan endpoints using the AntiVirus Scan Now Dropdown/button.	
Reboot Endpoints	Reboot endpoints using the Reboot Now button.	
Inventory		
View Inventory	View the endpoint inventory.	
Export Inventory	Export the endpoint inventory list.	
Groups		
View Groups	Access the groups.	
Manage Groups	Add, edit, enable, disable, and delete groups.	
Export Groups	Export the groups list.	
Users		
View Users	Access the user groups.	
Manage Users	Add or remove users from individual user policies.	
Export Users	Export the user groups list.	

Access Right	Description	Access
Deployments and Tasks		
Create Deployments	Ability to create new deployments.	
View My Deployments and Tasks	Access the deployments and tasks that this user has created.	
View All Deployments	Access the deployments that all users have created.	
View All Virus and Malware scan tasks	Access the Virus and Malware Scan Now tasks that all users have created.	
Manage Deployments and Tasks	Deploy, enable, disable, abort, and delete deployments and tasks that this user has access to.	
Export Deployments and Tasks	Export the deployments and tasks in the list that this user has access to.	
Packages		
View Packages	Access the package data.	
Manage Packages	Create, edit, and delete packages.	
Export Packages	Export the package data list.	
Cache Packages	Ability to download packages from the GSS onto the local machine.	
Agent Policy Sets		
View All Agent Policy Sets	Access the agent policy sets.	
Manage All Agent Policy Sets	Create, edit and delete agent policy sets.	
Export All Agent Policy Sets	Export the agent policy sets list.	
AntiVirus Policies		
View centralized AV Policies	View AntiVirus policies centrally.	
Manage centralized AV Policies	Create, edit, enable, disable, and delete centralized AntiVirus policies.	

Access Right	Description	Access
Assign and remove centralized AV Policies	Assign and remove centralized AntiVirus policies.	
Export centralized AV Policies	Export centralized AntiVirus policy list.	
View Group/Endpoint AV Policies	View AntiVirus policies at user-assigned groups and endpoints.	
Manage Group/ Endpoint AV Policies	Create, edit, enable, disable, and delete AntiVirus policies from user-assigned groups and endpoints.	
Assign Group/Endpoint AV Policies	Assign and remove AntiVirus policies from user-assigned groups and endpoints.	
Export Group/Endpoint AV Policies	Export AntiVirus policy lists for user-assigned groups and endpoints.	
Application Control Policies		
View Group/Endpoint/ Users AC Policies	View Application Control policies in the context of groups, endpoints, and users.	
Manage Group/ Endpoint AC Policies	Create Application Control policies in the context of groups and endpoints.	
Assign Group/Endpoint AC Policies	Assign and unassign Application Control policies in the context of groups and endpoints (unassign only for users).	
Export Group/Endpoint/ Users AC Policies	Export Application Control policy lists in the context of groups, endpoints, and users.	
View Centralized AC Policies	View Application Control policies centrally.	
Manage Centralized AC Policies	Create, edit, enable, disable, copy, and delete centralized Application Control policies.	
Assign Centralized AC Policies	Assign and remove centralized Application Control policies.	
Export Centralized AC Policies	Export centralized Application Control policy list.	
Device Control Policies		
View Group/Endpoint/ User DC Policies	View Device Control policies in the context of groups, endpoints, and users.	

Access Right	Description	Access
Manage Group/ Endpoint/User DC Policies	Create Device Control policies in the context of groups, endpoints, and users.	
Assign Group/ Endpoint/User DC Policies	Assign and unassign Device Control policies in the context of groups, endpoints, and users.	
Export Group/Endpoint/ User DC Policies	Export Device Control policy list in the context of groups, endpoints, and users.	
View Centralized DC Policies	View Device Control policies in **Manage** > **Device Control Policies**.	
Manage Centralized DC Policies	Create, edit, enable, disable, and delete Device Control policies in **Manage** > **Device Control Policies**.	
Assign Centralized DC Policies	Assign and unassign Device Control policies in **Manage** > **Device Control Policies**.	
Export Centralized DC Policies	Export Device Control policy list in **Manage** > **Device Control Policies**.	
Mobile Policies		
View Group/Endpoint/ User Mobile Policies	View MDM policies in the context of groups, endpoints, and users.	
Manage Group/ Endpoint/User Mobile Policies	Create MDM policies in the context of groups, endpoints, and users.	
Assign Group/ Endpoint/User Mobile Policies	Assign and unassign MDM policies in the context of groups, endpoints, and users.	
Export Group/Endpoint/ User Mobile Policies	Export MDM policy list in the context of groups, endpoints, and users.	
Application Library		
View Application Library	Access to view the application library page.	
Manage Application Library	Access to create, edit, move, delete, assign and remove applications / application groups.	
Export Application Library	Access to export application information from application library.	

Access Right	Description	Access
Security Configuration Management		
View SCM Data	Access to view SCM data on the endpoint detail and groups views.	
Reports		
Reports Administer	Generate reports regardless of access rights for groups and endpoints.	
View My Core Reports	Generate core reports only for those items this user has access to.	
View My AV Reports	Generate AntiVirus reports only for those items this user has access to.	
View My PR Reports	Generate Patch and Remediation reports only for those items this user has access to.	
View My LAC Reports	Generate Application Control reports only for those items this user has access to.	
View My PM Reports	Generate PM reports only for those items this user has access to.	
View My DC Reports	Generate Device Control reports only for those items this user has access to.	
Export Reports	Export the generated reports.	
Configure Enterprise Reporting (ER)	Configure settings to manage Configure Enterprise Reporting (ER)	
Users/Roles		
View Users	Access the users and roles list view.	
Manage Users	Create, delete, enable, and disable users and roles.	
Export Users	Export the users and roles list.	
Change Password	Ability to change the password for users other than themselves.	
Manage Server Modules		
Installation Manager	Access the Installation Manager to install, update and uninstall server modules.	

Access Right	Description	Access
Subscriptions		
View Subscription	Access the subscription service information.	
Manage Subscription	Edit or update subscription service updates.	
Export Subscription	Export the subscription service information.	
Directory/Computer Synchronization		
View Directory Sync Schedule	Access to view the active directory sync schedule page.	
Manage Directory Sync Schedule	Create, edit, delete, enable, disable directory syncs.	
Export Directory Sync Schedule	Export the directory sync schedule lists.	
Device Control Tools and Options		
Recover Password	Access the **Tools** > **Device Control** > **Recover Password** function.	
Grant Temporary Permissions	Access the **Tools** > **Device Control** > **Grant Temporary Permissions** function.	
Email notifications		
View Email Notifications	Access the email notifications page.	
Manage Email Notifications	Create and edit email notifications and settings for core feature. Note: All types of notifications may be deleted with this right.	
Manage AV Email Notifications	Create and edit AntiVirus email notifications and settings.	
Manage PR Email Notifications	Create and edit Patch and Remediation email notifications and settings. Note: All types of notifications may be deleted with this right.	
Export Email Notifications	Export the emails notifications list.	
Options		
View Options	Access to general, agent and deployment default server options.	

Access Right	Description	Access
Manage Options	Set and edit general, agent and deployment default server options.	
Export Options	Export the options list.	
View Global DC Options	View Device Control tab of the **Tools** > **Options** page.	
Manage Global DC Options	Manage the settings on the Device Control tab of the **Tools** > **Options** page.	
View MDM Options	View Mobile Mgmt tab of the **Tools** > **Options** page.	
Manage MDM Options	Manage the settings on the Mobile Mgmt tab of the **Tools** > **Options** page.	
Technical Support		
View Technical Support	Access the technical product support information.	
Export Technical Support	Export the technical product support information.	
Licenses		
View Licenses	Access the product licenses.	
Manage Licenses	Update product licenses.	
Export Licenses	Export the product license information.	
Device Library		
View DC Library	Access to view the Device Control library.	
Manage DC Library	Access to create, edit, move, delete, and assign Device Control Library collections.	
Export DC Library	Access to export Device Control information from library.	

Chapter 5

Configuring Notifications

In this chapter:

Ivanti Endpoint Security contains several features to notify users of system events and Global Subscription Service updates.

- Patch and Remediation adds new Email Notifications related to content and deployments. For additional information, refer to The Email Notifications Page on page 104.
- You can subscribe to an RSS feed that notifies you when new content is posted to the Global Subscription Service. For additional information, refer to GSS Notifications on page 115.

The Email Notifications Page

You can configure your server to send email notifications when certain system events occur. These notifications alert you when the system requires administration.

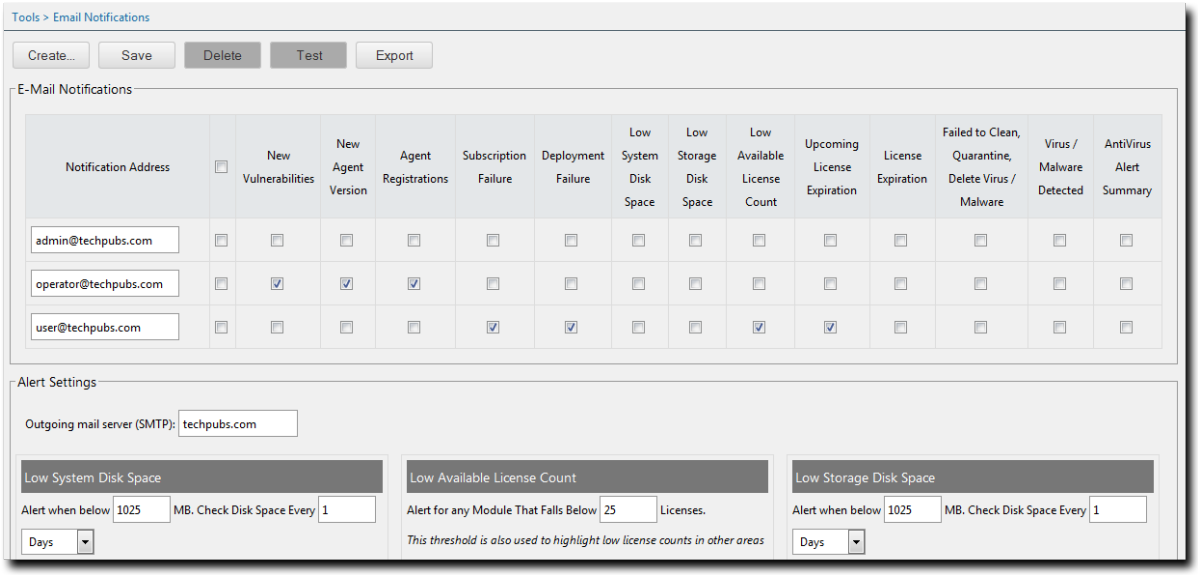


Figure 29: Email Notifications Page

From this page, you can perform the following actions:

- Define your mail server.
- Define email notification alert settings
- Define email addresses to receive notifications.
- Select email notifications

To open this page, select **Tools** > **Email Notifications** from the navigation menu.

Email Notification Page Buttons

These buttons let you use functions available on the ***Email Notification*** page.

Table 56: Email Notification Page Buttons

Button	Function
Create...	Creates a new item to **Email Notifications**. For additional information, refer to Creating Email Notifications on page 112.
Save	Saves any page edits made.

Button	Function
Delete	Deletes selected items from **Email Notifications**. For additional information, refer to Deleting Email Notification Addresses on page 113.
Test	Sends a test email to selected email addresses. For additional information, refer to Testing Email Notifications on page 113.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Email Notifications Table

This table lists the email addresses that receive system alerts. You can also use this table to define a limitless number of addresses. The alert types sent to each email address can be customized.

Installation of the Patch and Remediation modules adds new notifications:

- **New Vulnerabilities**, which alerts when new content items are available for deployment.
- **Deployment Failure**, which alerts when a deployment fails.

For additional information about the other email notifications, refer to *The Email Notifications Table* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Installation of the AntiVirus modules adds new notifications:

- **Failed to Clean, Quarantine, Delete Virus / Malware**, which alerts when virus and malware actions fail on endpoints.
- **Virus / Malware Detected**, which alerts when virus and malware instances are detected on endpoints.
- **AntiVirus Alert Summary**, which sends a daily or weekly status e-mail containing a summary of all alerts.

For additional information about the other email notifications, refer to *The Email Notifications Table* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Table 57: E-Mail Notification Table

Column	Description
Notification Address	Lists the email address that receives alert notifications. This address is not validated.
New Vulnerabilities (Patch and Remediation only)	Alerts when a new content item becomes available for deployment.

Column	Description
New Agent Version	Alerts when a new version of the agent is downloaded.
Agent Registrations	Alerts when an agent successfully registers or attempts and fails to register with the server.
Subscription Failure	Alerts when any subscription replication fails.
Deployment Failure (Patch and Remediation only)	Alerts when a deployment fails.
Low System Disk Space	Alerts when the available system drive space on the server falls below the defined minimum.
Low Storage Disk Space	Alerts when the available storage space on the drive where content is stored falls below the defined minimum.
Low Available License Count	Alerts when the number of licenses available to the server falls below the defined minimum.
Upcoming License Expiration	Alerts when licenses will expire within the defined time frame.
APNS Certificate Expiration	Alerts that the APNS certificate used to send iOS devices push notifications is going to expire. Emails are sent at the following intervals at time of replication: • 30 days to expiration • 14 days to expiration • 7 days to expiration • After 7 days, once every 24 hours until the certificate is renewed.
License Expiration	Alerts when a license expires.
Failed to Clean, Quarantine, Delete Virus/ Malware (AntiVirus only)	Alerts when AntiVirus fails to clean, quarantine, or delete a detected virus or malware.
Virus/Malware Detected (AntiVirus only)	Alerts when a virus or malware has been detected on a network endpoint.
Antivirus Alert Summary (AntiVirus only)	Alerts when an AntiVirus alert summary has been completed.

Note: Check boxes only display in **Email Notifications** after you create an email notifications entry.

Alert Settings

Alert settings are values that trigger notification emails. These values are defined from the **Alert Settings** options. Edit these values to suit your network.

The following table describes the **Alert Settings** options.

Table 58: Alert Settings Options

Option	Definition	
Outgoing Mail Server (SMTP)	The mail host used to send emails. **Note:** The **Outgoing Mail Server (SMTP)** is not an alert value setting. However, completion of this field with your network SMTP server is required to send email notifications.	
Low System Disk Space	Defines the threshold that initiates email notifications due to low system disk space.	
	Alert When Below *x* MB	Defines the level of system disk space that your server must drop below before an alert is sent (1-99999 MBs [97.65 GB]).
	Check Disk Every *x Interval*	Defines the interval between **Low System Disk Space** threshold checks. This interval is defined in minutes, hours, or days (1-999).
Low Storage Disk Space	Defines the threshold that initiates email notifications due to low storage disk space.	
	Alert When Below *x* MB	Defines the level of storage disk space that your server must drop below before an alert is sent (1-99999 MBs [97.65 GB]).
	Check Disk Every *x Interval*	Defines the interval between **Low Storage Disk Space** threshold checks. This interval is defined in minutes, hours, or days (1-999).

Option	Definition	
Low Available License Count	Defines the threshold that initiates email notifications due to low available license count.	
	Alert for any Module That Falls Below *x* Licenses	Defines the number of available licenses that your server must drop below before an alert is sent (1-999).
	While License Count Remains Low, Send a Reminder E-mail Every *x* Days	Defines if an alert is sent and the interval in days (1-99).
Upcoming License Expiration	Defines the threshold that initiates email notifications due to upcoming license expiration.	
	Alert for any License That Will Expire Within *x* Days	Defines the number of days before an alert is generated due to upcoming license expiration (1-99).
	While Licenses Aren't Renewed After This Alert, Send a Reminder E-mail Every *x* Days	Defines if an alert is sent and the interval in days (1-99).
Failed to Clean, Quarantine, Delete Virus/ Malware (AntiVirus only)	Defines the threshold that initiates email notifications due to virus/ malware cleanse, quarantine, deletion failures.	
	Notify When at Least *x* Virus/Malware Actions Failed Across All Endpoints	Defines the number of virus/malware action failures that must occur before an alert is generated. The default is value is 10.
	Notify When Affecting at Least *x* Endpoints	Defines the number of endpoints upon which virus/malware action failures must occur upon before an alert is generated. The default value is 1.
	Notify When Within a Period of *x Interval*	Defines the time period within a defined number of virus/malware action failures must occur within before an alert is generated. The default value is 60 minutes.
	Send This Email Notification at Most Once Every *x Interval*	Defines the time period over which an alert is generated. The default value is once every 60 minutes.

Option	Definition	
Virus/Malware Detected (AntiVirus only)	Defines the threshold that initiates email notifications due to virus/malware detection. Define the following options:	
	Notify When at Least *x* Instances of Virus/Malware are Detected Across All Endpoints	Defines the number of virus/malware instances that must be detected before an email is generated. The default value is 100.
	Notify When Affecting at Least *x* Endpoints	Defines the number of endpoints that must be affected with viruses/malware before an email is generated. The default value is 20.
	Within a Period of *x Interval*	Defines the time period in which viruses/malware are detected before an email is generated. The default value is 4 hours.
	Send This Email Notification at Most Once Every *x Interval*	Defines the time period over which an alert is generated. The default value is 8 hours.
Antivirus Alert Summary (AntiVirus only)	Defines the threshold that initiates email notifications of AntiVirus alert summaries. The default is once a day at 9:00 AM (server time). Select one of the following options:	
	Send Status Email Once a Day at *Time*	Selection of this option sends alerts that summarize your network antivirus status once a day at the selected time.
	Send Status Email Once a Week on *Day* at *Time*	Selection of this option sends alerts that summarize your network antivirus status once a week on a selected day and time.

Thresholds define the value that trigger email notifications, but not email notifications themselves. Email notifications are sent following Discover Applicable Updates tasks that find values below the defined thresholds.

Working with Email Notifications

From the ***Email Notifications*** page, you can define the email addresses that receive notifications. You can also define the events and values that trigger notification emails.

Configuring Alert Settings

Alert settings are values that trigger the Ivanti Endpoint Security server to send email notifications. Define these values for preventive maintenance purposes.

Define alert settings from the ***Email Notifications*** page.

1. From the **Navigation Menu**, select **Tools** > **Email Notifications**.
2. In the **Outgoing Mail Server (SMTP)** field, type the name of your outgoing mail server.

   Note: The outgoing mail server is not an alert setting value, but is necessary to define email notification addresses.

3. Define the **Low System Disk Space** options.

   This alert setting defines when email notifications are sent due to low system disk space.

   a) Type a value in the **Alert When Below *x* MB** field (1-99999).
   b) Type a value in the **Check Disk Space Every *x Interval*** field (1-999).
   c) Select an interval from the **Check Disk Space Every *x Interval*** list (**Minute(s)**, **Hours**, **Days**).

4. Define the **Low Storage Disk Space** options.

   This alert setting defines when email notifications are sent due to low storage disk space.

   a) Type a value in the **Alert When Below *x* MB** field (1-99999).
   b) Type a value in the **Check Disk Space Every *x Interval*** field (1-999).
   c) Select an interval from the **Check Disk Space Every *x Interval*** list (**Minute(s)**, **Hours**, **Days**).

5. Define the **Low Available License Count** options.

   This alert setting defines the number of available licenses that Ivanti Endpoint Security must drop below before an email notification is generated.

   a) Type a value in the **Alert for any Module That Falls *x* Licenses** field. (1-999).
   b) If applicable, select the check box and type a value in the **While License Count Remains Low, Send a Reminder Email Every *x Interval*** field (1-99).

6. Define the **Upcoming License Expiration** options.

   This alert setting defines the number of days before an email notification is generated to upcoming license expiration.

   a) Type a value in the **Alert for any Licenses That Will Fall Within *x* Days** field (1-99).
   b) If applicable, select the check box and type a value in the **While Licenses Aren't Renewed After This Alert, Send a Reminder Email Every *x Interval*** field. (1-99).

7. Define the **Failed to Clean, Quarantine, Delete Virus/Malware** options.

   This alert setting defines the threshold that initiates email notifications due to virus/malware cleanse, quarantine, deletion failures.

   a) Type a value in the **At least *x* Virus/Malware Actions Failed Across All Endpoints** field.
   b) Type a value in the **Affecting at Least *x* Endpoints** field.
   c) Type a value in the **Within a Period *x Interval*** field.
   d) Select a value from the **Within a Period *x Interval*** list (**Minutes**, **Hours**, **Days**).
   e) Type a value in the **Send This Email Notification at Most Once Every *x Interval*** field.
   f) Select a value from the **Send This Email Notification at Most Once Every *x Interval*** list (**Minutes**, **Hours**, **Days**).

8. Define the **Virus/Malware Detected** options.

   This alert setting defines the threshold that initiates email notifications due to detected viruses/malware.

   a) Type a value in the **At least *x* Instances of Virus/Malware Are Detected Across All Endpoints** field.
   b) Type a value in the **Affecting at Least *x* Endpoints** field.
   c) Type a value in the **Within a Period of *x Interval*** field.
   d) Select a value from the **Within a Period of *x Interval*** list (**Minutes**, **Hours**, **Days**).
   e) Type a value in the **Send This Email Notification at Most Once Every *x Interval*** field.
   f) Select a value from the **Send This Email Notification at Most Once Every *x Interval*** list (**Minutes**, **Hours**, **Days**).

9. Select an **Antivirus Alert Summary** option.

   Complete one of the following sets of substeps to select an option.

Option	Steps
To send status emails daily:	1. Select the **Send Status Email Once a Day at *time*** option. 2. Type a time in the **Send Status Email Once a Day at *time*** field in the following format: `hh:mm AM/PM`.

Option	Steps
To send status emails weekly:	1. Select the **Send Status Email Once a Day at *time*** option. 2. Select a day from the **Send Status Email Once a Week on *day*** list. 3. Type a time in the **Send Status Email Once a Week on *time*** field in the following format: `hh:mm AM/PM`.

10. Click **Save**.

Result: Your alert setting values are saved.

Creating Email Notifications

You can configure your mail server to alerts to people when system events occur. Define email notification recipients for preventative maintenance and administrative purposes.

Prerequisites:

Complete Configuring Alert Settings on page 110.

Create email notifications from the ***Email Notifications*** page.

1. From the **Navigation Menu**, select **Tools** > **Email Notifications**.
2. Click **Create**.

   Step Result: A new row displays in the **Email Notifications** table.
3. Type an email address in the **Notification Address** field of the new row.

   Note: The server does not validate email addresses.
4. Select the email notifications you want the address to receive.
5. Click **Save**.

Result: The email address and the selected notifications are saved. The address will receive a notification when system events occur.

Editing Email Notification Addresses

After an email notification address is created, you can edit the email address itself, or you can change notification types it receives.

Edit email notification addresses from the ***Email Notifications*** page.

1. From the **Navigation Menu**, select **Tools** > **Email Notifications**.
2. From the **Notification Address** column, edit the desired email address fields.
3. Select or clear **E-Mail Notification** check boxes.

4. Click **Save**.

Deleting Email Notification Addresses

Delete email notification addresses that no longer need notification of Ivanti Endpoint Security events.

Delete email notification recipients from the ***Email Notifications*** page.

1. From the **Navigation Menu**, select **Tools** > **Email Notifications**.
2. Select the notification addresses that you want to delete.

   Step Result: The **Delete** button become active.

3. Click **Delete**.

   Step Result: The ***Message from webpage*** opens indicating the selected recipients have been removed.

4. Click **OK**.

Result: The notification address is deleted. An email that confirms the deletion is sent to the selected email addresses. Afterward, notification emails are not longer sent.

Exporting Email Notification Data

You can export email notification data to a comma separated value (`.csv`) file for reporting and analytical purposes.

All data on the page is exported. To export email notification data, select **Tools** > **Email Notifications** and click **Export**. For additional information, refer to Exporting Data on page 47.

Testing Email Notifications

Testing email notifications ensures that defined email addresses and Ivanti Endpoint Security are properly configured for alerts. If a test fails, you should first verify that the email address is typed correctly in the **Email Notifications** table. If it is, you should then examine email and Ivanti Endpoint Security settings.

Prerequisites:

An email address must be added to the **Email Notifications** table.

Test email notifications from the ***Email Notifications*** page.

1. From the **Navigation Menu**, select **Tools** > **Email Notifications**.
2. Select the notification address(es) that you want to test.

   Step Result: The **Test** button become active.

   Tip: When the **Select All** check box is selected, all items become checked within the list and the **Test** button becomes active.

3. Click **Test**.

Result: A notification informs you that the test email was sent. Acknowledge the notification by clicking **OK**. Access the applicable email address to ensure the notification was successful.

APNS Renewal Alerts

Environments supporting iOS devices requires an APNS (Apple Push Notification Service) certificate, which must be renewed annually.

The When your APNS certificate expiration is approaching, The Ivanti Endpoint Security Web console notifies you of upcoming APNS certificate expiration several ways:

- The console displays a system alert for the upcoming certificate expiration.
  - The alert first displays within seven days of expiration.
  - The alert displays over all Mobile Device Management pages.
  - The alert displays daily until you renew the certificate.

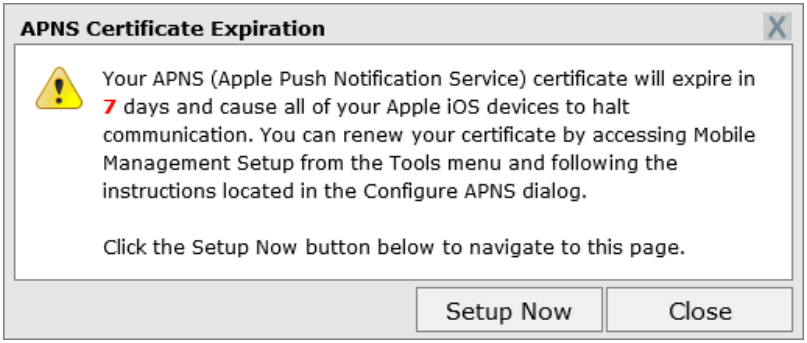


Figure 30: APNS Certificate Expiration Alert

- The ***Mobile Management Setup*** page displays an alert in **Configure you Apple Push Notification Services (APNS) Certificates for iOS devices**.

Figure 31: Mobile Management Setup Page Alert

These alerts can be resolved by renewing your APNS certificate. From **Configure your Apple Push Notification Services (APNS) Certicates for the iOS devices** on ***Mobile Management Setup*** page,

click **APNS** and use the dialog to complete the renewal process. For step-by-step instructions, see Renewing Your APNS Certificate.

GSS Notifications

Ivanti hosts a website that lists updates posted to the Global Subscription Service.

You can view these updates at http://gssnews.lumension.com/news/default.aspx?oem=Lumension .

Tip: Subscribe to the page RSS feed to receive regular GSS notifications.

Chapter 6

Licensing, Subscriptions, and Support

In this chapter:

While using Ivanti Endpoint Security (Ivanti Endpoint Security), you may need to request technical support or view information about your Ivanti Endpoint Security licenses.

View licensing information from the The Product Licensing Page on page 123. This page lists the Ivanti Endpoint Security modules you are licensed for.

View your subscription history from the The Subscription Updates Page on page 126. This page lists a history of replications with the Global Subscription Service.

Request technical support from the The Technical Support Page on page 118. From this page you can request technical support and review technical information about your Ivanti Endpoint Security server.

The Technical Support Page

This page contains links to various technical support pages. You can also use this page to give Ivanti feedback for future product releases.

This page also lists system data about your Ivanti Endpoint Security Server.

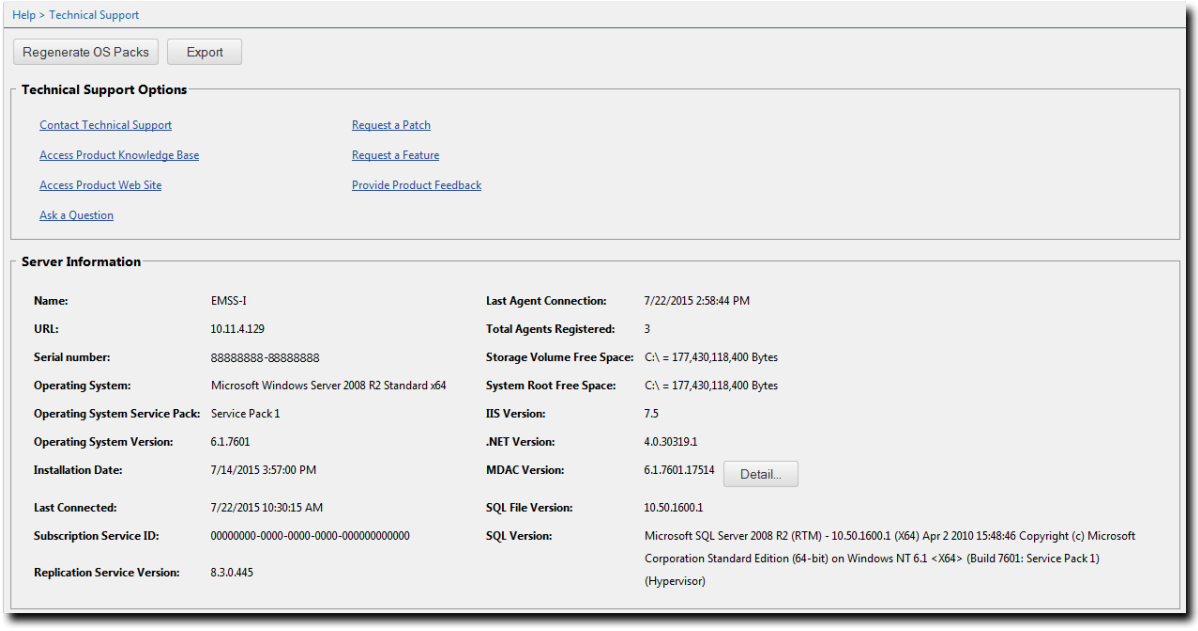


Figure 32: Technical Support Page

Viewing the Technical Support Page

Navigate to this page to access out-of-program technical support pages.

1. From the **Navigation Menu**, select **Help** > **Technical Support**.
2. Review the page.

Technical Support Page Buttons

The ***Technical Support*** page features a button to download the most recent OS packs. OS packs are files used detect operating systems.

The following table describes each button.

Table 59: Technical Support Page Buttons

Button	Function
Regenerate OS Packs	Regenerates and synchronizes the relevant information for each of the operating systems supported by Ivanti Endpoint Security. For additional information, refer to Regenerating OS Packs on page 122.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Detail...	Opens a dialog that displays a detailed list of Microsoft Directory Access Components product and file versions. For additional information, refer to MDAC File Version Information on page 121.

Technical Support Options

Ivanti provides access to various out-of-program technical support pages. Use these pages to communicate with Ivanti. Click each link to open a new window to a support page.

Contact Technical Support	When having difficulty using Ivanti Endpoint Security or any of its modules, send an email to Ivanti technical support to open a ticket. Support staff will help you resolve your issues.
Access Product Knowledge Base	The Ivanti Knowledge Base contains release notes for release notes, defects, hotfixes, frequently asked questions, how-to procedures, and troubleshoot information for the Ivanti software portfolio.
Access Product Web Site	The Ivanti corporate Web site for Ivanti Endpoint Security includes information about its software portfolio and how it can benefit your enterprise. It also contains helpful information about how to identify and prevent IT security issues.
Ask a Question	If you have questions about Ivanti Endpoint Security or other Ivanti software, contact us.
Request a Patch	If you need a patch to keep your enterprise secure, send a message using our feature request page.

Request a Feature	If you want a new feature to improve your Ivanti Endpoint Security user experience, send them using our feature request page.
Provide Product Feedback	Ivanti uses customer feedback to improve Ivanti Endpoint Security. If you have an idea to improve it, see our customer feedback Web page.

Server Information

These fields list general information regarding the Ivanti Endpoint Security server.

The following table describes the **Server Information** fields.

Table 60: Server Information Fields

Field	Description
Name	The name of the server Ivanti Endpoint Security (Ivanti Endpoint Security) is installed on.
URL	The URL of the server Ivanti Endpoint Security is installed on.
Serial Number	The serial number used by Ivanti Endpoint Security.
Operating System	The operating system installed and running on the Ivanti Endpoint Security server.
Operating System Service Pack	The service pack applied to the operating system, if applicable.
Operating System Version	The operating system version number.
Installation Date	The date and time Ivanti Endpoint Security was installed.
Last Connected	The date and time Ivanti Endpoint Security last connected to the Global Subscription Service (GSS).
Subscription Service ID	The ID assigned to Ivanti Endpoint Security upon registration with the GSS.
Replication Service Version	The replication service version number.
Last Agent Connection	The date and time a registered Ivanti Endpoint Security Agent last connected to the Ivanti Endpoint Security server.
Total Agents Registered	The total number of agents registered with Ivanti Endpoint Security.
Storage Volume Free Space	The amount of free disk space on your storage volume.
System Root Free Space	The amount of free disk space on your system volume.
IIS Version	The Internet Information Services (IIS) version installed.
.NET Version	The .NET Framework version(s) installed.

Field	Description
MDAC Version	The Microsoft Data Access Components (MDAC) version. The **Detail** button adjacent to the field opens the ***MDAC File Version Information*** dialog.
SQL File Version	The SQL Server file version installed.
SQL Version	The SQL Server version number followed by detailed information.

Viewing the MDAC File Version Information Dialog

Navigate to this dialog to view MDAC file version information.

You can access this dialog from the ***Technical Support*** page.

1. From the **Navigation Menu**, select **Help** > **Technical Support**.
2. Click **Detail**.

   Step Result: The ***MDAC File Version Information*** dialog opens.

3. View the MDAC file version data.

MDAC File Version Information

The ***MDAC File Version Information*** dialog lists the individual `.dll` files included within the version of Microsoft Data Access Components (MDAC) installed on your Ivanti Endpoint Security server. To open this dialog, click the **Detail** button within **Component Version Information**.

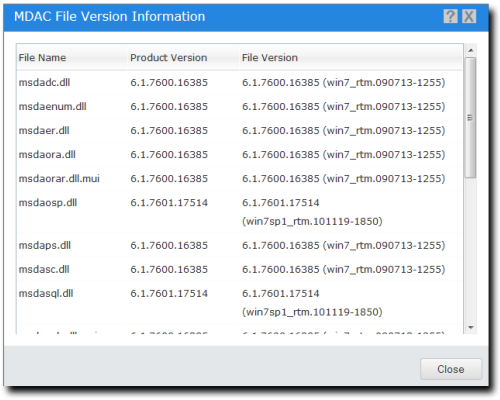


Figure 33: MDAC File Version Information Dialog

The following table describes the contents of the ***MDAC File Version Information*** dialog.

Table 61: MDAC File Version Information

Column	Description
File Name	The name of the MDAC `.dll` file.

Column	Description
Product Version	The product version number of the file.
File Version	The file version number of the file.

Suite Version Information

Suite Version Information displays the version number of Ivanti Endpoint Security (Ivanti Endpoint Security), each platform component installed, and each module component installed.

The following table describes each **Suite Version Information** field.

Table 62: Suite Version Information Fields

Field	Description
Server Suite Version	The version number of Ivanti Endpoint Security installed on your Ivanti Endpoint Security server.
Core Version	The version number of the Ivanti Endpoint Security core installed on your Ivanti Endpoint Security server.
***Module* Version**	The name and version number of a Ivanti Endpoint Security module installed on your Ivanti Endpoint Security server. A field appears for each module installed on your server.

Regenerating OS Packs

This task re-generates the file used during Discover Applicable Updates tasks that determines if patches apply to an endpoint. You'll rarely need to regenerate OS packs because this process occurs during the daily replication. You'll likely only use this process for troubleshooting purposes.

Regenerate OS packs from the ***Technical Support*** page.

1. From the **Navigation Menu**, select **Help** > **Technical Support**.
2. Click **Regenerate OS Packs**.

   Step Result: A dialog displays, asking you to acknowledge the regeneration.
3. Click **OK**.

   Step Result: A dialog displays, asking you to acknowledge that the regeneration has been scheduled.
4. Acknowledge the scheduling by clicking **OK**.

Result: The OS pack regeneration is scheduled. It runs the next time the server communicates with the Global Subscription Service. During regeneration, no Discover Applicable Updates tasks occur.

Exporting Technical Support Data

You can export the data listed on the ***Technical Support*** page for reporting and analytical purposes.

Exported data includes **Technical Support Options**, **Server Information**, and **Suite Version Information**. To export this data, select **Help** > **Technical Support** and click **Export**. For additional information, refer to Exporting Data on page 47.

The Product Licensing Page

Use this page to view, validate, and export license information. It summarizes product component licenses applicable to your endpoint management activities. After you purchase Mobile Device Management, an item for the module is added to the page list.

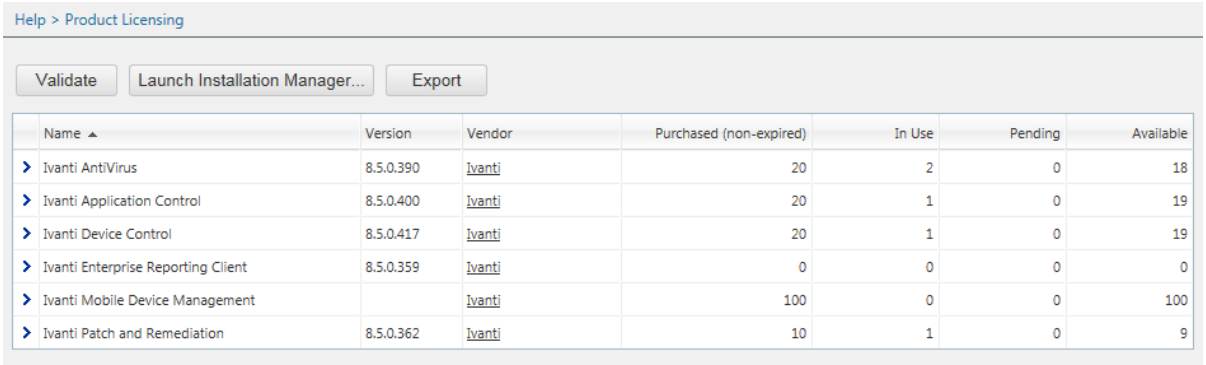


Figure 34: Product Licensing Page

Open this page by selecting **Help** > **Product Licensing**.

Product information is updated during daily replication with the Global Subscription Service. Additionally, the page lists how many endpoint licenses you have, how many of those licenses are in use, and how many of those licenses are available.

Viewing the Product Licensing Page

Navigate to this page to view information about license validity and daily replication.

1. From the **Navigation Menu**, select **Help** > **Product Licensing**.
2. View your product license data.

The Product Licensing Page Buttons

Use page buttons to initiate license replications or open Ivanti Installation Manager. Ivanti recommends initiating license replication after installing a new module.

The following table describes each button.

Table 63: Product Licensing Page Buttons

Button	Function
Validate	Initiates license replication. For additional information, refer to Initiating Subscription License Replication on page 125.
Launch Installation Manager...	Opens Ivanti Installation Manager. For additional information, refer to Using Ivanti Installation Manager Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Product Licensing Page List

This list itemizes licensing information for each Ivanti Endpoint Security module. View this table for an overview of license availability.

Table 64: Product Licensing Page List

Column	Description
Name	The product module name.
Version	The product module version number.
Vendor	The source of the license. Click the link to open the vendor home page.
Purchased (non-expired)	The total number of licenses purchased for the module that haven't expired.
In Use	The number of licenses in use for the module.
Pending	The number of licenses pending use or removal for the module.
Available	The number of licenses available for the module.

The list item for each product module can be expanded to display license group information. License groups are blocks of licenses purchased at a time. For example, you may have 3 license groups comprising 500 total licenses. Initially, a group of 300 licenses was purchased, and then 2 additional groups of 100 licenses were added during subsequent purchases.

To expand a list item, click its arrow (**>**).

Table 65: Expanded Product Licensing List Item

Column	Description
Purchase Date (Server)	The date and time the license group was purchased.
Effective Date (Server)	The date and time the license went into effect. This date is the first day that the licenses became valid, not necessarily the installation date.
Expiration Date (Server)	The date and time the license group expires.
Purchased	The total number of licenses purchased in the license group.

Initiating Subscription License Replication

Initiate replication to validate your licenses. Updates are made if your subscription has changed. Initiate replication after purchasing new modules.

Initiate license replication from the ***Product Licensing*** page.

1. From the **Navigation Menu**, select **Help** > **Product Licensing**.
2. Click **Validate**.

   Step Result: A dialog opens, prompting you to acknowledge the validation initiation.
3. Click **OK**.

Result: Replication begins. Completion may take several minutes.

Exporting Product Information

You can export product information data to a comma-separated value (.csv) file for reporting and analytical purposes.

To export this data, select **Help** > **Product Licensing** and click **Export**. For additional information, refer to Exporting Data on page 47.

The Subscription Updates Page

Periodically, your server downloads system updates from the Global Subscription Service. You can initiate these downloads, called *replications*, from the ***Subscription Updates*** page.

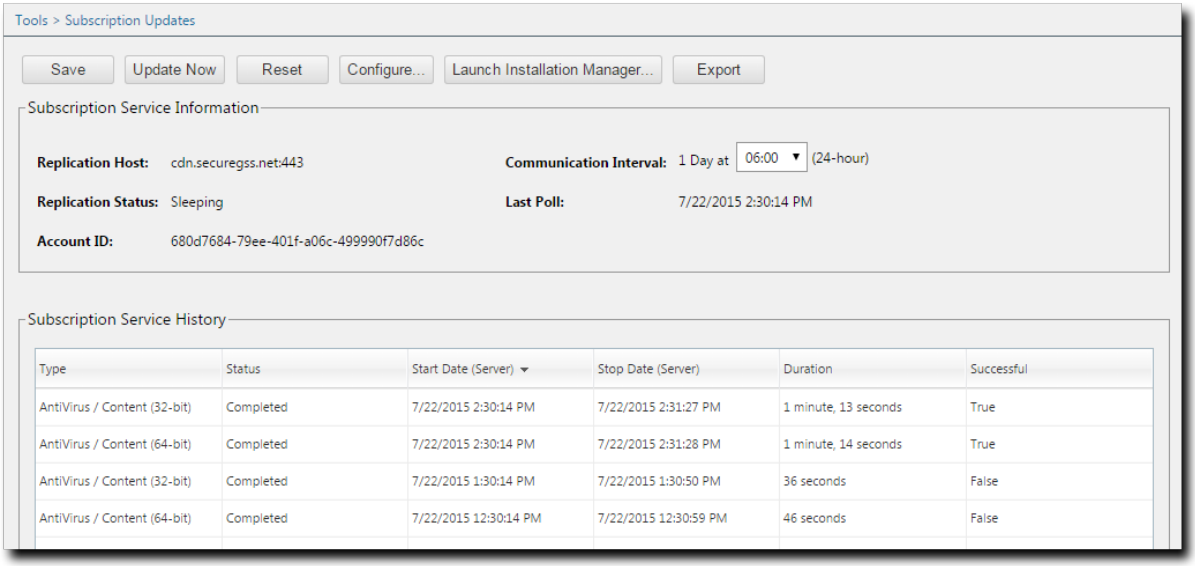


Figure 35: Subscription Updates Page

From this page, you can perform the following actions:

- Modify the subscription communication interval
- Initiate a replication
- Configure the subscription service
- View the subscription service replication history

Viewing the Subscription Updates Page

Navigate to the ***Subscriptions Updates*** page to view the subscription update history or to edit subscription settings.

You can access this page from the navigation menu.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. [Optional] Perform a task listed in Working with Subscription Updates on page 137.

Subscription Updates Page Toolbar

This toolbar controls the functions available from the ***Subscription Updates*** page. Click a toolbar button to initiate subscription function.

The following table describes each button's function

Table 66: Subscription Updates Page Buttons

Button	Function
Save	Saves the page edits.
Update Now	Replicates all license, system, and content changes since the last replication with the Global Subscription Service (GSS). For additional information, refer to Updating Ivanti Endpoint Security System Files and Content on page 137.
Reset	Resets the replication status. For additional information, refer to Resetting the Replication Status on page 138.
Configure...	Configures subscription communication settings. For additional information, refer to The Subscription Service Configuration Dialog on page 130.
Launch Installation Manager...	Opens Ivanti Installation Manager. For additional information, refer to Using Ivanti Installation Manager Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Subscription Service Information

These fields list information about the Global Subscription Service and its communication history with your server.

Table 67: Subscription Service Information

Field	Description
Replication Host	The name and port of the Global Subscription Service (GSS).
Replication Status	The current replication status. Replication ensures that your server remains current with the latest content, package, and license information.

Field	Description
Account ID	Your account ID. The ID is uploaded to the GSS, which validates the update request. The account ID is created by your server when it registers with the GSS.
Communication Interval	The time your server connects to the GSS for replication. For additional information, refer to Editing the Communication Interval on page 139.
Last Poll	The date and time your server last replicated with the GSS.

Note: The **Communication Interval** field is the only setting within **Subscription Service Information** that can be edited.

Subscription Service History

This table lists a record of subscription license replications and content replications. Additional details for each replication are included.

Mobile Device Management adds a new **Type** to the **Subscription Service History**. View this update from the ***Subscription Updates*** page (**Tools** > **Subscription Updates**).

MDM Configuration	Downloads data used for Mobile Device Management cloud communications.

Patch and Remediation adds new replication **Types** to the **Subscription Service History**:

Package	Downloads the patch content (or packages) selected for caching. If automatic critical package caching is enabled, all critical packages are downloaded .
Patch / Content	Downloads the current patch content definitions according to: • The subscription type and operating system subscriptions defined for the account. • The content languages selected within the Ivanti Endpoint Security console. For additional information, refer to Configuring the Languages Tab on page 141.
Patch / Components	Updates a file used during Discover Applicable Updates tasks that contains patch content definitions from vendors and the Global Subscription Service.
Patch / OS Packs	Updates a file used during Discover Applicable Updates tasks that contains patch content definitions from vendors, the Global Subscription Service, and any locally created content.

For additional information about the remaining page information, refer to *Subscription Service History* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/)

Table 68: Subscription Service History Table

Column	Description	
Type	The type of replication. The types include:	
	Licenses	Verifies the validity of your system licenses.
	System	Downloads new core system files, including operating system definitions and agent upgrades.
	AntiVirus / Content	During communication with the GSS, Ivanti Endpoint Security downloads antivirus definition files and the content needed for virus resolution (AntiVirus and Application Control only).
	MDM Configuration	Downloads data used for Mobile Device Management cloud communications.
	Package	Downloads the patch content (or packages) selected for caching. If automatic critical package caching is enabled, all critical packages are downloaded (Patch and Remediation only).
	Patch / Content	Updates the list of patch content available for download from the Global Subscription Service: • The operating systems you are licensed for. • The content languages you've selected. (Patch and Remediation only)
	Patch / Components	Updates a file used during Discover Applicable Updates tasks that contains patch content definitions from vendors and the Global Subscription Service.
	Patch / OS Packs	Updates a file used during Discover Applicable Updates tasks that contains patch content definitions from vendors, the Global Subscription Service, and any locally created content.
Status	The status of the replication task. The statuses include:	
	`Initializing Replication`	Replications are initializing.
	`Downloading`	Replications are downloading.
	`Completed`	Replications are complete.

Column	Description
Start Date (Server)	The date and time on the server that the replication started.
Stop Date (Server)	The date and time on the server that the replication completed.
Duration	The duration of the replication.
Successful	The replication completion status (`True`, `False`, or `Failed`). **Tip:** Hover over an AntiVirus/Content replication `False` status to reveal the Latest Scan Engine Version, Definition Version, and Date Created.

The Subscription Service Configuration Dialog

Use this dialog to configure communication behavior while your server is contacting the Global Subscription Service.

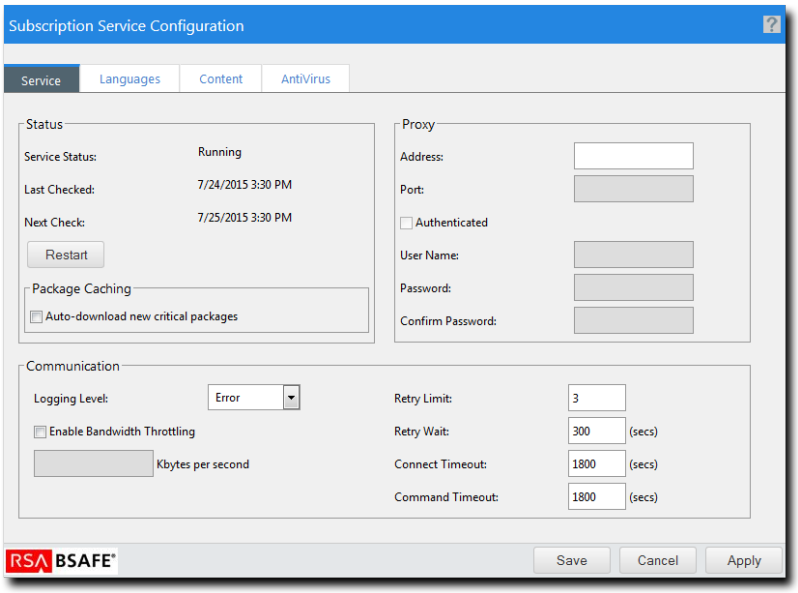


Figure 36: Subscription Service Configuration Dialog

Patch and Remediation adds a new option to the The Service Tab on page 131.

Additionally, the following tabs are added to the ***Subscription Service Configuration*** dialog:

- The Languages Tab on page 133
- The Content Tab on page 135

Viewing the Subscription Service Configuration Dialog

Use this dialog to configure subscription service settings.

You can access this dialog from the ***Subscription Updates*** page.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Configure**.

Result: The ***Subscription Service Configuration*** dialog opens.

The Service Tab

Using this tab, you can customize communication settings between your server and the Global Subscription Service.

You can use this tab to perform the following actions related to communications between your server and the Global Subscription Service:

- Select a logging level
- Configure a proxy
- Restart the subscription service

Status

The **Status** section lists whether the subscription service is running, as well as information about past and pending communication with the Global Subscription Service.

Table 69: Status Fields and Controls

Field or Control	Description
Service Status	The current status of the replication service on your server.
Last Checked	The last date and time on your server that the replication service last communicated with the GSS.
Next Check	The next scheduled date and time that the replication service will communicate with the GSS.
Restart	Restarts the replication service. For additional information, refer to Restarting the Replication Service on page 140.

Package Caching
This section lets you select whether packages related to critical vulnerabilities are automatically downloaded. Caching packages makes them available for immediate deployment, but consume additionally storage space.

Table 70: Package Caching Option

Option	Description
Auto-download download critical packages	Indicates whether packages related to critical vulnerabilities are automatically downloaded. For additional information, refer to Configuring the Service Tab on page 139.

Proxy
When using a proxy for communication between the Ivanti Endpoint Security server and the Global Subscription Service, you must define the applicable proxy information within Ivanti Endpoint Security before communication can occur.

Note: Refer to the Ivanti Endpoint Security: Requirements Guide (https://help.ivanti.com) for a complete list of proxy types that Ivanti Endpoint Security supports.

Define this proxy information from the ***Subscription Service Configuration*** dialog ***Service*** tab. The following table describes each setting.

Table 71: Proxy Setting Descriptions

Setting	Description
Address (field)	The IP address or name of the proxy used for communication between Ivanti Endpoint Security (Ivanti Endpoint Security) and the Global Subscription Service (GSS).
Port (field)	The proxy port used for communication between Ivanti Endpoint Security and the GSS.
Authenticated (check box)	This check box enables the remaining fields when proxy authentication is required.
User Name (field)	A user name that will authenticate with the proxy.
Password (field)	The password associated with the user name.
Confirm Password (field)	The password retyped.

Communication

When configuring replication service communication, you can set options for how your server communicates with the Global Subscription Service.

Define communication options from the ***Subscription Service Configuration*** dialog ***Service*** tab.

Table 72: Communication Option Descriptions

Option	Description	
Logging Level	Defines the level of detail in logs recorded during communication between you server and the Global Subscription Service. The available values include:	
	Debug	Logs errors, warnings, system actions, and debugging information. **Note:** This logging level is the most comprehensive. Only use this setting for troubleshooting purposes due to increased log size and replication times.
	Information	Logs errors, warnings, and system actions.
	Warning	Logs errors and warnings.
	Error	Logs only errors.
Enable Bandwidth Throttling	Limits the transmission speed during replication.	
***x* Kbytes per second**	Defines the maximum transmission speed when **Enable Bandwidth Throttling** is selected.	
Retry Limit	The number of times your server attempts to reestablish communication with the GSS if the first attempt fails.	
Retry Wait	The number of seconds between retries.	
Connect Timeout	The number of seconds before a connection attempt is considered unsuccessful.	
Command Timeout	The number of seconds of inactivity before a command is considered unsuccessful.	

The Languages Tab

Patch and Remediation content and content definitions are available in multiple languages. From the ***Languages*** tab, you can define the languages that security content definitions are replicated for.

This tab is added after you install Patch and Remediation.

Generally, you should only select the languages that suit your network environment. The following languages are available:

Table 73: Agent Supported Languages

Description	Language Code	LCID string	Decimal	Hexadecimal
Chinese - China (Simplified)	zh	zh-cn / za-chs	2052	0804
Chinese - Taiwan (Traditional)	zh	zh-tw / zh-cht	1028	0404
Danish	da	da	0406	1030
Dutch - Netherlands	nl	nl-nl	1043	0413
English - United States	en	en-us	1033	0409
English - United Kingdom	en	en-gb	0809	041d
English - South Africa	en	en-za	7177	1c09
Finnish - Finland	fi	fi	1035	040b
French - France	fr	fr-fr	1036	040c
German - Germany	de	de-de	1031	0407
Italian-Italy	it	it-it	1040	0410
Japanese - Japan	ja	ja	1041	0411
Korean - Korea	ko	ko	1042	0412
Norwegian - Nynorsk	no	no-no	1044	0414
Portuguese - Brazil	pt	pt-br	1046	0416
Russian - Russia	ru	ru	1049	0419
Spanish - Spain (Modern Sort)	es	es-es	3082	0c0a
Swedish - Sweden	sv	sv-se	1053	041d

The Content Tab
This tab lists Websites that your server can access through its firewall to download content directly from vendors rather than the Global Subscription Service.

- In some cases, you may need to download content directly from vendor Websites rather than the Global Subscription Service. This process expedites your access to new content within Ivanti Endpoint Security.
- Click **Export** to export the external sites listed on the tab.

The AntiVirus Tab
Configure AntiVirus module settings, including engine and definition file polling frequency and content storage locations.
AntiVirus Engine & Definition Versions (Server) Section
This section provides information about the current AntiVirus engine and definition files installed (both 32- and 64-bit) and enables you to immediately download updates.

The following table describes each **AntiVirus Engine & Definition Versions (Server)** field and control.

Table 74: Latest AntiVirus Engine & Definition Versions (Server) Fields and Controls

Field or Control	Description
AV engine and definition version	Version number of the scan engine and definition file.
Definitions created on	Date and time the AntiVirus engine and definition file installed in the system was created.
Definitions downloaded on	Date and time the AntiVirus definition file installed in the system was download.
Download now	Enables you to immediately download AntiVirus engine and definition file updates from the Global Subscription Service to the Application Server, if available. Distribution of new AntiVirus definitions from the application server to endpoints is managed through Agent Policy Sets.

Note: An AntiVirus ***Agent version 7.2 to 8.1*** area will appear in this section if you have such agents in your environment. Scan Engine and Definition versions are displayed separately.

AntiVirus Engine & Definition Download Settings (Server to GSS) Section
This section enables you to set the frequency at which Ivanti Endpoint Security checks for AntiVirus engine and definition file updates and displays the date and time of the last check.

The following table describes each **AntiVirus Communication Settings** field and control.

Table 75: AntiVirus/Content Polling Frequency Controls

Field or Control	Description
AntiVirus/ Content polling freqeuncy	The frequency (in hours) at which the system is to check for engine and definition file updates. The polling frequency intervals available range from a minimum of 0.5 hours to a maximum of 24 hours. The default interval is 1 hour.
Daily at	Once a day at a specified time.
Last checked (GSS)	Date and time the system last checked the Global Subscription Service for new engine and definition files.

AntiVirus Content Storage Location Section
This section enables you to designate where Ivanti Endpoint Security is to check for and download AntiVirus engine and definition files.

The following table describes each **AntiVirus Content Storage Location** field and control.

Table 76: AntiVirus Content Storage Fields and Controls

Field or Control	Description
AntiVirus/ Content location (URL)	Field to specify a full link (URL) with file name to where the AntiVirus engine and definition file content is stored. The default link is http://cache.lumension.com/avcontent.
Add	Adds the link entered in **AntiVirus / Content location (URL)** field to the URL list.
Test Link...	Checks that the URL you entered works correctly. A dialog opens informing you about the validity of the URL.
Remove	Removes selected links on the URL list.

Note: An AntiVirus ***Agent version 7.2 to 8.1*** area will appear in this section if you have such agents in your environment. You must set separate content storage locations to download content for 7.2 to 8.1 agents. The default links are http://cache.lumension.com/antivirus/avfilelist.xml and http://cache.patchlinksecure.net/antivirus/avfilelist.xml

Working with Subscription Updates

You can configure how the Ivanti Endpoint Security server receives subscription updates from the Global Subscription Service by using the ***Subscription Updates*** page.

Updating Ivanti Endpoint Security System Files and Content

You can update the latest Ivanti Endpoint Security system components and content by completing a process call *Replication*. Replication downloads any system components, content definitions, or licensing information posted to the Global Subscription Service since the previous replication. Although the system automatically replicates once daily, you may occasionally need to replicate manually from time to time. Additionally, in network environments with the Ivanti AntiVirus module installed, you can use this function to manually download new virus definitions.

Prerequisites:

Mobile Device Management licensing has been purchased.

Initiate replications from the ***Subscriptions Updates*** page.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Update Now**.

   Step Result: A notification dialog opens.

   Note: In network environments with the Ivanti AntiVirus module installed, the notification dialog contains selectable options (**System and License Replication** and **Virus Engine and Definition Update**). In this scenario, select the desired options before proceeding to the next step.

3. Acknowledge the replication by clicking **OK**.

Result: Replication begins immediately. All license and content changes since the last replication are downloaded. This process may take several minutes, and no Discover Applicable Update tasks run during completion.

After Completing This Task:
Install the server module. For more information, see Installing the Mobile Device Management Server Component.

Resetting the Replication Status

Resetting the replication status forces the Ivanti Endpoint Security server to re-download (or update) the licenses, packages, and content.

Reset the replication status from the ***Subscription Updates*** page.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Reset**.

   Step Result: The ***Reset Replication*** dialog opens.
3. Select a replication option.

Note:

- The options available in the ***Reset Replication*** dialog change based on whether the **Auto-download new critical packages** option is selected. For additional information, refer to Package Caching on page 132.
- If you have cached packages for content that is disabled, those packages are not updated during replication if a new version is available.

Context	Options
If the Auto-download new critical packages option is selected	Select from the following options: • Cache metadata and critical packages for only new and changed content. • Cache metadata and critical packages for all historical content.
If the Auto-download new critical packages option is cleared	Select from the following options: • Cache both metadata and critical packages. • Only cache metadata.

4. Define when you want to begin replication.
   Click the applicable button.
   - To begin replication immediately, click **Update Now**.
   - To being replication at the next scheduled interval, click **Update Later**.

Result: You replication status is reset when the next replication begins.

Editing the Communication Interval

Edit the communication interval to control the daily time when you server downloads content and license data from the Global Subscription Service.

Edit the communication interval from the ***Subscription Updates*** page.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Select a time from the **Communication Interval** list.
   This list includes a value for every half-hour.
3. Click **Save**.
   Step Result: A dialog opens, notifying that the new setting was saved.
4. Click **OK**.

Result: The selected communication interval is saved. Your server will replicate daily at the selected time.

Configuring the Service Tab

Configuring the ***Service*** tab defines communication, proxy, and log settings for replication.

Prerequisites:

If you are configuring Mobile Device Management to use a proxy server, the proxy server must using http 1.1 or later with chunked encoding.

- Ensure you are logged in to the Ivanti Endpoint Security Web console.
- Ensure your proxy meets requirements. For more information, see Proxy Requirements.

Configure the ***Service*** tab from the ***Subscription Service Configuration*** dialog. Patch and Remediation introduces the **Auto-Download new critical packages** option. For additional information about the remaining options, refer to *Configuring the Service Tab* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Configure**.
   Step Result: The ***Subscription Service Configuration*** dialog opens.
3. Ensure the ***Service*** tab is selected.

4. To automatically download packages associated with content items with a status of critical, select the **Auto-download new critical packages** check box .
5. Define **Proxy** options.

   These options define the proxy information used for communication between the server and the Global Subscription Service (GSS).

   Tip: For additional information about each option, refer to Proxy on page 132.

   a) Complete the **Address** and **Port** fields.
   b) If your proxy server requires authentication, select the **Authenticated** check box and complete the **User Name**, **Password**, and **Confirm Password** fields.
6. Define **Communication** options.

   These options define actions related to your server communication with the GSS.

   Tip:

   - For additional information about each option, refer to Communication on page 133.
   - Under most conditions, the **Retry Limit**, **Retry Wait**, **Connect Timeout**, and **Command Timeout** options require no editing.

   a) Select a **Logging Level** from the list.
   b) To limit communication speeds during replication, select the **Enable Bandwidth Throttling** check box and type a number in the ***X* Kbytes per second** field.
   c) Type a number in the **Retry Limit** field.
   d) Type a number in the **Retry Wait** field.
   e) Type a number in the **Connect Timeout** field.
   f) Type a number in the **Command Timeout** field.
7. Click **Save** to apply your changes.

   Tip: If you want to continue using the ***Configuration Settings*** dialog, click **Apply** instead of **Save**.

Result: Your edits are saved. These edits will take effect the next time Ivanti Endpoint Security communicates with the GSS.

After Completing This Task:
If you edited the **Logging Level**, you must restart the replication service before the changes take place. For additional information, refer to Restarting the Replication Service on page 140.

Restarting the Replication Service

You can restart the replication service on your server using the Web console.

You can restart the subscription service from the ***Subscription Service Configuration*** dialog ***Service*** tab.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.

2. Click **Configure**.

   Step Result: The ***Subscription Service Configuration*** dialog opens.

3. Ensure the ***Service*** tab is selected.
4. Click **Restart**.
5. Acknowledge the notification by clicking **OK**.

Result: The replication service is restarted on your server.

Configuring the Languages Tab

Selecting language options downloads new localized content definitions to your server. You can deploy their content later. Select additional languages when you administrate an environment that uses multiple localizations.

Select language options from the ***Subscription Server Configuration*** dialog ***Languages*** tab.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Configure**.

   Step Result: The ***Subscription Service Configuration*** dialog opens.

3. Select the ***Languages*** tab.
4. Select the check boxes for each language you want content item definitions. Clear any unused languages.

   Note:

   - Selecting multiple languages increases the number of content definitions downloaded, slowing replication times.
   - The **English** check box cannot be cleared.

5. Click **Save**.

   Tip: If you want to continue working withing the ***Subscription Server Configuration***, click **Apply** instead.

Result: Your edits are saved. Content definitions for the selected languages are downloaded during the next replication.

Exporting Enhanced Content Data

While viewing the ***Content*** tab, you can export the listed content URLs to a comma separated value (`.csv`) file.

To export the listed URLs, select **Tools** > **Subscription Updates** and click **Configure**. Then select the ***Content*** tab and click **Export**. For additional information refer to Exporting Data on page 47.

Exporting Subscription Update Data

You can export data displayed on the ***Subscription Updates*** page to a comma separated value (`.csv`) file for reporting and analytical purposes.

Both **Subscription Service Information** and **Subscription Service History** are exported. To export this data, select **Tools** > **Subscription Updates** and click the **Export** button. For additional information refer to Exporting Data on page 47.

Chapter 7

Using Endpoints

In this chapter:

While using Ivanti Endpoint Security (Ivanti Endpoint Security), you can view and manage network endpoints after installing agents.

The ***Endpoints*** page contains a listing of all endpoints that have an agent registered with the Ivanti Endpoint Security server. From this list of endpoints, you can access the endpoint details. The endpoint details include endpoint-specific information.

About Endpoints

The ***Endpoints*** page is used to manage the computers and devices, referred to as *endpoints*, on your network. The Ivanti Endpoint Security server manages your endpoints by sending user-defined and automated commands to your endpoints' agents. When the agent contacts the server, the commands are executed.

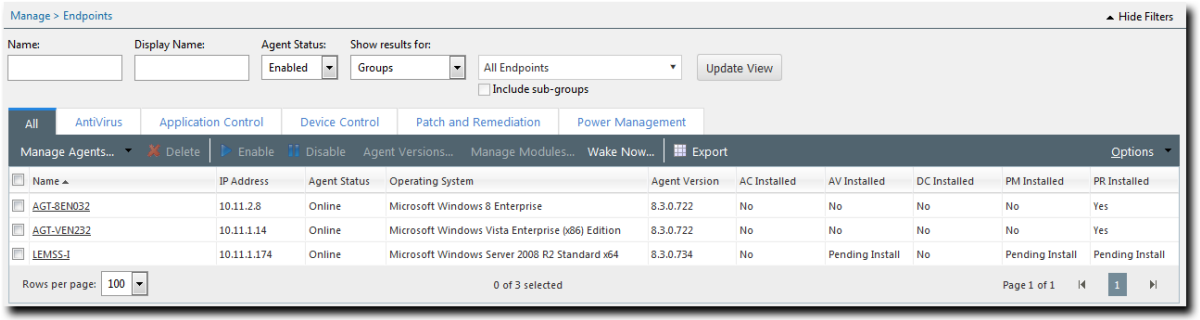


Figure 37: Endpoints Page

The ***Endpoints*** page lists all endpoints registered to the Ivanti Endpoint Security server. The page displays general information about the endpoint, such as the endpoint name, status, operating system, and agent version.

The Endpoints Page

The ***Endpoints*** page contains information about the managed endpoints on your network. From the ***Endpoints*** page, you can use features associated with endpoints.

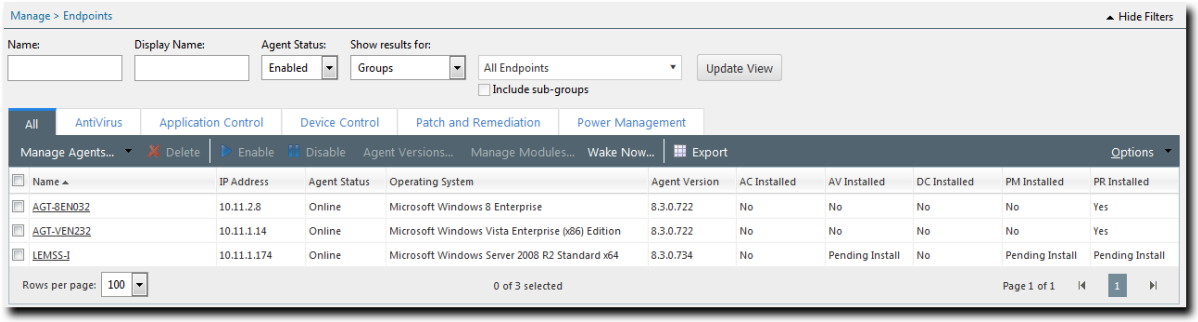


Figure 38: Endpoints Page

After installing Patch and Remediation, you can access the ***Patch and Remediation*** tab from the ***Endpoints*** page.

- The All Tab on page 148
- The AntiVirus Tab on page 153
- The Application Control Tab on page 158
- The Device Control Tab on page 172
- The Patch and Remediation Tab on page 163
- The Power Management Tab

The All Tab Toolbar

The ***All*** tab toolbar contains buttons used to manage basic endpoint functions.

The following table describes the toolbar functions used in the ***Endpoints*** page.

Table 77: All Tab Toolbar Functions

Button	Function
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Install agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management JobInstalling Agents by Agent Management Job.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.

Button	Function
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.
Enable	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182. **Note:** This button is only available when an endpoint is disabled.
Disable	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 179.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Installing Endpoint Modules on page 184.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The All Tab List

The ***All*** tab list itemizes endpoint operating system information, identification information, agent information, and module information.

The following table describes the columns within the ***All*** tab list and the comma separated value (`.csv`) file you can export from it (refer to Exporting Data on page 47).

Table 78: All Tab List Columns

Column	Description	
Name	The name of the endpoint. Click the link to view its details.	
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..	
IP Address	The IP address of the endpoint.	
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:	
	Online	The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior.
	Offline	The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.

Column	Description
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
Operating System	The operating system that the endpoint uses.
Agent Version	The version of the Ivanti Endpoint Security Agent installed. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

Column	Description	
***Module* Installed**	Indicates whether a module is installed on the endpoint. A new ***Module* Installed** column is added for each module installed on your Ivanti Endpoint Security Server. The following list defines column entry values:	
	Yes	The module is installed.
	No	The module is not installed.
	Pending Install	The module is in the process of installing.
	Pending Uninstall	The module is in the process of uninstalling.
	Pending Reboot	The module has been installed, but the endpoint needs to reboot to complete installation.
	Error	There was an error while installing or uninstalling the module. Click the for additional information about the error.
	Expired	The module license has expired.

The All Tab

This tab lists information about endpoints, the agent version installed on them, and the module features active on them.

This tab displays by default when you open the ***Endpoints*** page.

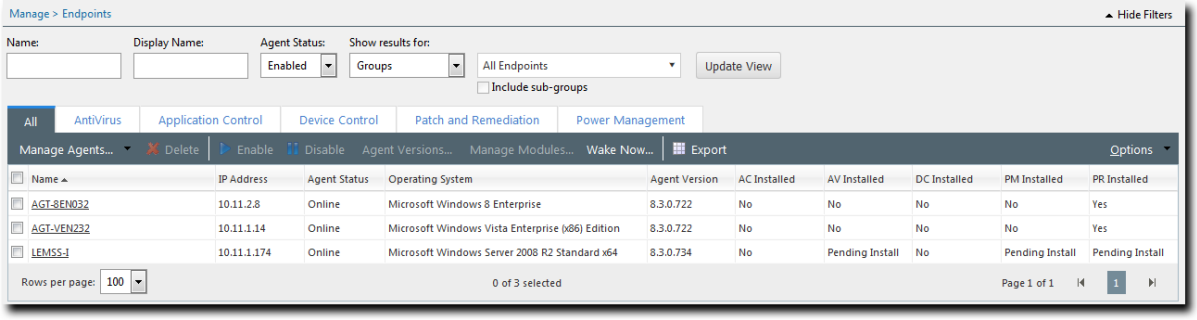


Figure 39: All Tab

The All Tab Toolbar

The ***All*** tab toolbar contains buttons used to manage basic endpoint functions.

The following table describes the toolbar functions used in the ***Endpoints*** page.

Table 79: All Tab Toolbar Functions

Button	Function
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Install agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management JobInstalling Agents by Agent Management Job.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.
Enable	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182. **Note:** This button is only available when an endpoint is disabled.
Disable	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 179.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Installing Endpoint Modules on page 184.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The All Tab List

The ***All*** tab list itemizes endpoint operating system information, identification information, agent information, and module information.

The following table describes the columns within the ***All*** tab list and the comma separated value (`.csv`) file you can export from it (refer to Exporting Data on page 47).

Table 80: All Tab List Columns

Column	Description
Name	The name of the endpoint. Click the link to view its details.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.

Column	Description	
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:	
	Online	The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior.
	Offline	The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.	

Column	Description	
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values:	
	Started	EDS server has started and is in an operational state accepting workloads.
	Starting	EDS server is in the process of starting its service.
	Stopped	EDS server has stopped and is not accepting workloads.
	Stopping	EDS server is in the process of stopping so as to not accept workloads.
	Offline	EDS server is offline as it has not contacted the database in the configured amount of time.
Operating System	The operating system that the endpoint uses.	
Agent Version	The version of the Ivanti Endpoint Security Agent installed.	
	Note: A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.	

Column	Description	
***Module* Installed**	Indicates whether a module is installed on the endpoint. A new ***Module* Installed** column is added for each module installed on your Ivanti Endpoint Security Server. The following list defines column entry values:	
	Yes	The module is installed.
	No	The module is not installed.
	Pending Install	The module is in the process of installing.
	Pending Uninstall	The module is in the process of uninstalling.
	Pending Reboot	The module has been installed, but the endpoint needs to reboot to complete installation.
	Error	There was an error while installing or uninstalling the module. Click the for additional information about the error.
	Expired	The module license has expired.

The AntiVirus Tab

This tab lists endpoint name and address information, anti-virus definition version and update information, and scan status.

View this tab from the ***Endpoints*** page.

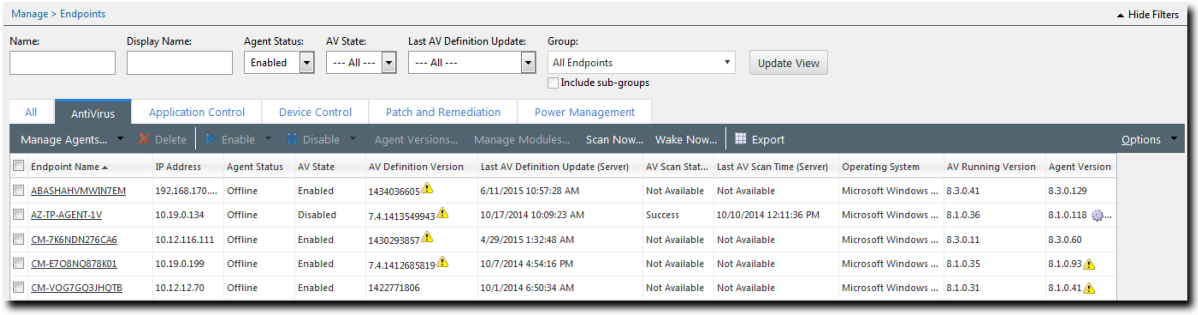


Figure 40: The AntiVirus Tab

The AntiVirus Tab Toolbar

The **AntiVirus** tab toolbar contains the tasks and functions that are available for you to perform for managed endpoints with AntiVirus features enabled.

The following table describes the toolbar functions in the ***Endpoints*** page when the **AntiVirus** tab is selected.

Table 81: AntiVirus Toolbar Functions

Button	Function
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 179.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.
Enable (Menu)	Expands the **Enable** menu.
Enable Module (**Enable** menu item)	Enables the AntiVirus agent module on selected endpoints.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182. **Note:** This button is only available when an endpoint is disabled.
Disable (Menu)	Expands the **Disable** menu.

Button	Function
Disable Module (**Disable** menu item)	Disables the AntiVirus agent module on selected endpoints. For additional information, refer to Disabling Modules on an Endpoint on page 182.
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Manage Modules	Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions. For additional information refer to Installing Endpoint Modules on page 184.
Scan Now...	Launches the ***Virus and Malware Scan Wizard***. Use this wizard to launch an immediate anti-virus scan on the selected endpoint(s). For additional information refer to Running Scan Now on an Endpoint.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options	Opens the **Options** menu. For more information see The Options Menu on page 39.

The AntiVirus Tab List

The **AntiVirus** tab list itemizes endpoint identification data, server connectivity, operating system, and agent information. It also displays the antivirus definition file version and scan status for each endpoint.

The following table describes the columns within the **AntiVirus** tab list and the comma separated value (`.csv`) file you can export from it (refer to Exporting Data on page 47).

Table 82: AntiVirus Tab List Columns

Column	Description
Name	The name of the endpoint. Click the link to view its details.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.

Column	Description	
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:	
	Online	The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior.
	Offline	The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.	

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
AV State	State of the AntiVirus agent module (`Enabled`, `Disabled`).
AV Definition Version	Version of the definition file currently installed on the endpoint. **Note:** If the definition version is not the latest available, a warning triangle is displayed.
Last AV Definition Update (Server)	Date and time that the anti-virus definition was last updated on the endpoint.
AV Scan Status	Status of the latest anti-virus scan to run on the endpoint (`In-progress`, `Success`).
Last AV Scan Time (Server)	Date and time that the last anti-virus scan started, shown as server time.
Operating System	Operating system the endpoint is running.
AV Running Version	Version number of the AntiVirus module component installed on the endpoint.

Column	Description
Agent Version	Indicates the version of the agent that the endpoint is currently running. **Note:** A icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

The Application Control Tab

This tab lists endpoint name and IP address information, application control state and policy information, and agent information.

Note: This content is only available when the Application Control module is installed.

View this tab from the ***Endpoints*** page.

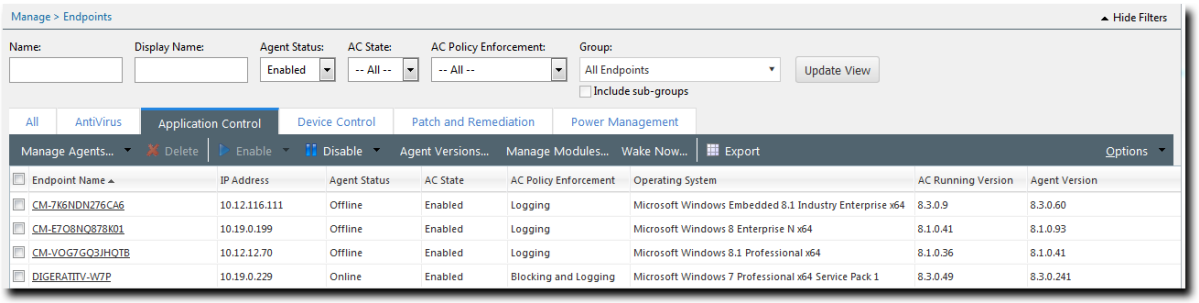


Figure 41: The Application Control Tab

The Application Control Tab Toolbar

The Application Control tab toolbar contains buttons you can use to enable or disable the Application Control module component on endpoints that have it installed.

The following table describes each toolbar button.

Table 83: Application Control Tab Toolbar

Button	Description
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job.

Button	Description
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.
Enable (Menu)	Expands the **Enable** menu.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182.
Enable Module (**Enable** menu item)	Enables the Application Control agent module on only selected endpoints. For additional information, refer to Enabling Modules on an Endpoint on page 181.
Disable (Menu)	Expands the **Disable** menu.
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Disable Module (**Disable** menu item)	Disables the Application Control agent module on only selected endpoints. For additional information, refer to Disabling Modules on an Endpoint on page 182.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to add and remove modules to or from the endpoint. For additional information, refer to Installing Endpoint Modules on page 184.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Application Control Tab List

The **Application Control** tab contains a list of all endpoints that have the Application Control module component installed.

The following table describes the columns within the **Application Control** tab list and the comma separated value (`.csv`) file you can export from it (refer to Exporting Data on page 47).

Table 84: Application Control Tab List Columns

Column	Description
Endpoint Name	Indicates the name of the endpoint. Clicking the ***Endpoint Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.

Column	Description	
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:	
	Online	The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior.
	Offline	The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.	

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
LAC State	Indicates the state of the Application Control module component on the endpoint (`Enabled` or `Disabled`).
LAC Policy Enforcement	Indicates the Application Control policy enforcement.
Operating System	The operating system that the endpoint uses.
LAC Running Version	Indicates the version of the Application Control module component installed on the endpoint.
Agent Version	The version of the Ivanti Endpoint Security Agent installed. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

The Patch and Remediation Tab

This tab lists identification for endpoints that have the Patch and Remediation module installed.

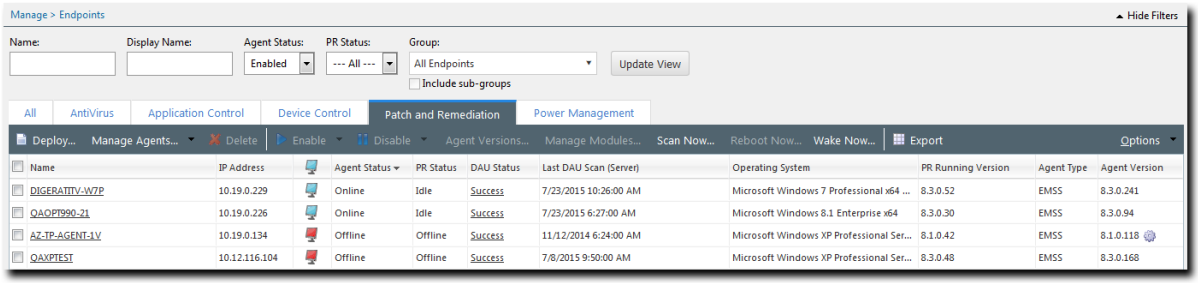


Figure 42: Patch and Remediation Tab

The Patch and Remediation Tab Toolbar

The Patch and Remediation Tab toolbar contains the tasks and functions that are available for you to perform for managed endpoints with Patch and Remediation features enabled.

The following table describes the Patch and Remediation Tab toolbar functions.

Table 85: Patch and Remediation Tab Toolbar Functions

Button	Function
Deploy...	Launches the ***Deployment Wizard***, which allows you to create a deployment for the selected endpoints (Patch and Remediation only). For additional information, refer to Deploying Content to Endpoints (Patch and Remediation Tab) on page 178.
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Install agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.

Button	Function
Enable (Menu)	Expands the **Enable** menu.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182.
Enable Module (**Enable** menu item)	Enables the Patch and Remediation endpoint module on only selected endpoints. For additional information, refer to Enabling Modules on an Endpoint on page 181.
Disable (Menu)	Expands the **Disable** menu.
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Disable Module (**Disable** menu item)	Disables the Patch and Remediation endpoint module on only selected endpoints. For additional information, refer to Disabling Modules on an Endpoint on page 182.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 179.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to add and remove modules to or from the endpoint. For additional information, refer to Installing Endpoint Modules on page 184.
Scan Now...	Prompts the Discover Applicable Updates task to launch immediately (within the agent hours of operation) and scan all agent-managed endpoints within your network for vulnerabilities. This scan queues an inventory of vulnerabilities that will run the next time the agent checks in with the server (Patch and Remediation only). For additional information, refer to Using Scan Now to Scan Inventory (Patch and Remediation Tab) on page 185.
Reboot Now...	Prompts the selected endpoint to reboot. For additional information, refer to Rebooting Endpoints on page 186.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Button	Function
Options	Opens the **Options** menu. For more information, see The Options Menu on page 39.

The Patch and Remediation Tab List

The Patch and Remediation tab list itemizes identification data, server connectivity, operating system, and agent information for endpoints with the Patch and Remediation agent module.

The following table describes the columns within the ***Endpoints*** page.

Table 86: Patch and Remediation Tab List Columns

Column	Description
Name	The name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.
Status (icon)	The icon representing the Patch and Remediation module status. You can mouse over the icon to display description of the Patch and Remediation status. For additional information, refer to Agent Module Status Icons on page 168.

Column	Description	
Agent Status	Indicates the status of the endpoint. The following list defines column values:	
	Online	The agent is able to communicate with the Ivanti Endpoint Security server in the predefined time period. Refer to Configuring the Agents Tab on page 89 for additional information on configuring agent default behavior.
	Offline	The agent is unable to communicate with the Ivanti Endpoint Security server in the predefined time period. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status, indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is either offline or has an update required status. Click the icon to find out additional status details and EDS server information.
	Disabled	The agent will no longer enforce any module policies or complete tasks. All endpoints must show a `Disabled` status in order to delete the endpoint. Refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.	

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
PR Status	The status for Patch and Remediation module on the endpoint (`Working`, `Idle`, `Sleeping`, `Offline`, `Disabled`).
DAU Status	The status of the Discover Applicable Updates (DAU) scan when last run. The status is also a link to the applicable ***Deployment Results*** page. Status values include: `Success` or `Failure` followed by the failure code, and `Not Available`, which indicates that the endpoint has not checked in. **Note:** The `Not Available` **DAU Status** is not a hyperlink (Patch and Remediation only).
Last DAU Scan (Server)	The date and time of the last successful DAU scan (server side). A value of `Not Available` indicates the endpoint has not completed a DAU scan (Patch and Remediation only).
Operating System	The operating system the endpoint is running.
PR Running Version	The Patch and Remediation module version number running on the endpoint.
Agent Type	The type of agent that is running on the endpoint and communicating with Ivanti Endpoint Security (Ivanti Endpoint Security or Patch).

Column	Description
Agent Version	Indicates the version of the agent that the endpoint is currently running. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

Agent Module Status Icons
Within Ivanti Endpoint Security, icons are used to indicate agent statuses regarding agent activity. These icons appear on various pages. By understanding these icons, you can understand what activity is occurring on any specified patch endpoint.

The following table defines agent (endpoint) status and associated icons.

Table 87: Endpoint Status Icons

Active	Pending	Description
	N/A	The agent is currently working on a deployment (animated icon).
		The agent is idle, and has pending deployments.
		The agent is offline.
	N/A	The agent is offline because the Endpoint Distribution Service the endpoint is connected to is offline or requires an update.
		The agent is sleeping due to its hours of operation settings.
		This agent is disabled.
		The agent is offline and is in a chain status (can accept chained deployments until only after reboot).

Active	Pending	Description
		The agent is offline and is in a reboot status (can accept no more deployments until after it reboots).
		The agent is in a chain status (the agent can accept chained deployments only until after a reboot).
		The agent is in a reboot status (the agent can accept no more deployments until after it reboots).
		The agent is in a chain status (the agent can accept chained deployments only until after a reboot) and is sleeping due to its hours of operation settings.
		The agent is in a reboot status (the agent can accept no more deployments until after it reboots) and is sleeping due to its hours of operation settings.
	N/A	Unable to identify the agent status.

For more information about reboot and chained endpoint status, refer to Reboot and Chained State on page 246.

The Power Management Tab

The ***Power Management*** tab, which is added to the ***Endpoints*** page after Power Management is installed, lists the endpoints that the module is installed on, providing details such as Ivanti Power Management status and running version.

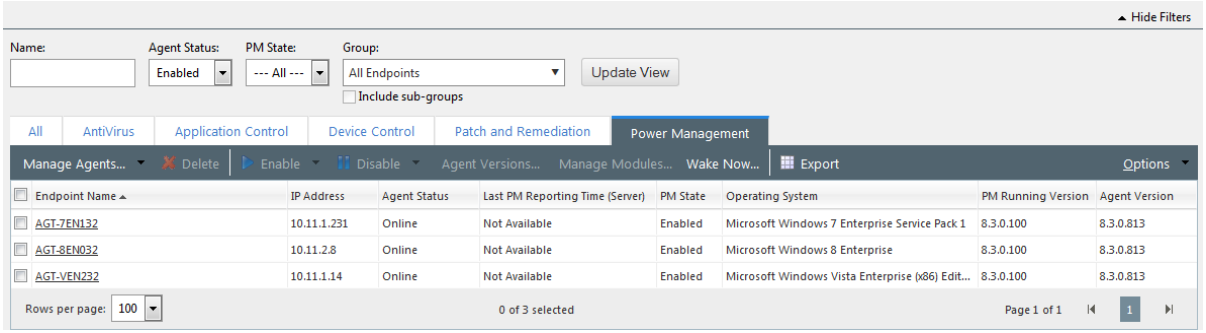


Figure 43: Power Management Tab

The Power Management Tab Toolbar

The ***Power Management*** tab toolbar contains the tasks and functions that are available for you to perform on managed endpoints.

The following table describes the toolbar functions used on the **Power Management** tab.

Table 88: Power Management Tab Toolbar Functions

Button	Function
Manage Agents (menu)	Opens the **Manage Agents** menu.
Install Agents (**Manage Agents** menu item)	Installs agents on selected endpoints.
Uninstall Agents (**Manage Agents** menu item)	Uninstalls agents from the selected endpoints.
Download Agent Installer (**Manage Agents** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security.
Agent Versions	Defines the agent version(s) that can be installed on an endpoint.
Delete	Deletes a disabled endpoint.
Enable	Enables a disabled endpoint. **Note:** This button is only available when an endpoint is disabled.
Disable	Disables an enabled endpoint.
Manage Modules	Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Button	Function
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

Note: For additional information on how to use the toolbar buttons, refer to *The All Tab Toolbar* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

The Power Management Tab List

The **Power Management** tab list contains records of the endpoints that have Ivanti Power Management installed on them.

The following table describes the columns within the ***Power Management*** tab list.

Table 89: Power Management Tab List Columns

Column	Description
Endpoint Name	Indicates the name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page.
IP Address	Indicates the IP address of the endpoint.
Agent Status	Indicates the status of the endpoint (`Online`, `Offline`, or `Disabled`).
Last LPM Reporting Time (Server)	Indicates the last time the Ivanti Power Managementstate was reported to the server.
PM State	Indicates the status of Ivanti Power Management (`Enabled` or `Disabled`).
Operating System	Indicates the operating system the endpoint is running.
PM Running Version	Indicates the version of Ivanti Power Management installed on the endpoint.
Agent Version	Indicates the version of the agent that the endpoint is currently running. **Note:** A icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

The Device Control Tab

This tab lists the endpoints in your network that have the Device Control endpoint component installed. Use this tab to enable or disable the module functions for an endpoint.

The Device Control Tab Toolbar

This toolbar contains buttons you can use to enable or disable the Device Control component on listed endpoints.

The toolbar includes the following buttons.

Table 90: Device Control Tab Toolbar

Button	Description
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.
Enable (Menu)	Expands the **Enable** menu.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182.
Enable Module (**Enable** menu item)	Enables the Device Control agent module on only selected endpoints. For additional information, refer to Enabling Modules on an Endpoint on page 181.
Disable (Menu)	Expands the **Disable** menu.

Button	Description
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Disable Module (**Disable** menu item)	Disables the Device Control agent module on only selected endpoints. For additional information, refer to Disabling Modules on an Endpoint on page 182.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 179.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to add and remove modules to or from the endpoint. For additional information, refer to Installing Endpoint Modules on page 184.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Device Control Tab List

The ***Device Control*** tab includes a listing of endpoints with the Device Control endpoint module component installed. The list includes general information and module state for each endpoint.

The following table describes the columns within the ***Device Control*** tab list and the comma separated value (`.csv`) file you can export from it (refer to Exporting Data on page 47).

Table 91: Device Control Tab List

Column	Description
Endpoint Name	The name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..

Column	Description
IP Address	The IP address of the endpoint.

Column	Description	
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:	
	Online	The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior.
	Offline	The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent is

Column	Description
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
DC State	Indicates the state of Device Control module component on the endpoint (`Enabled` or `Disabled`).
Operating System	The operating system that the endpoint uses.
DC Running Version	Indicates the version of the Device Control module component installed on the endpoint.

Column	Description
Agent Version	The version of the Ivanti Endpoint Security Agent installed. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.
Last Logged Event (Server)	Indicates the last date and time an event was recorded in the Device Control log.
Policy Up To Date	Indicates whether the Device Control policy is up to date (`True` or `False`).

Viewing the Endpoints Page

The ***Endpoints*** page has filters that allow you to customize your view of the computers and other devices that are managed on your network.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. [Optional] Complete a task listed in Working with the Endpoints Page on page 177.

Working with the Endpoints Page

You can perform a number of tasks related to endpoints using toolbar buttons on the ***Endpoints*** page. Click a button to perform a task. Some buttons are not available until one or more list item is selected.

The following list displays the tasks that you can perform from the ***Endpoints*** page.

Note: For additional information about features included in the default installation, refer to *Working with the Endpoints Page* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Deploying Content to Endpoints (Patch and Remediation Tab)

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including the ***Endpoints*** page ***Patch and Remediation*** tab. When deploying from this tab, the ***Deployment Wizard*** is preconfigured to deploy to endpoints selected from the ***Patch and Remediation*** tab list.

You can deploy content from the ***Endpoints*** page ***Patch and Remediation*** tab. For additional information about deployments, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the ***Patch and Remediation*** tab.
3. [Optional] Select the endpoints you want to deploy content to.
4. Click **Deploy**.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete the subsequent tasks.

Installing an Agent

Before you can manage a network endpoint, you must install an agent. You can install an agent manually or using a wizard.

There are two ways in which you can install an agent on an endpoint:

- Install an agent remotely by creating an Agent Management Job. For additional information, refer to Installing Agents by Agent Management JobInstalling Agents by Agent Management Job.
- Install an agent locally by browsing to the Ivanti Endpoint Security server from the endpoint that you want to manage and downloading the agent installer. For additional information, refer to Downloading the Agent Installer on page 180.

Installing Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of installing agents using an Agent Management Job. To create an Agent Management Job that installs agents from the ***Endpoints*** page, select **Manage Agents** > **Install Agents** from the toolbar.

Tip: You can predefine job targets by selecting endpoints from the page list.

For additional information, refer to Installing Agents by Agent Management JobInstalling Agents by Agent Management Job.

Uninstalling Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of uninstalling agents using an Agent Management Job. To create an Agent Management Job that uninstalls agents from the ***Endpoints*** page, select **Manage Agents** > **Uninstall Agents** from the toolbar.

Tip: You can predefine job targets by selecting endpoints from the page list.

For additional information, refer to Uninstalling Agents by Agent Management Job.

Upgrading Endpoints

From the ***Endpoints*** page, you can upgrade your endpoints to the latest version of the Ivanti Endpoint Security Agent. You can update all the endpoints at once, but, as a test, you should upgrade just a few endpoints.

Upgrade your agents using the ***Manage Agent Versions*** dialog, which can be opened from any tab on the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the endpoints you want to upgrade.
3. Click **Agent Versions**.

   Step Result: The ***Manage Agent Versions*** dialog opens.

4. Select the latest agent version from the **Select One** menu and click **Apply to All Agents**.

Tip:

- You can also select an agent version for each endpoint by using the **Agent Version** column menu.
- The agent versions available for upgrading can be selected from the ***Agents*** tab on the ***Options*** page.

5. Click **OK**.

Result: Your endpoints begin upgrading.

- Endpoint upgrade progress displays on the **Manage** > **Endpoints** page.
- Endpoints in the process of upgrading display the icon  in the **Agent Version** column.
- When the icons stops displaying, and the agent version updates, the upgrade is complete.

Downloading the Agent Installer

You can install an agent locally by connecting to the Ivanti Endpoint Security, downloading the agent installer, and running the installer on the endpoint that you want to manage.

The following procedure describes the steps required to download the agent installer to the endpoint that you want to manage using Ivanti Endpoint Security. The agent system requirements and installation procedure varies by operating system. For complete instructions regarding the installation of agents on supported operating systems, refer to the Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .

1. Log in to the target computer as the local administrator (or a member of the **Local Administrators** group).
2. Log into your Ivanti Endpoint Security.
   For additional information, refer to Logging In on page 19.
3. From the **Navigation Menu**, select **Tools** > **Download Agent Installer**.
4. Select the endpoint operating system from the **Operating System** drop-down list.
5. Select the agent version that you want to install on the endpoint from the **Agent Version** drop-down list.

Note: The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab. For additional information, refer to Agent Versions on page 83.

6. Click **Download**.

Result: A ***Download File*** dialog opens, prompting you to save or open the installer.

Deleting an Endpoint

Deleting an endpoint removes its record from the Ivanti Endpoint Security.

Prerequisites:

The endpoints you want to delete must be disabled. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.

Delete endpoints from the ***Endpoints*** page ***All*** tab.

Note: Deleting an endpoint removes its record from the Ivanti Endpoint Security database, but it does not remove the agent on the endpoint.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Ensure the ***All*** tab is selected.
3. Ensure the page is filtered to display disabled agents.
   For additional information, refer to Using Filters on page 42.
4. Select one or multiple endpoints with disabled agents.
5. In the toolbar, click **Delete**.

   Step Result: A ***delete confirmation*** dialog displays.
6. Click **OK** to confirm the deletion.

Result: The endpoint is deleted from the list.

Enabling Modules on an Endpoint

Enabling a module's endpoint component activates the functions an agent's installed module after it has been disabled.

Prerequisites:

Endpoints must have the applicable agent module installed, and the endpoint must be licensed for the agent module. For additional information, refer to Installing Endpoint Modules on page 184.

Enable a module from the applicable ***Endpoints*** page tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the tab for the module that you want to enable for an endpoint.

   Note: The tabs available will vary based on the module(s) you have installed.
3. Select one or more endpoint that does not have the module enabled.
4. From the toolbar, select **Enable** > **Enable Module**.

Result: The module for the selected endpoints is enabled.

Enabling the Ivanti Endpoint Security Agent

Disabled Ivanti Endpoint Security Agents can be reenabled at any time. Enabling a Ivanti Endpoint Security Agent allows it to be included in the security management activities of the Ivanti Endpoint Security.

Enable endpoints from the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the disabled endpoint(s) you want to enable.
3. Click **Enable**.

Tip: You can enable endpoints from any ***Endpoints*** page tab. To enable an endpoint from an ***Endpoints*** page tab other than the ***All*** tab, select **Enable** > **Enable Agent** from the toolbar.

Result: The agent and all modules are enabled.

Disabling Modules on an Endpoint

Disabling a module's endpoint components deactivates the module functions for the endpoint's agent.

Prerequisites:

The module you want to disable must currently be enabled.

Disable a module from the applicable ***Endpoints*** page tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the tab for the module that you want to disable for an endpoint.

Note: The tabs available will vary with which module(s) you have installed.

3. Select one or more endpoints with the agent module enabled.
4. From the toolbar, select **Disable** > **Disable Module**.

Step Result: A notification displays, informing you that disabling the module stops module-related functions.

Note: Disabling a module does not release applicable agent license. To release an agent license, you must completely uninstall the agent module on the endpoints. For additional information, refer to Installing Endpoint Modules on page 184

5. Click **OK** to dismiss the notification.

Result: The module for the selected endpoints is disabled.

Disabling the Ivanti Endpoint Security Agent

Once the Ivanti Endpoint Security Agent on an endpoint is disabled, the installed modules no longer function. Disabled Ivanti Endpoint Security Agents remain listed and can be re-enabled at any time.

Disable endpoints from the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the enabled endpoint(s) you want to disable.
3. Click **Disable**.

Tip: You can enable an endpoint from an ***Endpoints*** page tab. To enable an endpoint from a tab other than the ***All*** tab, select **Disable** > **Disable Agent** from the toolbar.

Result: The endpoint is displayed in the list of endpoints identified with the disabled icon in the **Status** column. After disabling an agent, the endpoint can be deleted from Ivanti Endpoint Security.

Note: Once disabled, the endpoint may not appear in the list based on the **Status** filter settings. To include disabled endpoints in the list, ensure you select **Disabled** or **All** in the **Status** filter.

The Add/Remove Modules Dialog

This dialog lists information about each module license you have purchased. You can also use it to install or remove module endpoint components to or from individual endpoints within your network.

Open this dialog from the ***Endpoints*** page by selecting one endpoint or more and clicking **Manage Modules**.

The following describes each item in the dialog table.

Table 92: Add/Remove Dialog Table

Item	Description
Licenses	The modules you are currently licensed for. A column appears for each module you are licensed for.
Purchased	The number of licenses purchased for the applicable module.
In Use	The number of licenses in use for the applicable module.
Pending	The number of licenses pending installation or removal for the applicable module.
Available	The number of module licenses available for assignment.

The following table describes each column in the dialog list.

Table 93: Add/Remove Dialog List

Column	Description
Endpoint Name	Indicates the name of managed endpoint.
IP Address	Indicates the IP address of the managed endpoint.
Agent Version	Indicates the agent version number defined for the endpoint.
Module Name	Indicates if the module endpoint component for the applicable module is installed on the endpoint. A selected check box indicates the component is installed on the endpoint. A cleared check box indicates the module is not installed on the endpoint.

Note: There is a ***Module Name*** column for each module you have purchased.

Installing Endpoint Modules

Before you can use a module's functions on your Ivanti Endpoint Security network endpoints, you must first install the module's endpoint component on the applicable endpoints. After installing a module endpoint, you can remove it any time.

Prerequisites:

If installing a module's endpoint components, the module's server component must be installed.

Manage module endpoint components for individual endpoints from the ***Add/Remove Modules*** dialog.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the checkbox(es) associated with the endpoints for which you want to manage modules.
3. Click **Manage Modules**.

   Step Result: The ***Add/Remove Modules*** dialog opens.
4. Manage modules for each endpoint.
   - To add a module for a particular endpoint, select the module checkbox for the applicable endpoint.
   - To remove a module for a particular endpoint, clear the module checkbox for the applicable endpoint.

5. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes. The begins installing or uninstalling the selected modules. As module management occurs, the endpoint ***Module*** **Installed** status changes in the ***Endpoint*** page list.

Note: When installing the Device Control endpoint module, target endpoints must be rebooted to complete installation.

Waking Endpoints from the All Tab

After installing Ivanti Wake on LAN, a **Wake Now** button is added to the ***Endpoints*** page ***All*** tab toolbar. Use this button to wake selected endpoints immediately.

Wake endpoints from the ***Endpoints*** page ***All*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the endpoints you want to wake immediately.
3. Click **Wake Now**
4. Click **OK** to dismiss the notification.

Result: Wake requests are sent to the selected endpoints. The endpoints will wake within the next ten minutes.

Using Scan Now to Scan Inventory (Patch and Remediation Tab)

You can initiate a Discover Applicable Updates task at any time. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to the Ivanti Endpoint Security server, which you can view.

You can launch a Discover Applicable Updates task for all network endpoints or selected network endpoints from the ***Endpoints*** page ***Patch and Remediation*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the ***Patch and Remediation*** tab.
3. Schedule a DAU task for all endpoints or selected endpoints.
   Use one of the following methods.

Method	Steps
To schedule a DAU task for all endpoints:	1. Click **Scan Now**. 2. Select **Yes, scan all members of the selected** group check box.

Method	Steps
To schedule a DAU tasks for selected endpoints:	1. From the toolbar, select the check boxes associated with the desired endpoint(s). 2. Click **Scan Now**. 3. Select the **Yes, scan the selected endpoints** check box.

4. Click **Schedule**.
5. Acknowledge the scheduling by clicking **Close**.

Result: The scan is scheduled. As with all deployments, the Discovery Applicable Updates task is scheduled for immediate execution. Deployment occurs the next time the target endpoints communicate with the server.

Rebooting Endpoints

You can use Ivanti Endpoint Security to reboot the managed endpoints on your network. This function is useful after installing content.

Reboot endpoints from the ***Endpoints*** page **Ivanti Patch and Remediation** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the ***Patch and Remediation*** tab.
3. Select the endpoints you want to reboot.
4. Click **Reboot Now**.

   Step Result: The ***Reboot Now*** dialog opens.
5. Select the **Yes, Reboot the selected endpoint** check box.
6. Click **Reboot**.

   Step Result: The system schedules the reboot.
7. Click **Close**.

Result: The dialog closes and the devices reboot the next time they check in with the server.

Waking Endpoints from the All Tab

After installing Ivanti Wake on LAN, a **Wake Now** button is added to the ***Endpoints*** page ***All*** tab toolbar. Use this button to wake selected endpoints immediately.

Wake endpoints from the ***Endpoints*** page ***All*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the endpoints you want to wake immediately.
3. Click **Wake Now**

4. Click **OK** to dismiss the notification.

Result: Wake requests are sent to the selected endpoints. The endpoints will wake within the next ten minutes.

Exporting Endpoint Information

You can export the endpoint information generated in the Ivanti Endpoint Security so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.csv`) file format. For additional information, refer to Exporting Data on page 47.

The Endpoint Details Page

The ***Endpoint Details*** page lists general endpoint information, agent information, the modules installed on the endpoints, the groups the endpoint is included in, and the group policies applied to it. This page also includes a tab for each module installed.

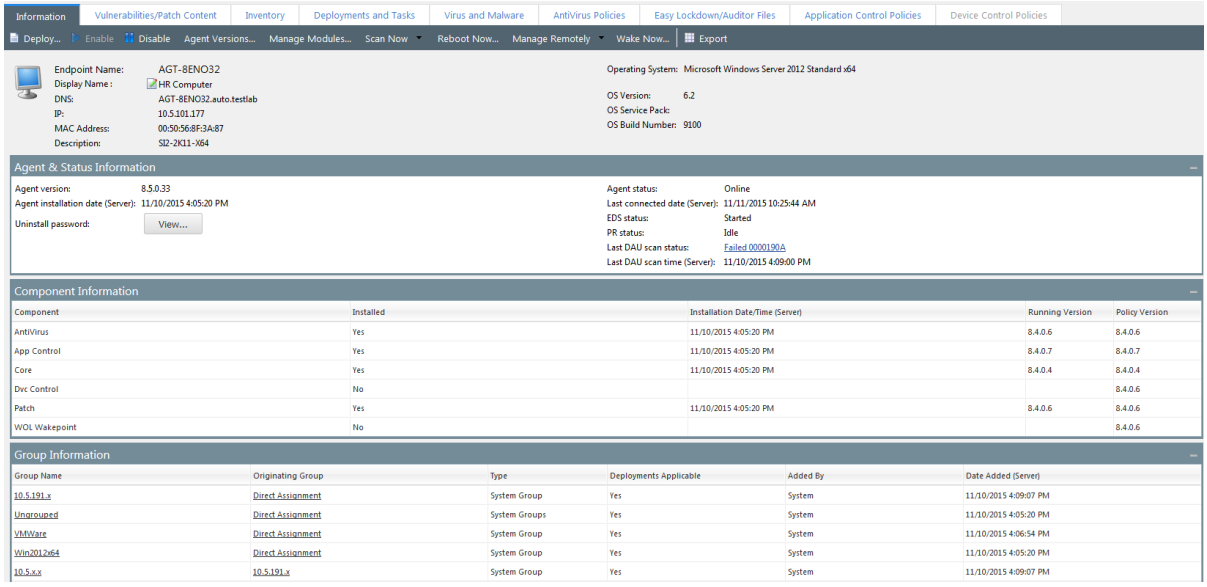


Figure 44: Endpoint Details Page

This page features the following tabs:

- The Information Tab on page 189
- The Vulnerabilities/Patch Content Tab on page 198
- The Security Configuration Tab List on page 202
- The Inventory Tab on page 204
- The Deployments and Tasks Tab on page 207
- The Virus and Malware Tab on page 209
- The Antivirus Policies Tab on page 211
- The Easy Lockdown/Auditor Files Tab on page 212 (Application Control only)
- The Application Control Policies Tab on page 214 (Application Control only)
- The Device Control Policies Tab on page 216 (Device Control only)

Viewing the Endpoint Details Page

The ***Endpoint Details*** page contains comprehensive details for an endpoint and its activity within the Ivanti Endpoint Security system.

View the ***Endpoint Details*** page for an endpoint by clicking an endpoint name link from the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the **Name** link associated with the endpoint details you want to review.

   Step Result: The ***Endpoint Details*** page opens to the ***Information*** tab.
3. [Optional] Complete a task listed in Working with the Endpoint Details Page on page 217.

The Information Tab

The ***Information*** tab displays information about a selected endpoint. The page displays general information organized into endpoint, agent, status, component, group, and policy sections.

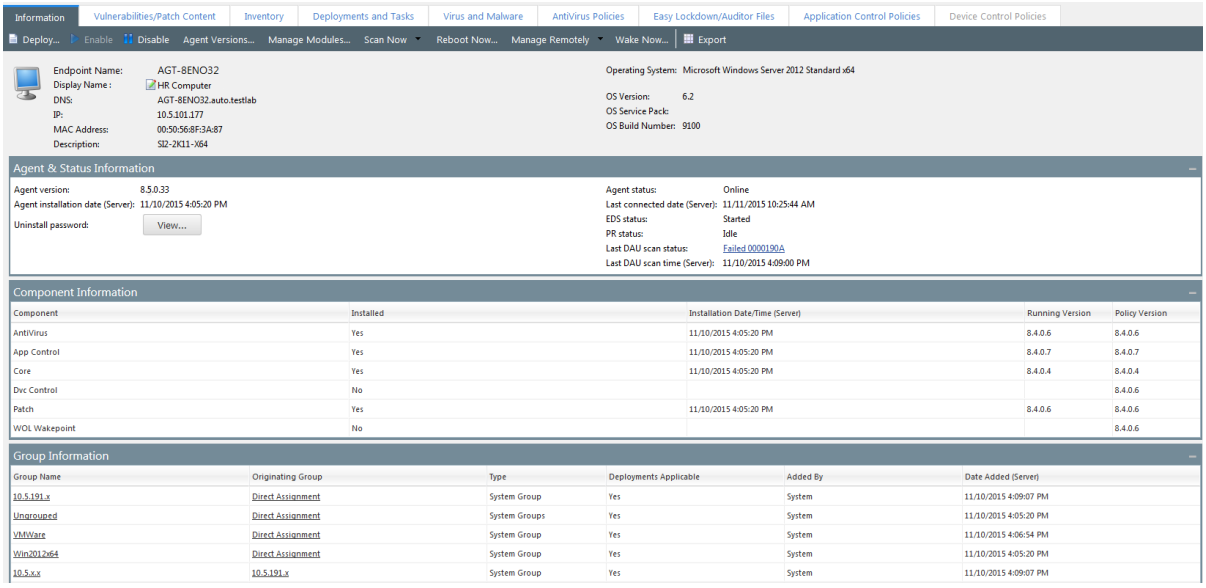


Figure 45: The Information Tab

Tip:

- Each ***Information*** tab section can be collapsed and expanded.
- Each section can also be dragged higher or lower on the page. Place more frequently used information high on the page.

The Information Tab Toolbar

The ***Information*** tab toolbar contains the endpoint assessment tasks and functions that are available for you to perform on managed endpoints.

The following table describes the buttons available in the ***Information*** tab toolbar.

Table 94: Information Tab Toolbar Buttons

Toolbar Button	Description
Deploy...	Opens with ***Deployment Wizard***, which lets you deploy content to the applicable endpoint. For additional information, refer to Deploying Content (Endpoint Details Page) on page 221.
Enable	Enables the endpoint (if it is disabled). For additional information, refer to Enabling an Endpoint on page 222.

Toolbar Button	Description
Disable	Disables the endpoint (if it is enabled). For additional information, refer to Disabling an Endpoint on page 222.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading the Agent on a Single Endpoint on page 219.
Manage Modules...	Opens the ***Add/Remove Modules*** dialog, which lets you manage agent features for modules install on Ivanti Endpoint Security. For additional information, refer to Managing Endpoint Modules on page 225.
Scan Now (Menu)	Opens the **Scan Now** menu.
Discover Applicable Updates... (**Scan Now** Menu Item)	Prompts the Discover Applicable Updates task to immediately check the endpoint. For additional information, refer to Using Scan Now (Endpoint Details Page) on page 226.
Reboot Now... (Patch and Remediation only)	Prompts the selected endpoint to reboot. For additional information, refer to Rebooting Endpoints on page 186.
Update AV Definitions	Updates AntiVirus definitions. For additional information refer to Updating AntiVirusDefinitions on page 227.
Manage Remotely (menu)	Opens the **Manage Remotely** menu. For additional information, refer to Management Options.
Launch Remote Desktop... (**Manage Remotely** menu item)	Launches the log in page for the Windows Remote Desktop Connection (RDC), which allows you to connect to a computer in another location. For additional information, refer to Starting the Remote Desktop Connection.
Launch MMC: Computer Management... (**Manage Remotely** menu item)	Launches the Microsoft Management Console (MMC), which allows you to manage and monitor Windows systems. For additional information, refer to Starting the Microsoft Management Console.
Launch NSLookup... (**Manage Remotely** menu item)	Launches the `NSLookup` MS-DOS command to the endpoint. For additional information, refer to Accessing the NSLookup MS-DOS Command.
Launch Ping... (**Manage Remotely** menu item)	Launches the `Ping` MS-DOS command to the endpoint. For additional information, refer to Accessing the PING MS-DOS Command.

Toolbar Button	Description
Launch Putty... (**Manage Remotely** menu item)	Launches PuTTY, a remote management tool that allows you to remotely control target computers over the Internet. For additional information, refer to Starting the PuTTY Communication Tool.
Launch VNC... (**Manage Remotely** menu item)	Launches the log in page for the Virtual Network Connection (VNC), which allows you to remotely access another computer. For additional information, refer to Starting the Virtual Network Connection Tool.
Wake Now...	Wakes the endpoint. For additional information, refer to Waking Endpoints from the Information Tab on page 227.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Tip: For additional information about using core features, refer to *The Information Tab Toolbar* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Endpoint Information
The fields that appear in this section of the ***Information*** tab contain identifier and operating system details, such as the IP address and the operating system.

The **Endpoint Information** section displays the following endpoint data:

Table 95: Endpoint Information Field Descriptions

Field	Description
Endpoint Name	The name of the endpoint.
DNS	The DNS name of the endpoint.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information you can provide here includes what system it belongs to, where it is located, and what it is used for. The Display Name will appear as a tool-tip when you hover over the Endpoint Name in the on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view).
IP	The IP Address of the endpoint.

Field	Description
MAC Address	The MAC address of the endpoints.
Description	The description of the endpoint, if available.
Operating System	The abbreviated name of the operating system detected on the endpoint.
OS Version	The version number of the operating system running on the endpoint.
OS Service Pack	The service pack level of the endpoint.
OS Build Number	The build number of the operating system running on the endpoint.

Agent Information

The fields that appear in the **Agent Information** section of the ***Information*** tab contain agent status, version, and connectivity details for the agent installed on the endpoint.

The **Agent Information** section displays the following agent data.

Table 96: Agent Information Field Descriptions

Field	Description
Agent version	The version of the agent that the endpoint is currently running. **Note:** A icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.
Agent installation date (Server)	The date and time on the server when the agent registered with Ivanti Endpoint Security. This is typically the date the agent was installed on the endpoint.
Uninstall password (button)	Click **View** to view the uninstall password assigned to the endpoint. See Viewing the Agent Uninstall Password on page 218 for more information.

Status Information
The fields that appear in the **Status Information** section of the ***Information*** tab contain status and connectivity details for the agent installed on the endpoint.

The following fields are added to **Status Information** after Patch and Remediation is installed.

Table 97: Status Information Field Descriptions

Field	Description	
Agent status	Indicates the status of the endpoint. The following list defines column values:	
	Online	The agent is able to communicate with the Ivanti Endpoint Security server in the predefined time period. Refer to Configuring the Agents Tab on page 89 for additional information on configuring agent default behavior.
	Offline	The agent is unable to communicate with the Ivanti Endpoint Security server in the predefined time period. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent will no longer enforce any module policies or complete tasks. All endpoints must show a `Disabled` status in order to delete the endpoint. Refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Last connected date (Server)	The date and time on the server that the agent last communicated with Ivanti Endpoint Security.	
EDS Status	The status of the Endpoint Distribution Service on the server. Service statuses include **Started** and **Stopped**.	
PR status	The Patch and Remediation status for the endpoint.	

Field	Description
Last DAU scan status	The status of the Discover Applicable Updates (DAU) scan when last run. The status also serves as a link to the ***Deployment Results*** page. Status values include: `Success`, `Failure` followed by the failure code, and `Not Available`, which indicates that the endpoint has not checked in. **Note:** The `Not Available` **Last DAU Status** does not serve as a hyperlink.
Last DAU scan time (server)	The time of the last successful DAU scan. A value of `Not Available` indicates the endpoint has not completed a DAU scan.
Last PM reporting time (Server)	The date and time that endpoint last uploaded power management information to the server.

Component Information
This table lists which module components are installed on the endpoint. It also lists additional information about each module.

Information for the Patch and Remediation endpoint module is displayed after its installation.

The following table describes each **Component Information** table column.

Table 98: Component Information Table

Column	Description	
Component	Indicates the name of the applicable module.	
Installed	Indicates whether the module is installed on the endpoint. Values include:	
	Yes	The module is installed.
	No	The module is not installed.
	Pending Install	The module is in the process of installing.
	Pending Uninstall	The module is in the process of uninstalling.
	Pending Reboot	The module has been installed, but the endpoint needs to reboot to complete installation.
	Error	There was an error while installing or uninstalling the module. Click the for additional information about the error.
	Expired	The module license has expired.

Column	Description
Installation Date/Time (Server)	Indicates the date and time on the server that the user initiated a module install.
Running Version	Indicates the version of the module installed on the agent.
Policy Version	Indicates the version of the module that is should be installed based on the agent version defined in the applicable agent policy set.

Group Information

The columns that appear in the **Group Information** section of the ***Information*** tab contain group membership details for the endpoint.

The **Group Information** section displays the following group data for an endpoints.

Table 99: Group Information Column Descriptions

Column	Description
Group Name	The group that the endpoint holds membership in, either through direct assignment or inheritance. Click the group name to open ***Group Information*** page.
Originating Group	The name of the group in the parent hierarchy from which the the endpoint inherits membership. If the endpoint is directly assiged to a group, the value displayed is **Direct Assignment**. Click the value to go to the ***Group Information*** page.
Type	The group type, which can include: • **System Group**: a group created by Ivanti Endpoint Security • **Custom Group**: a group created by a user • **My Groups**: an indication that the group is within the group hieracrchy
Deployments Applicable	Indicates that there are applicable deployments available for this endpoint.
Added By	The Ivanti Endpoint Security user who added the endpoint to the group. If the endpoint was added Ivanti Endpoint Security, the column contains a value of `System`.

Column	Description
Date Added (Server)	The date and time that the endpoint was added to the group.

Note:

- If the values in the **Group Name** and the **Originating Group** columns are identical, then the endpoint is directly assigned to that group and is not inherited..
- Groups listed in gray indicate that the endpoint holds group membership through inheritance.

Policy Information

The fields that appear in the **Policy Information** section of the ***Information*** tab contain details about the policies used by the endpoint during a deployment.

New Ivanti Patch and Remediation policies are listed if they have been applied to the endpoint.

These policies are the results of applying each of the policies defined by the endpoint's group membership and filling in any undefined policies from the Global Policy. Conflict resolution rules are applied when applicable.

Table 100: Policy Information Column Descriptions

Column	Description
Name	The name of the policy applied to the endpoint.
Value	The value of the policy applied to the endpoint.
Description	The description of the policy.

Tip: For a description of all agent policies, including agent policies not applied to the endpoint, refer to The Agent Policy Sets Page List on page 423.

Antivirus Policies

This section lists the antivirus policies assigned, and whether or not that policy set is directly assigned or inherited from a parent. This section only shows the antivirus policies assigned; you cannot use it to assign one. Assign an antivirus policy to the selected group via the **Antivirus Policies** view.

The following reference describes the **Antivirus Policies** table.

Table 101: Antivirus Policies

Field	Description
Policy Name	Indicates the name of the antivirus policy.
Policy Type	Indicates if the antivirus policy type is a *Recurring Virus and Malware Scan* or a *Real-time Monitoring Policy*.

Field	Description
Source	Indicates if the antivirus policy is directly assigned or inherited from a parent.

Antivirus Real-time Monitoring Resultant Policy
If two or more real-time monitoring policies are assigned, their combined resultant effect is displayed in this section. The policy details can only be viewed here; you cannot change or edit them.

The following reference describes the **Antivirus Real-time Monitoring Resultant Policy** table.

Table 102: Antivirus Real-time Monitoring Resultant Policy

Field	Description
Virus Detection Action	Indicates actions to take upon virus/malware detection.
Local users	Indicates real-time scan options for local users.
Services and remote users	Indicates real-time scan options for services and remote users.
Exclude Path/ Filename	Indicates if path(s)/filename(s) will be excluded from the scan
Optional drives	Indicates if optional drives will be included in the scan.

The Vulnerabilities/Patch Content Tab

The ***Vulnerabilities/Patch Content*** tab displays vulnerability information associated with the selected endpoint. The tab displays the same information shown on each ***Patch Content*** page (My Default Patch View, Vulnerabilities, Software, and so on). However, this tab is filtered for the endpoint.

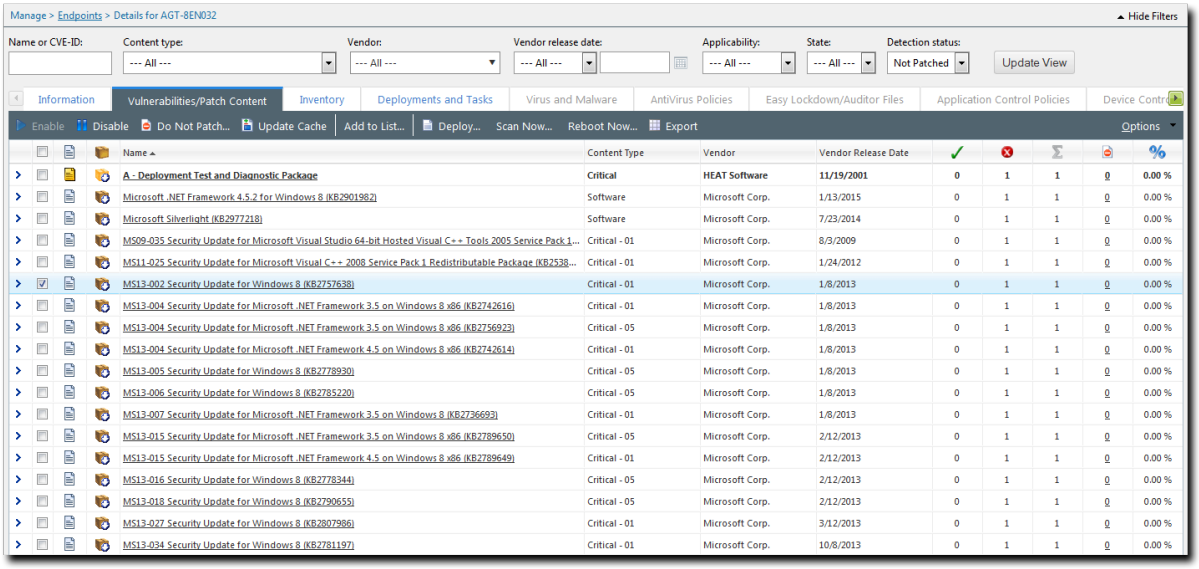


Figure 46: The ***Vulnerabilities/Patch Content*** Tab

The Vulnerabilities/Patch Content Tab Toolbar

The ***Vulnerabilities/Patch Content*** tab toolbar contains the tasks and functions that are available for you to perform on managed endpoints.

Table 103: Vulnerabilities/Patch Content Tab Toolbar Functions

Button	Function
Enable	Enables a selected disabled vulnerability. For additional information, refer to Enabling Content on page 219.
Disable	Disables a selected enabled vulnerability. For additional information, refer to Disabling Content on page 220.
Do Not Patch...	Disables the selected patch for specific groups and endpoint that you select. For more information, see Disabling Content for Groups/Endpoints on page 480.
Update Cache	Updates the package cache for selected packages. For additional information refer, to Updating the Cache on page 220.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Deploying Content (Endpoint Details Page) on page 221.

Button	Function
Scan Now...	Prompts the Discover Applicable Updates task to launch immediately and scan all agent-managed endpoints within your network for vulnerabilities. For additional information, refer to Using Scan Now (Endpoint Details Page) on page 226.
Reboot Now...	Prompts the selected endpoint to reboot. For additional information, refer to Rebooting the Endpoint on page 227.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Vulnerabilities/Patch Content Tab List

The ***Vulnerabilities/Patch Content*** tab list tracks package name, cache status, content type, and deployment data.

The following table describes each list column.

Table 104: Column Definitions

Column	Icon	Definition
Status		The content item status, which indicates when the server downloaded the content item metadata. For additional information, refer to Content Status and Type on page 474.
Package Status		The cache status for the content item, which indicates if the server downloaded the content item packages. For additional information, refer to Content Icons and Descriptions on page 475.
Name	N/A	The content item name, which links to the ***Patch Status*** of the item. For additional information, refer to The Patch Status Page on page 489.

Column	Icon	Definition
Content Type	N/A	Indicates the content item type. For more information, see one of the following topics: • Vulnerabilities on page 461 • Software Content on page 462 • Other Content on page 462
Vendor	N/A	The name of the vendor that created the software in the content item.
Vendor Release Date	N/A	The date and time that the vendor released the software in the content item.
Number of endpoints which came up Patched	✓	The number of endpoints patched with the content item.
Number of endpoints which came up Not Patched	⊗	The number of endpoints not patched with the content item.
Total Applicable	Σ	The number of endpoints that the content item applies to.
Number of endpoints which came up Do Not Patch	⊖	The number of endpoints that administrators have created a patch exception for.
Percent Patched	%	The the percentage of applicable endpoints patched with the content item.

Additionally, you can expand each content item by clicking its arrow (**>**). The following table describes each field that displays when you expand a content item.

The following detail information appears on this page.

Table 105: Content Item Field Descriptions

Name	Description
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Associated packages	The number of packages associated with the content item.
Packages status	The cache status for the content item packages.
Ivanti Endpoint Security ID	The Ivanti Endpoint Security identifier for the content item.

Name	Description
Custom Patch Lists	A listing of all Custom Patch Lists that the content item is included in.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The Ivanti Endpoint Security user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/time (UTC)	The date and time the vendor released the software in the content item.
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

The Security Configuration Tab

The ***Security Configuration*** tab contains security configuration assessment data for endpoints that have agent policy sets that include security configuration benchmarks received during **Security Configuration Assessment** package deployment.

You can expand the assessment sets to view the individual assessments performed on the endpoint. Icons next to the individual assessments indicate if the endpoint passed or failed the assessment.

This tab is only available when you are licensed for the Ivanti Security Configuration Management module, and the module is installed.

The ***Security Configuration*** tab has functionality that allows you export assessment results. The following table describes this functionality.

Table 106: Security Configuration Export Functionality

Button	Definition
Export	Exports the security configuration assessment results in .csv file format. For additional information, refer to Exporting SCM Data to CSV.
Export XCCDF	Exports the security configuration assessment results in XML eXtensible Checklist Configuration Description Format (XCCDF). For additional information, refer to Creating the XCCDF Export Job.

The Security Configuration Tab List

The **Security Configuration** tab list tracks security configuration benchmark identification information, assessment parameters, and assessment status data.

The following table describes the column headers found on the **Security Configuration** tab.

Table 107: Column Definitions

Column	Icon	Definition
Benchmark	N/A	Indicates the security configuration assessment benchmark applied to the endpoint through an agent policy set.
Profile	N/A	Indicates the benchmark profile applied to the endpoint.
Assessment Engine	N/A	Indicates the version number of the check tool in use at the time the benchmark was uploaded.
Date Assessed	N/A	Indicates the date on which the endpoint was assessed.
Number of assessments which came up Compliant		Indicates the number of assessments that the endpoint passed.
Number of assessments which came up Non-Compliant		Indicates the number of assessments that the endpoint failed.
Number of assessments which came up Error		Indicates the number of assessments that did not run.
Total Percent Complete		Indicates the percentage of assessments that the endpoint passed.

Individual Assessment Results Fields

The ***Assessment Details*** window contains fields that provide a narrative description of the assessment and the criteria applied to determine passed/failed status.

The following table describes the columns that appear in the assessment details table. These are the values that the assessment criteria are evaluated against.

Note: You can click the **Expand** button to view the registry location evaluated by the assessment.

Table 108: Column Definitions

Column	Definition
TestID	A unique identifier for the assessment.
Actual Value	The value found on the endpoint by the assessment.
Operation	The mathematical operation between the actual value and the expected value that was performed during assessment.
Expected Value	The value that, if found, would result in a pass result.
Result	The end result of the criterion assessment.

The Inventory Tab

The **Inventory** tab displays the inventory information for the selected endpoint. Inventory is organized by hardware device class. The page displays the same information as is presented in the ***Inventory*** page.

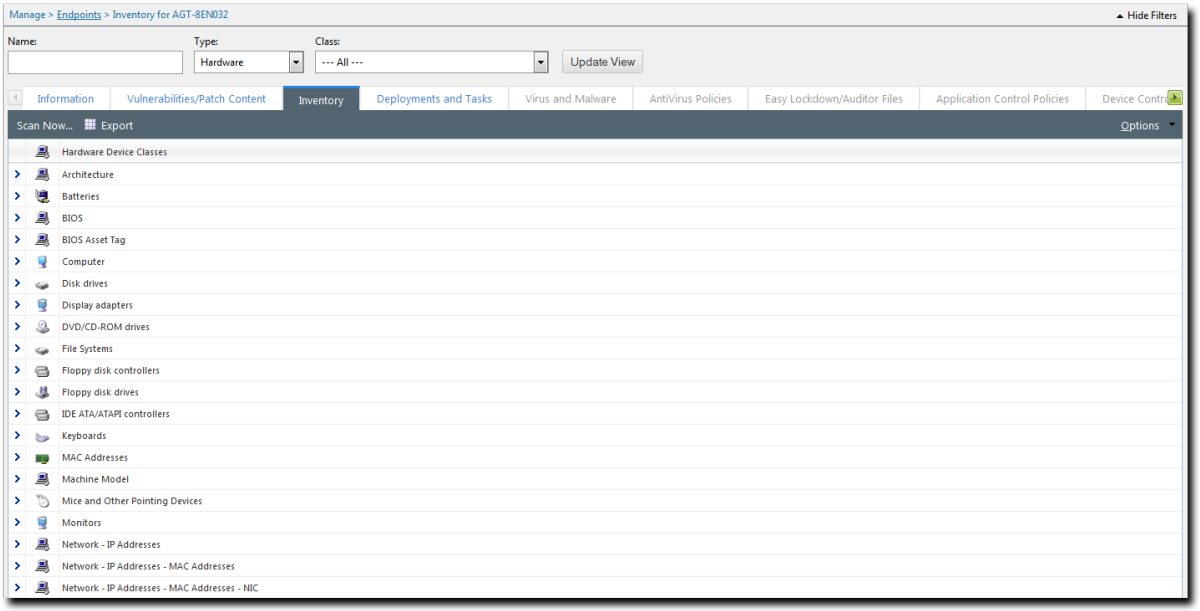


Figure 47: Inventory Tab

The Inventory Tab Toolbar

The ***Inventory*** tab toolbar contains functions that allow you to detect inventory on managed endpoints.

The following table describes the toolbar functions used in the ***Inventory*** tab.

Table 109: Device Inventory Tab Toolbar Functions

Toolbar Item	Description
Scan Now...	Prompts the Discover Applicable Updates (DAU) task to launch on the endpoint. For additional information, refer to Using Scan Now (Endpoint Details Page) on page 226.

Toolbar Item	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Inventory Tab List
The ***Inventory*** tab lists the components found on each endpoint registered with the Ivanti Endpoint Security Server. From this tab you can view info about the operating system, software, hardware, and services found on the endpoint. You can change the inventory listed on the page by selecting a

Operating System Inventory
When the ***Inventory*** tab filter row is set to type **Operating System**, the page list displays the following information:

Column	Description
Operating System	The operating system installed on the endpoint.
	The number of endpoints that the operating system is installed on. This is the total number of endpoints running this operating system, not just the endpoint you're working with.

Software Inventory
When the ***Inventory*** tab filter row is set to type **Software Programs**, the page list displays the following information:

Column	Description
Software Programs	The software programs installed on the endpoint. There's a row for each program.
	The number of endpoints that the program is installed on. This is the total number of endpoints that have this program installed, not just the endpoint you're working with.

Hardware Inventory
When the ***Inventory*** tab filter row is set to type **Hardware**, the page list displays the following information:

Column	Definition
Icon	An icon that depicts the **Hardware Device Class**.
Hardware Device Classes	Indicates the hardware device class.

Each **Hardware Device Class** can be expanded to list class devices found on endpoints. To expand a class, click the **rotating chevron** (**>**). The following table describes the columns that display after expanding a class.

Column	Definition
Device	Indicates the hardware devices found for the class.
Icon	Indicates the number of endpoints that host the device.

Services Inventory

When the ***Inventory*** tab filter row is set to type **Hardware**, the page list displays the following information:

Column	Definition
Service Name	The name of the service on the endpoint.
System Name	The filepath that the service is running from.
Current State	The state that the service is in.
Startup State	The state the service enters upon startup.

The Deployments and Tasks Tab

The ***Deployments and Tasks*** tab lists the deployments assigned to an endpoint and their status. Deployments remain listed until deleted.

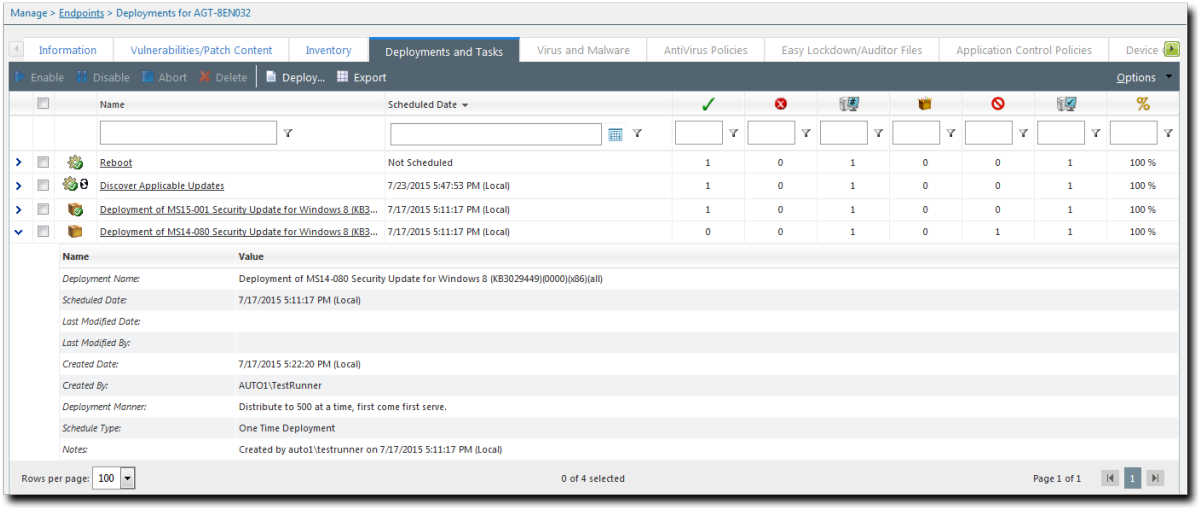


Figure 48: Deployments Tab

The Deployments and Tasks Tab Toolbar

The ***Deployments and Tasks*** tab toolbar contains buttons that let you control existing deployments and export deployment data.

The following table describes each toolbar button.

Table 110: Deployments and Tasks Tab Toolbar Functions

Menu Item	Function
Enable	Enables the selected disabled deployment. For additional information, refer Enabling Deployments on page 223.
Disable	Disables the selected deployment. For additional information, refer to Disabling Deployments on page 223.
Abort	Cancels the deployment or task for any endpoints which have not already received the deployment package. For additional information, refer to Aborting Deployments on page 224.
Delete	Removes the deployment from your Ivanti Endpoint Security. For additional information, refer to Deleting Deployments on page 224.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Deploying Content (Endpoint Details Page) on page 221.

Menu Item	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Deployments and Tasks Tab List

The ***Deployments and Tasks*** tab list contains a record of each deployment for the endpoint. Each list item remains until deleted.

The following table describes each list column.

Table 111: Deployments and Tasks Tab List Column Descriptions

Column	Icon	Description
Action	N/A	Contains **Edit** and **Delete** icons you can use to control packages in a deployment. For additional information see: • Editing Package Deployment Options on page 255 • Deleting Deployments on page 259
Name	N/A	The name of an individual package or task included in a deployment targeted at the endpoint (*not* the name of the deployment itself). Click the name display ***Deployment Details***. For more information, see The Deployment Details Page on page 292.
Scheduled Date	N/A	The date and time a user scheduled the package or task to deploy.
Status Icon	N/A	An icon that indicates the status of the package deployment. For information on what each icon means, see Deployment Status Icons on page 252.
Number of Successful Endpoints	✓	The total number of endpoints and groups that finished the deployment successfully.
Number of Failed Endpoints	⊗	The total number of endpoints and groups that finished the deployment unsuccessfully.
Number of Endpoints Assigned to the Deployment		The total number of endpoints and groups that are assigned to the deployment.

Column	Icon	Description
Number of In Progress Endpoints		The total number of endpoints and groups that are receiving the deployment. **Note:** If you deploy to a group using Agent Local Time, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.
Total Not Deployed		The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, or marked *Do Not Patch*).
Number of Endpoints That Have Completed the Deployment		The total number of endpoints and groups that finished the deployment.
The Percentage of Completed Endpoints		The percentage of endpoints and groups that finished the deployment. Percentage = [Total Finished endpoints / Total Assigned endpoints]

The Virus and Malware Tab

Use the ***Virus and Malware*** tab on the ***Endpoint Details*** page provides a view of all alerts generated by virus and malware scans performed by Ivanti AntiVirus on a selected endpoint.

The information and features enable you to:

Review current status	You can see the types of malware that have been detected and the endpoints that have been infected. This information will help you to determine how the infection originated and the best way to handle it.
Take remedial action	You can use Scan Now to launch the ***Virus and Malware Scan Wizard***, configuring it to perform specific actions that will reduce the threat to the network. See Using the Virus and Malware Scan Wizard for more information.

The Virus and Malware Tab Toolbar
Enables you to perform functions on the listed event alerts, and to run an on-demand scan on a selected endpoint.

Table 112: Virus and Malware Tab Toolbar

Button	Function
Scan Now	Opens the ***Virus and Malware Scan Wizard***. This enables an administrator to react to incoming alerts with an immediate scan on the endpoint. When configured appropriately, this scan can eliminate the problem by cleaning or deleting the infected files. For more information on running these scans, see Using the Virus and Malware Scan Wizard.
Remove	Removes the selected event alert(s) from the list.
Export	Exports the event alerts list to a comma separated value (`.csv`) file.

Note: Only event alerts from the previous 90 days are displayed. If there are a large number of event alerts and you no longer need to view all of them, you can use the **Remove** button to remove unwanted alerts from the list. This does not delete them from the database, however, so you can always view these removed alerts by generating an appropriate report.

The Virus and Malware Tab List
Provides a comprehensive and constantly updated list of all event alerts generated by virus and malware scans performed on the endpoint.

Table 113: Virus and Malware Event List

Column	Description
Virus/Malware Name	The name of the virus or malware detected. **Note:** If a virus or malware is detected by behavior-based techniques such as Sandbox, it will not have a unique name. Instead, the column will indicate how the malware was identified. **Note:** Each example links to the relevant entry in the ***Virus/Malware Details*** page.
Alert Source	The type of scan that generated the alert: • Real-time Monitoring Policy • Recurring Virus and Malware Scan • Scan Now

Column	Description
Alert Message	The message related to the alert status: •  (Cleaned) •  (Deleted) •  (Not Cleaned) •  (Quarantined) **Note:** Both the *Cleaned* status and *Deleted* status use the same icon because in both cases the malicious code has been removed and no longer presents a danger.
File Name	The name of the file in which the malware was detected.
File Path	The file path of the file in which the malware was detected.
Last Detected Date (Server)	The date and time the alert was generated (server time).

Tip: You can use the **Group By** row, available above the list, to sort list items into groups based on column headers. This feature (along with the filters above the toolbar) is useful when you need to examine a large number of event alerts.

The Antivirus Policies Tab

Use the **Antivirus Policies** tab on the ***Endpoint Details*** page to manage antivirus policies for a selected endpoint.

The Antivirus Policies Tab Toolbar

Contains the tasks and functions that are available for you to perform on an endpoint with AntiVirus features enabled.

Table 114: Antivirus Policies Toolbar Buttons

Button	Function
Create	Enables you to create a *Recurring Virus and Malware Scan* policy or a *Real-time Monitoring Policy*.
Assign	Assigns the selected policy to one or more endpoints or groups.
Un-assign	Un-assigns the selected policy from one or more endpoints or groups.
Export	Exports the selected policy to a comma separated value (`.csv`) file. See Exporting Data on page 47 for more information.

Button	Function
Options	Features options to set page views, filter data, and enable clipboard copy. See The Options Menu on page 39 for more information.

The Antivirus Policies Tab List
Provides information on existing antivirus policies assigned or inherited by a selected endpoint.

Table 115: Antivirus Policies List Columns

Column	Description
Select check box	Select this check box to perform an action on the policy.
Status	An icon representing whether the policy is enabled or disabled.
Policy Name	The name given by the policy creator.
Policy Type	• Recurring Virus and Malware Scan • Real-time Monitoring Policy
Source	Defines whether the policy is assigned or inherited.
Assigned Date (Server)	The server date and time when the policy was assigned to the endpoint.

The Easy Lockdown/Auditor Files Tab

Use the **Easy Lockdown/Auditor Files** tab on the ***Endpoint Details*** page to view the files that existed on a selected endpoint when an Easy Lockdown or Easy Auditor policy was assigned to it.

Note: This content is only available when the Application Control module is installed.

The Easy Lockdown/Auditor Files Tab Toolbar
The ***Easy Lockdown/Auditor Files*** tab toolbar contains buttons that you can use to allow or deny file use for the endpoint.

The following table describes each toolbar button.

Table 116: Easy Lockdown/Auditor Files Tab Toolbar

Button	Description
Authorize...	Opens the ***Authorize Selected Files*** dialog, which you can use authorize the selected files for the applicable endpoint. For additional information, refer to Authorizing Selected Files in Application Library.
Deny...	Opens the Deny Selected Files dialog, which you can use to deny the selected files for the applicable endpoint. For additional information, refer to Denying Selected Files in Application Library.

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Easy LockDown/Auditor Files Tab List

The ***Easy LockDown/Auditor Files*** tab contains a list of files and file details found during audits. This list is similar to the list featured on the ***Application Library*** page.

The following table describes each column in the tab list.

Table 117: Files List Columns

Column	Description
Verification	Indicates whether the file has been assessed by the Ivanti Endpoint Integrity Service.
File Name	The file name, including extension.
File Version	File version number.
First Found Path	The path where the file was first discovered by Application Control.
Company Name	The company that created the file.
Product Name	The product that the file is part of.
Certificate	The status of the file's certificate (if it has one): • None - there is no certificate. • Present - there is a certificate but it is not yet verified. • Valid - certificate is verified and not expired. • Expired - certificate was verified but is now expired.
Date Added To Library (Server)	The date and time that the file was added to Application Library, shown as server time (UTC).

The Application Control Policies Tab

Use the **Application Control Policies** tab on the ***Endpoint Details*** page to manage Application Control policies for a selected endpoint.

Note: This content is only available when the Application Control module is installed.

The Application Control Policies Tab Toolbar

The ***Application Control Policies*** tab toolbar contains buttons you can use to create and manage Application Control policies.

The following table describes each toolbar button.

Table 118: Application Control Policies Tab Toolbar

Button	Description
Create... (menu)	Opens the **Create** menu.
Trusted Publisher... (menu item)	Opens the ***Trusted Publisher*** dialog, which you can use to create trusted publisher policies.
Trusted Updater... (menu item)	Opens the ***Trusted Updated*** dialog, which you can use to create trusted updater policies.
Easy Auditor... (menu item)	Opens the ***Easy Auditor*** dialog, which you can use to create easy auditor policies.
Easy Lockdown... (menu item)	Opens the ***Easy Lockdown*** dialog, which you can use to create easy lockdown policies.
Assign... (menu)	Opens the **Assign** menu.
Trusted Publisher... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.
Trusted Path... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.
Trusted Updater... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.
Local Authorization... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.

Button	Description
Denied Applications Policy... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.
Easy Auditor... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.
Easy Lockdown... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.
Supplemental Easy Lockdown/Auditor Policy... (menu item)	Opens the ***Assign Policy*** dialog, which you can use to assign a policy to groups or endpoints.
Unassign	Unassigns the selected policy (or policies) from the applicable groups and endpoints.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Application Control Policies Tab List

The ***Application Control Policies*** tab contains a listing of Application Control policies assigned to the endpoint.

The following table describes each list column.

Table 119: Application Control Policies Tab List

Column	Description
Action	Removes the policy from the applicable groups and endpoints.
Status	Indicates the status of the policy (`Enabled` or `Disabled`).
Policy Name	Indicates the policy name.

Column	Description
Policy Type	Indicates the policy type (`Trusted Publisher`, `Trusted Path`, `Trusted Updater`, `Local Authorization`, `Denied Applications`, `Easy Auditor`, `Easy Lockdown`, or `Supplemental Easy Lockdown/Auditor`).
Source	Indicates the policy source.
Assigned Date (Server)	Indicates the date and time the policy was assigned to the applicable endpoints and groups.

The Device Control Policies Tab

Use the ***Device Control*** **Policies** tab on the ***Endpoint Details*** page to manage Device Control policies for a selected endpoint.

Note: This content is only available when the Device Control module is installed.

The Device Control Policies Tab Toolbar

The ***Device Control Policies*** tab toolbar contains buttons you can use to create and manage Device Control policies for the applicable endpoint.

The following table describes each toolbar button.

Table 120: Device Control Policies Tab Toolbar

Button	Description
Create	Displays a drop-down menu that allows you to select the type of policy to create. **Note:** A user should have **Manage Centralized DC Policies** access rights to access this functionality.
Assign	Opens the ***Assigned Users and Endpoints*** dialog for the selected policy. **Note:** This button is enabled only if the user has **Assign Centralized DC Policies** access rights and a policy is selected from the list.
Unassign	Allows you to unassign the selected policy. **Note:** This button is enabled only if the user has **Assign Centralized DC Policies** access rights and an assigned policy is selected from the list.
Delete	Allows you delete the selected policy. **Note:** This button is enabled only if the user has **Manage Centralized DC Policies** access rights.

Button	Description
Edit	Opens the respective policy wizard with the policy details. **Note:** This button is enabled only if the user has **Manage Centralized DC Policies** access rights.
Enable	Allows you enable a policy that is currently disabled.
Disable	Allows you disable a policy that is currently enabled.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Device Control Policies Tab List

The ***Device Control Policies*** tab contains a listing of Device Control policies assigned to the endpoint.

The following table describes each list column.

Table 121: Device Control Policies List Columns

Field	Description
Status	The enabled or disabled status of the policy.
Policy Name	The name of the policy.
Assigned	The assigned or unassigned status of the policy.
Device Class	The device class to which the policy applies.
Device Collection	The device collection to which the policy applies.
Last Update (Server)	The date the policy was modified last.

Working with the Endpoint Details Page

You can perform a number of tasks related to endpoints from the ***Endpoint Details*** page. You perform most of these tasks regardless of the tab selected. However, certain tasks are specific to certain tabs.

To perform most tasks associated with endpoints, click a toolbar button. To perform some tasks, selecting one or multiple endpoints from the page list may be necessary.

The following list displays the tasks you can perform from the ***Endpoint Details*** page.

Note: For additional information about features included in the default installation, refer to *Working with the Endpoint Details Page* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Viewing the Agent Uninstall Password

If you need to uninstall the agent from an endpoint, you will be prompted to enter a password during the uninstall. You can view this uninstall password from the ***Endpoint Details*** page for the endpoint.

View the agent uninstall password from the endpoint's ***Endpoint Details*** page ***Information*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the ***Name*** link for the relevant endpoint.

   Step Result: The ***Endpoints Details*** page opens to the ***Information*** tab.
3. From the toolbar, click **View**.

Result: The ***Agent Uninstall Password*** dialog opens, displaying the password. Record the password if necessary. Close the dialog when you are done.

The Agent Uninstall Password Dialog

The ***Agent Uninstall Password*** dialog contains the endpoint's name and the password that is required to uninstall the agent locally from an endpoint.

The following table describes the fields that appear on the ***Agent Uninstall Password*** dialog.

Table 122: Agent Uninstall Password Dialog Fields

Field	Description
Endpoint name	The endpoint's name.
Agent uninstall password	The password required to uninstall the agent from the endpoint locally.

Upgrading the Agent on a Single Endpoint

From the ***Endpoint Details*** page, you can upgrade the Ivanti Endpoint Security Agent installed on the endpoint to a newer version.

Define the agent version for the endpoint from the ***Information*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link associated with endpoint you want to define agent version(s) for.

   Step Result: The ***Endpoint Details*** page for the endpoint opens to the ***Information*** tab.
3. Click **Agent Versions**.

   Step Result: The ***Manage Agent Versions*** dialog opens.
4. Select an agent version from the **Agent Version** list.

   Note: The agent versions available for selections are defined from the ***Options*** page. For additional information, refer to Configuring the Agents Tab on page 89.
5. Click **OK**

Result: The ***Manage Agent Versions*** dialog closes. If an agent version other than the defined version is installed on the endpoints, the defined version is installed over the previous version.

Enabling Content

After disabling a content item, you can renable it from the ***Vulnerabilities/Patch Content*** tab. You can only deploy enabled content.

You can re-enable content from the ***Endpoint Details*** page ***Vulnerabilities/Patch Content*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to enable content for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Select the ***Vulnerabilities/Patch Content*** tab.
4. [Optional] Use the page filters to sort content.
5. Select one or multiple disabled content items from the list.
6. Click **Enable**.

Result: The content item displays with the **Enabled** icon in the status column.

Disabling Content

Disabling a content item will prevent that content item from being deployed.

You can disable content from the ***Endpoint Details*** page ***Vulnerabilities/Patch Content*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to disable content for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Select the ***Vulnerabilities/Patch Content*** tab.
4. [Optional] Use the page filters to sort content.
5. Select one or multiple content items from the list.
6. Click **Disable**.

   Note: If you disable a content item that's already been cached, the package will not be updated if a new version of the content item is released.

Result: The content item displays with the **disabled** icon in the status column.

Updating the Cache

Updating the cache initiates a process that gathers the packages associated with the selected vulnerability and copies those packages to your Ivanti Patch and Remediation Server.

You can update the cache for content from the ***Endpoint Detail*** page ***Vulnerabilities/Patch Content*** tab.

Note: For optimum installation order, Ivanti recommends caching content prior to deployment. Failure to cache content prior to deployment may result in repeated endpoint reboots that interrupt work flow on those endpoints.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint for which you want to cache content for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Select the ***Vulnerabilities/Patch Content*** tab.
4. [Optional] Use the page filters to sort content.
5. Select the check boxes associated with the content to cache.
6. Click **Update Cache**.

   Step Result: The ***Warning*** dialog box opens, informing you that the update request and this action may take an extended period of time.

   Note: The cache will not be updated for disabled content items that have had a new version released.

7. Click **OK**.

Result: The selected content begins caching.

Deploying Content (Endpoint Details Page)

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including the tabs of the ***Endpoints Details*** page. When deploying from this page, the ***Deployment Wizard*** is preconfigured according to the tab you deploy from.

For additional information, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the ***Patch and Remediation*** tab.
3. Click the link in the **Name** column that corresponds to the endpoint for which you want to deploy content for.

   Step Result: The ***Endpoints Details*** page opens.

4. Deploy content.

   To deploy content, select a tab and complete the applicable substeps. Tab selection controls how the ***Deployment Wizard*** is preconfigured for deployment.

Tab	Steps
To deploy content from the *Information* tab:	1. Ensure the ***Information*** tab is selected. 2. Click **Deploy** The ***Deployment Wizard*** opens, preconfigured to deploy content to the selected endpoint.

Tab	Steps
To deploy content from the *Vulnerabilities/Patch Content* tab:	1. Select the ***Vulnerabilities/Patch Content*** tab. 2. Select the content you want to deploy. 3. Click **Deploy** The ***Deployment Wizard*** opens, preconfigured to deploy the selected content to the selected endpoint.
To deploy content from the *Deployments and Tasks* page:	1. Select the ***Deployments and Tasks*** tab. 2. Click **Deploy**.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Enabling an Endpoint

Enabling an endpoint includes the endpoint in the content management activities of the Ivanti Endpoint Security.

You can enable an endpoint from the ***Endpoint Details*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to enable.
   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Click **Enable**.

Result: The endpoint is enabled.

Disabling an Endpoint

Disabling an endpoint stops agent functions on an endpoint. Disabled endpoints are not included in security management activity.

You can disable an endpoint from the ***Endpoint Details*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds with the endpoint you want to disable.
   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Click **Disable**.
   Step Result: A ***disable confirmation*** dialog displays.

4. In the ***confirmation*** dialog box, click **OK**.

Result: The endpoint is disabled. After disabling an agent, the endpoint can be deleted from Ivanti Endpoint Security.

Note: Once disabled, the endpoint may not appear in the ***Endpoints*** page list based on the **Status** filter settings. To include disabled devices in the list, ensure you select **Disabled** or **All** in the **Status** filter.

Enabling Deployments

Enabling deployments resumes disabled (or paused) deployments to continue.

You can enable deployments from the ***Endpoint Details*** page ***Deployments and Tasks*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to enable deployments for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Select the ***Deployments and Tasks*** tab.
4. [Optional] Use the page filters to sort deployments.
5. Select the disabled deployments you want to enable.
6. Click **Enable**.

Result: The selected deployments are enabled.

Disabling Deployments

Disabling deployments pauses deployments and stops the distribution of package(s) to an endpoint that has not already received the deployment.

You can disable deployments for a specific endpoint from the ***Endpoint Details*** page ***Deployments and Tasks*** tab.

Note: You cannot disable deployments of system task packages.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to disable deployments for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Select the ***Deployments and Tasks*** tab.
4. [Optional] Use the page filters to sort deployments.
5. Select the deployments you want to disable.

6. Click **Disable**.

Result: The selected deployments are disabled.

Aborting Deployments

Aborting deployments cancels deployments for the endpoint that has not already received the deployment.

Note: The endpoints that have already received the deployment will not be affected. The deployment will be aborted for endpoints that have not yet received the deployment.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to abort deployments for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Select the ***Deployments and Tasks*** tab.
4. [Optional] Use the page filters to sort deployments.
5. Select the deployments you wish to abort.
6. Click **Abort**.

   Step Result: A confirmation message displays, asking you to confirm that you want to abort the deployment.
7. Click **OK** to confirm that you want to abort the deployment.

Result: The selected deployment is canceled.

Note: You cannot abort system tasks or Mandatory Baseline deployments.

Deleting Deployments

Deleting deployments removes them from Ivanti Endpoint Security. Delete a deployment if you to prevent its content from reaching endpoints.

You can delete deployments for individual endpoints from their ***Endpoint Details*** page ***Deployments and Tasks*** tab.

Note: Deleting deployments has no effect on endpoints that have already received the deployments. You cannot delete system task deployments.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to delete deployments for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Select the ***Deployments and Tasks*** tab.
4. [Optional] Use the page filters to sort deployments.
5. Select the deployments you want to delete.
6. Click **Delete**.

Note: Before you can delete a deployment in progress, you must abort the deployments

Step Result: A confirmation message displays, asking you to confirm that you want to delete the selected deployments.

7. Click **OK** to delete the deployments.

Managing Endpoint Modules

You may select which module license an endpoint's agent uses. Using this feature allows you control which modules apply to a particular endpoint.

Manage modules for individual endpoints from the ***Add/Remove Modules*** dialog.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link for the endpoint you want to work with.

   Step Result: The ***Endpoints Details*** page opens.

3. Click **Manage Modules**.

   Step Result: The ***Add/Remove Modules*** dialog opens.

4. Manage modules for each endpoint.
   - Select an empty checkbox to add a module.
   - Clear selected checkboxes to remove a module.
5. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes and modules are either installed or uninstalled according to your changes.

Viewing Individual Assessment Results

After you have collected security assessment data from your managed endpoints, you can view assessment results for the individual assessments performed on an endpoint. Assessment details include a narrative description of the assessment and the criteria applied to determine passed/failed status.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to export security configuration assessment data for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Select the ***Security Configuration*** tab.
4. Click the **Expand** button to view a security configuration benchmark. Continue expanding the assessment groups until the individual assessments are displayed.
5. Click the hyperlink for the individual assessment that you want to view.

   Step Result: The ***Assessment Details*** window for the assessment displays.
6. Click the **Expand** button to view the registry location evaluated by the assessment.
7. To change the way the data is displayed in the window, perform one of the following.
   - Click **Table** to display the data in a formatted table. This is the default view.
   - Click **XML** to display the data in its native XML format.

Using Scan Now (Endpoint Details Page)

You can initiate a Discover Applicable Updates task at any time. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to the Ivanti Endpoint Security server, which you can view.

You can schedule a Discover Applicable Updates task for the selected endpoint the ***Endpoint Details*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the ***Patch and Remediation*** tab.
3. Click the *Endpoint Name* link of the endpoint you want to schedule a Discover Applicable Updates task for.

   Step Result: The ***Endpoint Details*** page for the endpoint opens.
4. Select one of the following tabs:
   - ***Information***
   - ***Vulnerabilities***
   - ***Inventory***
5. From the toolbar, click **Scan Now**.

   Note: If scheduling from the Information tab, select **Scan Now** > **Discover Applicable Updates**.
6. Select the **Yes, scan the selected endpoint** check box.
7. Click **Schedule**.
8. Acknowledge the scheduling by clicking **Close**.

Result: The scan is scheduled. As with all deployments, although the Discovery Applicable Updates task is scheduled for immediate execution. It will not actually occur until the next time the agent checks in.

Rebooting the Endpoint

You may reboot an endpoint at any time. Rebooting an endpoint may be necessary following some deployments.

You can reboot an individual endpoint from its ***Endpoint Details*** page ***Information*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds with the endpoint you want to reboot.
3. Select one of the following tabs:
   - The **Information** tab
   - The **Vulnerabilities/Patch Content** tab
4. Click **Reboot Now**.

   Step Result: The ***Reboot Now*** dialog opens.
5. Select the **Yes, Reboot the selected device** check box.
6. Click **Reboot**.

   Step Result: The system schedules the reboot.
7. Click **Close**.

Result: The window closes.

Updating AntiVirusDefinitions

Update an endpoint's anti-virus definitions to help maintain its security.

You can update an endpoint's antivirus definitions from the ***Endpoint Details*** page ***Information*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint for which you want to update antivirus definitions for.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Click **Update AV Definitions**.

Result: The endpoints anti-virus definitions begin updating.

Waking Endpoints from the Information Tab

After installing, a **Wake Now** button is added to the ***Endpoint Details*** page ***Information*** tab. From this tab, you can wake an individual selected endpoint.

You can wake endpoints from the ***Endpoint Details*** page ***Information*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.

2. Click the **Endpoint Name** link for the endpoint you want to wake.

   Step Result: The ***Endpoint Details*** page opens to the ***Information*** tab.

3. Click **Wake Now**.
4. Click **OK** to dismiss the notification.

Result: A wake request is sent to the endpoint. The endpoint will wake within ten minutes.

Exporting Endpoint Information

You can export the endpoint information generated in the Ivanti Endpoint Security so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.csv`) file format. For additional information, refer to Exporting Data on page 47.

Adding a Display Name to an Endpoint

You can associate an alternate name (50 characters maximum) with an endpoint to help you identify and distinguish it.

Use the Display Name to provide endpoint decision-making information like what system it belongs to, where it is located, and what it is used for.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to add a Display Name to.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Beside the **Display Name**, click the **Edit** icon.

   Step Result: An editable field appears.

4. Enter a word or phrase up to 50 characters in length. If you leave the field blank the **Endpoint Name** will be used.

5. Click the **Save** icon ( ) .

Note: The **Cancel** icon ( ) cancels your changes and anything you enter is not saved.

Result: A Display Name is added to the Endpoint information. It will appear on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view):

- Tool-tip when you hover over the Endpoint Name.
- Display Name column of Endpoint lists (the tool-tip when you hover over a Display Name is the Endpoint Name).
- Display Name column of the comma separated list (CSV) file you export.

Tip: You can filter endpoints by Display Name using the **Display Name** filter.

Editing the Display Name of an Endpoint

You can edit the alternate name associated with an endpoint on the **Manage** > **Endpoints** Information tab.

The Display Name is used to provide endpoint decision-making information like what system it belongs to, where it is located, and what it is used for.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to add a Display Name to.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Beside the **Display Name**, click the **Edit** icon.

   Step Result: An editable field appears.
4. Enter a word or phrase up to 50 characters in length. If you leave the field blank the **Endpoint Name** will be used.
5. Click the **Save** icon ( ).

Note: The **Cancel** icon ( ) cancels your changes and anything you enter is not saved.

Result: The Display Name is changed. It will appear on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view):

- Tool-tip when you hover over the Endpoint Name.
- Display Name column of Endpoint lists (the tool-tip when you hover over a Display Name is the Endpoint Name).
- Display Name column of the comma separated list (CSV) file you export.

Tip: You can filter endpoints by Display Name using the **Display Name** filter.

Removing the Display Name of an Endpoint

You can remove the alternate name associated with an endpoint on the **Manage** > **Endpoints** Information tab.

The Display Name is used to provide endpoint decision-making information like what system it belongs to, where it is located, and what it is used for.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to add a Display Name to.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Beside the **Display Name**, click the **Edit** icon.

   Step Result: An editable field appears.
4. Remove the name from the field.
5. Click the **Save** icon ( ).

Note: The **Cancel** icon ( ) cancels your changes and anything you enter is not saved.

Result: The custom Display Name is removed and the Endpoint Name is used instead. It will appear on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view):

- Tool-tip when you hover over the Endpoint Name.
- Display Name column of Endpoint lists.
- Display Name column of the comma separated list (CSV) file you export.

Chapter 8

Using Inventory

In this chapter:

After installing agents on network endpoints, you can view a list of operating systems, software applications, hardware devices, and services installed and running on the endpoints registered to the Ivanti Endpoint Security server. This list is known as *inventory*.

The ***Inventory*** page lists all inventory devices found in the your network. You can use this page to track the devices installed on specific endpoints.

About Inventory

Inventory captures a comprehensive view of the functional components of each agent. An inventory list of software, hardware, operating systems, and services installed on an endpoint can be retrieved. The inventory list displays items by inventory type.

In addition to viewing the list of inventory items, the inventory results can be exported to a file (`.csv`). Inventory information is also available at the endpoint and group level.

Note: Ivanti Endpoint Security only captures inventory data for endpoints that have the agent installed.

Viewing Inventory

After you have installed an agent on an endpoint, you can view the endpoint's inventory.

1. Select **Manage** > **Inventory**.

   Step Result: The ***Inventory*** page displays.

2. [Optional] Select your filter options.
3. Click **Update View**.

   Step Result: The inventory results display.

4. Click the applicable rotating chevron (**>**) to view the details of a particular inventory **Class**.

The Inventory Page

The ***Inventory*** page displays an inventory list. You can filter this list to display operating systems, software, hardware, or services detected in your network.

Unlike most list pages, which feature static columns, the ***Inventory*** page list columns that change based on how you filter the page. Select different items from the **Type** filter to change the list columns.

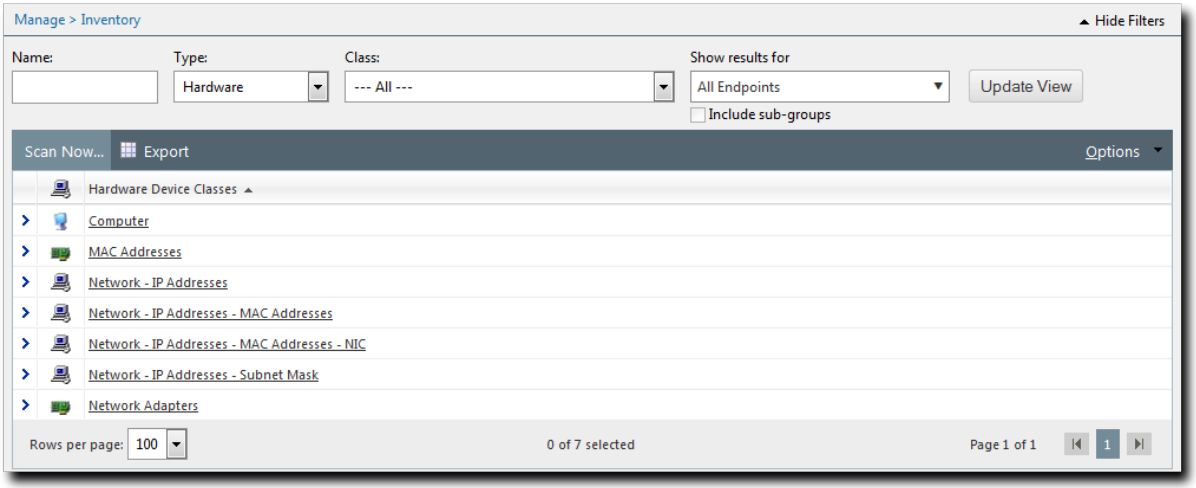


Figure 49: Inventory Page

The following topics describe the ***Inventory*** page list based on how you filter it:

- The Inventory Page List (Filtered for Operating Systems) on page 233
- The Inventory Page List (Filtered for Software) on page 234
- The Inventory Page List (Filtered for Hardware) on page 235
- The Inventory Page List (Filtered for Services) on page 236

The Inventory Page Toolbar

The ***Inventory*** page toolbar contains functions that are allow you to detect inventory on managed endpoints.

The following table describes the toolbar functions used in the ***Inventory*** page.

Table 123: Endpoint Inventory Page Toolbar Functions

Toolbar Item	Description
Scan Now...	Prompts the Discover Applicable Updates (DAU) task to launch for all endpoints. For additional information, refer to Using Scan Now to Scan Inventory (Inventory Page) on page 237.

Toolbar Item	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Inventory Page List (Filtered for Operating Systems)

When viewing the ***Inventory*** page, you can filter the page list to display information about all operating systems detected in your network. Expanding list items displays the endpoints running the applicable operating system.

The following table describes the list that displays when the **Operating Systems** type is selected. Filtering using this type displays information about the operating systems detected in your network. Click the (>) icon to expand each list item.

Table 124: Inventory Page List (Filtered for Operating Systems)

Column	Icon	Description
Operating System	N/A	The name of an detected within the network. A list item is available for every operating system detected within your network. Each name is a link to the ***Endpoints with Inventory*** page, which displays endpoints running the applicable operating system.
Number of Endpoints		The number of endpoints running the operating system.

The following table describes the information displayed when you expand an ***Inventory*** page list item (filtered for operating systems). The expanded list item displays Information about each endpoint running the applicable operating system.

Table 125: Expanded List Item (List Filtered for Operating Systems)

Column	Description
Endpoint Status	The icon representing the endpoint status. You can hover over the icon with your mouse to get a text description of the endpoint status. For more information, refer to Agent Module Status Icons on page 168.

Column	Description
Endpoint Name	The name of the endpoint. Clicking the ***Endpoint Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
OS Info	Any additional information about the operating system. This column typically lists any service packs installed.

The Inventory Page List (Filtered for Software)

When viewing the ***Inventory*** page, you can filter the page list to display information about all software installed on endpoints in your network. Expanding list items displays the endpoints hosting the softwaree.

The following table describes the list that displays when the **Software** type is selected. Filtering using this type displays each software program detected in the network. Click the (>) icon to expand each list item.

Table 126: Inventory Page List (Filtered for Software)

Column	Icon	Description
Software Programs	N/A	The name of a software program detected in the network. The name is a link to the ***Endpoint with Inventory*** page, which lists each endpoint hosting the software program.
Number of Endpoints		The number of endpoints hosting the software program.

The following table describes the information that displays when you expand an ***Inventory*** page list item (filtered for software). The expanded list item displays Information about each endpoint hosting the software.

Table 127: Expanded List Item (List Filtered for Software)

Column	Description
Endpoint Status	The icon representing the endpoint status. You can hover over the icon with your mouse to get a text description of the endpoint status. For more information, refer to Agent Module Status Icons on page 168.
Endpoint Name	The name of the endpoint. Clicking the ***Endpoint Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
OS Info	Any additional information about the operating system. This column typically lists any service packs installed.

The Inventory Page List (Filtered for Hardware)

When viewing the ***Inventory*** page, you can filter the page list to display information about all hardware detected in your network. Expanding list items displays the hardware devices found for a hardware class. Fully expanding list items displays the endpoints that host a specific hardware device.

The following table describes the list when the **Hardware** type is selected. Filtering using this type displays information about all hardware classes. Click the (>) icon to expand each list item.

Table 128: Inventory Page List (Filtered for Hardware)

Column	Description
Inventory Icon	The icon representing the hardware device class.
Hardware Device Classes	The hardware device classification.

The following table displays the information that displays when you expand an ***Inventory*** page list item (filtered for hardware). The expanded list item displays Information about the applicable hardware device class. Each item can be further expanded. Click the (>) icon to expand each device list item.

Table 129: Expanded List Item (List Filtered for Inventory)

Column	Icon	Description
Device	N/A	The name of a hardware device detected in your network. The name is a link to the ***Endpoint with Inventory*** page, which lists all endpoints hosting the hardware device.
Number of Endpoints		The number of endpoints hosting the hardware device.

The following table describes the information that displays for a fully expanded ***Inventory*** page list item (filtered for hardware). The fully expanded list item displays information about each endpoint that hosts the applicable hardware device.

Table 130: Expanded Hardware Device

Column	Description
Endpoint Status	The icon representing the endpoint status. You can hover over the icon with your mouse to get a text description of the endpoint status. For more information, refer to Agent Module Status Icons on page 168.
Endpoint Name	The name of the endpoint. Clicking the ***Endpoint Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.

Column	Description
OS Info	Any additional information about the operating system. This column typically lists any service packs installed.

The Inventory Page List (Filtered for Services)

When viewing the ***Inventory*** page, you can filter the page list to display information about all service operating in your network. Expanding list items displays the endpoints running the service.

The following table describes the list that displays when the **Services** type is selected. Filtering using this type displays information about services detected in the network. Click the (>) icon to expand each list item.

Table 131: Inventory Page List (Filtered by Services)

Column	Icon	Description
Service Name	N/A	The name of a service operating in your network. Each name is a link to the ***Endpoint with Inventory***, which lists each endpoint running the applicable service.
Number of Endpoints		The number of endpoints running the service.

The following table describes the information that displays when you expand an ***Inventory*** page list item (filtered for services). The expanded list item displays information about each endpoint running the applicable service.

Table 132: Expanded List Item (List Filtered for Services)

Column	Description
Endpoint Status	The icon representing the endpoint status. You can hover over the icon with your mouse to get a text description of the endpoint status. For more information, refer to Agent Module Status Icons on page 168.
Endpoint Name	The name of the endpoint. Clicking the ***Endpoint Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
OS Info	Any additional information about the operating system. This column typically lists any service packs installed.

About Scan Now (Scanning Inventory)

The Discover Applicable Updates task scans an endpoint for inventory.

In addition to determining security risks and other vulnerabilities, the Discover Applicable Updates (DAU) task also identifies the endpoint inventory. Each time the DAU runs, the current inventory

is compared against the `%Installation Directory%\HEAT Software\EMSSAgent\live\patch\localprofile.txt` file. If any changes exist, a differential report is uploaded to the Ivanti Endpoint Security server.

The DAU task occurs at least once daily and following successful deployments.

Using Scan Now to Scan Inventory (Inventory Page)
You can initiate a Discover Applicable Updates task at any time. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to the Ivanti Endpoint Security server, which you can view.

You can launch Discover Applicable Updates (DAU) tasks that scan all managed endpoints from the ***Inventory*** page.

1. Select **Manage** > **Inventory**.
2. Click **Scan Now**.

   Step Result: The ***Scan Now*** dialog opens.
3. Select the **Yes, scan all endpoints** check box.
4. Click **Schedule**.

   Step Result: A DAU task for all endpoints is scheduled
5. Click **Close** to dismiss the scheduling notification.

Using Custom Inventory

To use a custom inventory file, you must create the custom inventory file in XML and distribute it to each agent.

To distribute a custom XML file, create an XML file named CustomInventory.xml, an then add it to a custom patch that you create using the ***Package Editor Wizard***. The custom patch should install to the following filepaths:

- For Windows endpoints, `<Program Files>\HEAT Software\HEATAgent\live\patch\CustomInventory.xml`
- For Linux, Unix, or Mac endpoints, `<installdir>/update/conf.d/custominventory.xml`

For more information on creating a package, see Using the Package Editor on page 515.

Afterward, deploy the custom patch to your Patch endpoints. For more information, see Using the Deployment Wizard on page 260.

Guidelines for Linux/Unix/Mac-based Operating Systems

Using the syntax in this section, you can create custom inventory for Linux, Unix, or Mac-based operating systems.

The following section defines the valid XML guidelines for setting up custom inventory scripts for Linux/Unix/Mac based Operating Systems. In each case, the item will be added to the hardware inventory under the Default device class unless a specific device class (`item class=""`) is defined.

Literal

Allows the user to assign an actual text value type into XML.

The string added will be of the form "`name = value`" where `name` is the tag name, and `value` is the literal typed between the open and close tags.

Example XML (This example will return the string value defined between the open and close tags):

```
<item class="User Defined" name="Example Name" type ="Literal">
    Ivanti 8.6 Custom Inventory
</item>
```

Returns:

```
"Example Name = Ivanti 8.6 Custom Inventory"
```

Dynamic

Allows the user to search using a script.

The string added will be of the form "`name = value`" where `name` is the tag name, and `value` is the result of the script.

Example XML:

```
<item class="System" name="Ivanti Disk Usage" type="dynamic">
    <command>
        <!-- Define shell -->
        <shell>
            <![CDATA[/bin/sh]]>
        </shell>
        <!-- Define execution directory -->
        <dir>
            <![CDATA[/tmp]]>
        </dir>
        <envs>
            <env>
                <!-- Define the JAVA HOME environment variable -->
                <EnvName>
                    <![CDATA[JAVA HOME]]>
                </EnvName>
                <EnvValue>
                    <![CDATA[/usr/local]]>
                </EnvValue>
            </env>
        </envs>
        <!-- Script -->
        <content>
            <![CDATA[echo -n 'du -ks /usr/local/work/Ivanti \(in kb\)]]>
        </content>
    </command>
</item>
```

Returns:

```
"Ivanti Disk Usage = 18.1 (in kb)"d
```

Guidelines for Microsoft Windows-based Operating Systems

Using the syntax in this section, you can create custom inventory for Windows-based operating systems.

The following section defines the XML guidelines for setting up custom inventory scripts for Windows-based operating systems. In each case, the item will be added to the hardware inventory under the default device class unless a specific device class (`item class=""`) is defined.

Literal

Allows the user to assign an actual text value type into XML.

The string added will be of the form `"name = value"` where `name` is the tag name, and `value` is the literal typed between the open and close tags.

Example XML: (This example will return the string value defined between the open and close tags)

```
<item class="User Defined" name="Example Name" type="Literal">
    Ivanti 8.6 Custom Inventory
</item>
```

Returns:

```
"Example Name = Ivanti 8.6 Custom Inventory"
```

Registry

Allows the user to retrieve the registry key value.

The string added will be of the form `"name = value"` where `name` is the tag name and `value` is the value stored under the identified registry key.

Example XML (This example will return, from the Registry, the location and name of the custom inventory file):

```
<item name="Registry Example" type="registry">
    HKEY_LOCAL_MACHINE\Software\PatchLink.com\DiscoveryAgent\InventoryInputFile
</item>
```

Returns:

```
"Registry Example= C:\ProgramFiles\Ivanti\CustomInventory.xml"
```

Environment

Allows the user to return the value of an environment value.

The string added will be of the form `"name = value"` where `name` is the tag name and `value` is the expanded environment variable defined.

Example XML (This example will return the value of the defined environment variable):

```
<item name="Environment Example" Class="User Defined" type="Environment">
    %PROCESSOR_ARCHITECTURE%
</item>
```

Returns:

```
"Environment Example = i386"
```

WMI

Windows Management Instrumentation (WMI) allows the user to use scripting to control the WMI component, and tends to focus on operating system settings.

In the case of a WMI item, two additional attributes, `namespace` and `query` are used. If the namespace attribute is not specified, the default value of `ROOT\CIMV2` is used. The query attribute must be defined as a valid WQL query. The string added will be of the form `"name = value"` where `name` is the tag name and `value` is the actual value for the specified WMI property.

Example XML (This example will return the Serial Number property from the Operating System):

```
<item name="Windows SN" type="wmi" query=" SELECT * FROM Win32_OperatingSystem">
    SerialNumber
</item>
```

Returns:

```
"Windows SN = ABCD-EFGH-IJKL"
```

Example XML (This example will retrieve the Manufacturer property of the device):

```
<item name="Device Manufacturer" type="wmi" query=" SELECT * FROM Win32_OperatingSystem">
    Manufacturer
</item>
```

Returns:

```
"Device Manufacturer = Computer Manufacturer A"
```

Text_File

Allows the user to retrieve text data from a file.

The string added will be of the form `"name = value"` where each line of the text file contains a Name/Value pair separated with a delimiter (defined with the `delimiter` attribute). For each valid line, in the text file, an entry will be added to inventory. When specifying a file name an environment variable, such as `%WINDIR%` can be used.

Example XML (This example will return the Name/Value pairs from a `TXTSample.txt` file in the Windows directory):

```
<item name="ti" type="text_file" delimiter="=">
    %WINDIR%\TXTSample.txt
</item>
```

Returns:

```
"Line 1 = This is line one" Line 2 = This is line two"
```

Note: Each line item retrieved from the text file cannot exceed 200 characters. In the event that a line within a defined text file exceeds 200 characters, Ivanti recommends truncating the line item below the 200 character limit.

XML_File

Allows the user to retrieve text data from a file.

An external XML file will be referenced. The XML file structure must be defined by the `XPath` string. When specifying an XML file name an environment variable, such as `%WINDIR%` can be used.

Example XML (This example will return the value of the Asset Number tag from the `SampleXML.xml` file in the Windows directory):

```
<item name="Asset" type="xml_file" xpath="/Top/Inventory/AssetNumber">
    %WINDIR%\SampleXML.xml
</item>
```

Returns:

```
"Asset = PLA001"
```

Example XML (This example will return the value of the Location tag from the `SampleXML.xml` file in the Windows directory):

```
<item name="Building" type="xml_file" xpath="/Top/Inventory/Location">
    %WINDIR%\SampleXML.xml
</item>
```

Returns:

```
"Building = Scottsdale-Main"
```

Where the `SampleXML.xml` file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>

<Top>
    <Inventory>
        <AssetNumber>PLA001</AssetNumber>
        <Location>Scottsdale-Main</Location>
    </Inventory>
</Top>
```

An example XML file, using the valid Windows agent inventory options, is provided below:

```
<?xml version="1.0" encoding="utf-8"?>

<customInventory>
    <items>
        <item name="l1" class="User Defined" type="literal">
            value1
        </item>
        <item name="r1"class="My New Class" type="registry">
            HKEY_LOCAL_MACHINE\Software\PatchLink.com\DiscoveryAgent\InventoryInputFile
        </item>
        <item name="e1" class="My New Class" type="environment">
            %PROCESSOR_ARCHITECTURE%
        </item>
        <item
            name="w1"
            class="My New Class"
            type="wmi"
            namespace="ROOT\CIMV2"
            query="SELECT * FROM Win32_OperatingSystem">
            SerialNumber
        </item>
        <item name="t1" class="My New Class" type="text_file" delimiter="=">
            c:\sampleInventoryText.txt
        </item>
        <item name="x1" class="My New Class" type="xml_file" xpath="//inventory/AssetTag">
            c:\sampleInventoryXML.xml
        </item>
    </items>
    </customInventory>
```

Where the `C:\SampleInventory.txt` file is as follows:

```
Building = MainLocation = Scottsdale, AZDivision = Corporate
```

And the `C:\SampleInventoryXML.xml` file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>

    <inventory>
        <AssetTag>
            PLA00012
        </AssetTag>
    </inventory>
```

Chapter 9

Managing Deployments and Tasks

In this chapter:

A *deployment* initiates the download of security content by the agent to an endpoint for installation. It is the instruction set for a package, supplying an agent with the rules and conditions for deployment.

A deployment comprises all the information needed to perform the task(s) associated with the content. This includes required files and scripts for installing content, stopping a service, validating a system condition, or changing a database entry. The deployment is the mechanism that carries and supports a package.

A *task* is a deployment that initiates a system task. It contains no software or patches. Use tasks to reboot network endpoints or initiate DAU tasks.

About Deployments

The term *deployment* refers to the process of sending content items to managed endpoints.

Several key concepts and status indicators are associated with a deployment. These concepts are used to define deployment behavior.

The following topics include some of the key concepts and indicators that give definition to a deployment.

Topic	Description
Explaining Deployment Distribution Order on page 244	The order that the deployment is submitted to target endpoints.
Deployment Types on page 244	Deployments can be based on content, packages, or a Mandatory Baseline.
Standard and Chained Deployments on page 245	Deployments are processed as either standard or chained.

Explaining Deployment Distribution Order

When deploying more than one package to an individual endpoint or group of endpoints, the deployments can be scheduled to process at different times. Order is also influenced by deployment type, status, and reboot requirements.

Important: You must install an agent on an endpoint in order to deploy content to the endpoint. A deployment is assigned to the agent installed on an endpoint.

Deployments proceed in the following order prior to regularly scheduled system tasks and agent processes:

1. Chained deployments
2. Standard deployments
3. System Task: Reboot
4. Task – Reboot System
5. Discover Applicable Updates (DAU)

Although no deployment occurs before its scheduled time, a chained deployment whose scheduled time has elapsed will always precede a standard deployment whose scheduled time has also elapsed.

If multiple chained deployments are scheduled and some endpoints have the final reboot suppressed, the determination of a reboot override is based on the last scheduled deployment.

Deployment Types

Deployments are based on the content-type being deployed and how the content is being deployed. Deployment types include System Tasks, Package Deployments, and Mandatory Baseline Deployments.

System Task	System tasks are Ivanti Endpoint Security deployments where no actual patch content is deployed. Rather, they are instructions for the Ivanti Endpoint Security Agent to execute to determine if an endpoint is in need of patch content, and then further instructions to complete deployment of patch content. There are two types of System tasks: • Discover Applicable Updates: this task, also called a DAU, is a Ivanti Endpoint Security Agent scan that determines whether endpoints have applicable patch content available on the Global Subscription Service installed. By default Ivanti Endpoint Security schedules a global DAU for all endpoints every twenty six hours following replication, but you can modify DAU schedules using Agent Policy Sets. Additionally, DAUs run five minutes after the Ivanti Endpoint Security Agent installs a patch, immediately following an endpoint reboot, or immediately when you use the **Scan Now** feature. • Reboot: this task is usually executed following installation of a patch. You can also manually schedule a reboot as well.

Package Deployment	These deployments are a user-scheduled deployment of patch content. They include all patch content you select when completing the ***Deployment Wizard***. When the package deployment begins at the time you schedule, the Ivanti Endpoint Security Agent runs scripts on the endpoint you targeted for deployment. These scripts identify whether the patch content included in the deployment applies to the endpoint. If the patch content applies, the content is installed. For additional information, refer to About Packages on page 501.
Mandatory Baseline Deployment	Unlike package deployments, which are scheduled by the user, Mandatory Baseline deployments are deployments that Ivanti Endpoint Security automatically initiates. Here's how it works: You can form a group of endpoints, and then select the patch content that group members must have installed at all times—a mandatory baseline. Every DAU will check to make sure that patch content included in the mandatory baseline is installed. If patch content from the mandatory baseline is missing, Ivanti Endpoint Security deploys the patch content to incompliant endpoint immediately. For additional information, refer to About Mandatory Baselines on page 352.

Standard and Chained Deployments

Deployments come in two varieties: standard deployments and chained deployments.

Standard Deployment	A standard deployment is a deployment that has not been chained with another deployment. While not all standard deployments require a reboot, if the included package does require one and the reboot is suppressed, the endpoint will not accept additional deployments until it is rebooted.
Chained Deployment	A chained deployment is a deployment grouped with other deployments so the endpoint will not reboot after each one. Following the first chained deployment, the endpoint will accept only chained deployments until rebooted.

Reboot and Chained State
The reboot and chained states are the result of an endpoint not performing the required reboot following a deployment.

Table 133: Reboot and Chained State

State	Description
Reboot State	Indicates that the endpoint received a standard deployment requiring a reboot, but the reboot was suppressed. While in the reboot state, the agent only accepts deployments. A reboot deployment or a manual reboot clears this state.
Chained State	Indicates that the agent received a chained deployment in which the reboot was suppressed. While in the chained state, the agent only accepts another chained deployment or a reboot deployment.

The following deployments always perform a reboot.

Table 134: Reboot Deployments

Deployment	Description
Reboot System Package	A system task that is automatically added to the end of chained deployments where the final reboot is not suppressed. This is also sent to agents when you click the **Reboot Now** button on the ***Endpoints*** page.
Task - System Reboot	A task that permits the user to schedule a reboot using the scheduling features of the ***Schedule Deployment Wizard***.

Standard packages reboot for one of the following reasons:

- The deployed package required and forced the reboot (unless suppressed), during the installation.
- The package installer determined that it required a reboot.
- The reboot flag was sent to the agent. It is not necessary that the agent receive the Reboot System Package or Task. The agent performs the reboot on its own.

The Deployments and Tasks Page

Deployments, Virus and Malware Scans, and system tasks are reviewed on the ***Deployments and Tasks*** page. The page list displays each deployment job and the individual deployments or scans assigned to it.

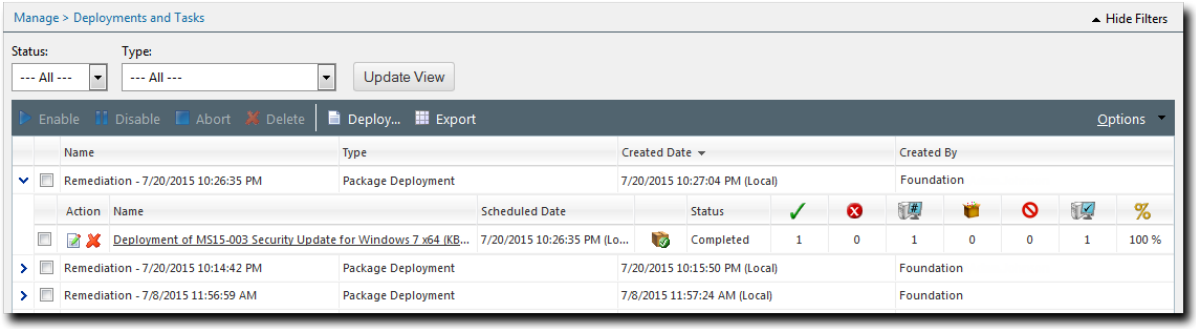


Figure 50: Deployments and Tasks Page

- For additional information about deployments, refer to About Deployments on page 243.
- For additional information about antivirus scans, refer to About Scan Now.

Viewing Deployments and Tasks

There are several pages within the Ivanti Endpoint Security from which you can view deployments and system tasks. Based on the page from which you are viewing deployments, deployments may be organized by content type, endpoints, groups, or deployments themselves.

You can view deployments and system tasks on the following pages:

Table 135: Deployment Pages

Navigation Menu	Menu Item	Menu Sub-Item
Review	**Vulnerabilities**	**All**
		Critical Vulnerabilities
		New Vulnerabilities
		Top Vulnerabilities
	Software	**All**
		Service Packs
		Software Installers
		Updates
	Other	**All**

Navigation Menu	Menu Item	Menu Sub-Item
		Detection Only
		Informationals
		Packages
		Policies
		Recommended
		System Management
		Tasks
		Virus Removal
Manage	**Endpoints** (***Patch and Remediation*** tab)	
	Endpoints	***Endpoint Details*** (***Vulnerabilities/Patch Content*** tab, ***Deployments and Tasks*** tab) **Note:** To access this page, click an endpoint link from the ***Endpoints*** page list.
	Groups	***Group Membership*** view
		Endpoint Membership view
		Vulnerabilities/Patch Content view
		Deployments and Tasks view
	Deployments and Tasks	

Viewing All Deployments and Tasks
You can view all deployments and system (either executed or scheduled) within Ivanti Endpoint Security from the ***Deployment and Tasks*** page. This page displays all system deployments, regardless of the page used to schedule the deployment.

View all system deployments and tasks from the ***Deployments and Tasks*** page.

Note: Recurring Virus and Malware Scans do not appear on this page.

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.
2. [Optional] Select the desired filter criteria and click **Update View**.

3. [Optional] To view the details for a deployment or task, expand a list item by clicking a rotating chevron (**>**).

Viewing Deployments and Tasks within Endpoints
You can view the deployments and tasks assigned to a specific endpoint from its ***Endpoint Details*** page. This page shows only the deployments for the selected endpoint, not the entire system.

View the deployments and tasks for an endpoint from the ***Endpoint Details*** page ***Deployments and Tasks*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select your filter options and click **Update View**.

   Step Result: The applicable endpoints display in the ***Endpoints*** page.
3. Click the link for an endpoint with at least one deployment or task to view its details.

   Step Result: The ***Endpoint Details*** page opens.
4. Select the ***Deployments and Tasks*** tab.

   Step Result: The ***Deployments and Tasks*** tab opens.
5. [Optional] To view details for a deployment or task, expand it by clicking the applicable rotating chevron (**>**).

Result: The deployment details display.

Viewing Deployments and Tasks within Groups
You can view deployments and tasks for specific endpoint groups from the ***Groups*** page. When viewing group deployments, you can only view deployments for the selected group; other system deployments are not listed.

View group deployments and tasks from the ***Groups*** page ***Deployments and Tasks*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. In the ***Groups*** page, select **Deployments and Tasks** from the **View** drop-down list.

   Step Result: The ***Deployments and Tasks*** view displays next to the ***Browser***.
3. Select a group from the browser.

Result: The selected group is highlighted and displays the assigned deployments and tasks.

The Deployments and Tasks Page Toolbar

This toolbar contains buttons that let you create new deployments, control existing deployments, and export deployment data.

The following table describes each toolbar button

Table 136: Deployments and Tasks Page Toolbar Functions

Menu Item	Function
Enable (Patch and Remediation only)	Enables the selected disabled deployment or task. For additional information, refer to Enabling Deployments on page 254.
Disable (Patch and Remediation only)	Disables the selected enabled deployment or task. For additional information, refer to Disabling Deployments on page 254.
Abort (Patch and Remediation only)	Cancels the deployment or task for any endpoints which have not already received the deployment package. For additional information, refer to Aborting Deployments and Tasks on page 254.
Delete (Patch and Remediation only)	Removes the deployment or task from your Ivanti Endpoint Security. For additional information, refer to Deleting Deployments on page 259.
Deploy... (Patch and Remediation only)	Deploys the selected packages or tasks. For additional information, refer to Deploying Content (Deployments and Tasks Page) on page 259.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Deployments and Tasks Page List

A record of each default deployment and each deployment that you have created resides in the ***Deployments and Tasks*** page list.

The following table describes the columns that appear in the ***Deployments and Tasks*** page list. Expand the deployment list item to view all the available column headers for the item.

Table 137: Deployments and Tasks Page List Column Descriptions

Column	Description
Name	The name of the deployment.
Type	The deployment type. For more information, see Deployment Types on page 244.
Created Date	The date and time a user created the deployment.
Created By	The user that created the deployment.

You can expand deployments to view the packages that are included in them. Expand deployments clicking the **Arrow** icon (**>**). The following table describes each column for an expanded deployment.

Table 138: Expanded Deployment Columns

Column	Icon	Description
Action	N/A	Contains **Edit** and **Delete** icons you can use to control packages in a deployment. For additional information see: • Editing Package Deployment Options on page 255 • Deleting Deployments on page 259
Name	N/A	The name of the package or task in the deployment. Click the name to display its ***Deployment Details*** page. For additional information, see The Deployment Details Page on page 292.
Scheduled Date	N/A	The date and time a user scheduled the package or task to deploy.
Status Icon	N/A	An icon that indicates the status of the package deployment. For information on what each icon means, see Deployment Status Icons on page 252.
Status	N/A	The status of the package deployment.
Number of Successful Endpoints	✓	The total number of endpoints and groups that finished the deployment successfully.
Number of Failed Endpoints	⊗	The total number of endpoints and groups that finished the deployment unsuccessfully.

Column	Icon	Description
Number of Endpoints Assigned to the Deployment		The total number of endpoints and groups that are assigned to the deployment.
Number of In Progress Endpoints		The total number of endpoints and groups that are receiving the deployment. **Note:** If you deploy to a group using Agent Local Time, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.
Total Not Deployed		The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, or marked *Do Not Patch*).
Number of Endpoints That Have Completed the Deployment		The total number of endpoints and groups that finished the deployment.
The Percentage of Completed Endpoints		The percentage of endpoints and groups that finished the deployment. Percentage = [Total Finished endpoints / Total Assigned endpoints]

Deployment Status Icons
When viewing deployments, you can quickly identify their progress by looking at the deployment status icons.

Table 139: Deployment Status Icons

New[1]	Current[2]	Local [3]	System[4]	MB[5]	Status	Description
					Aborted	The deployment was aborted.
					Disabled	The deployment was disabled.
					Scheduled	The deployment is scheduled.
					Deploying	The deployment is in progress.

New[1]	Current[2]	Local [3]	System[4]	MB[5]	Status	Description
					Completed	The deployment finished successfully. **Note:** The deployment is considered successful even if one or more endpoints were marked *Do Not Patch* and did not receive the deployment.
					Completed with Failures	The deployment finished unsuccessfully.
					No Deployment Target	The deployment did not occur because the patch did not apply to any endpoints.

1. New Package
2. Current Package
3. Local Package
4. System Package
5. Mandatory Baseline Package

Working With Deployments and Tasks

There are several procedures associated with deployments and tasks that manage and deploy content. The controls to begin these procedures are available on the ***Deployments and Tasks*** page toolbar.

You can perform the following tasks from the ***Deployments and Tasks*** page:

- Aborting Deployments and Tasks on page 254
- Disabling Deployments on page 254
- Enabling Deployments on page 254
- Editing Package Deployment Options on page 255
- Deleting Deployments on page 259
- Deploying Content (Deployments and Tasks Page) on page 259

Aborting Deployments and Tasks

Aborting deployments cancels deployments for endpoints that have not already received the deployment. Abort deployments when you do not want endpoints to receive their packages.

Abort deployments from the ***Deployments and Tasks*** page.

Note:

- Aborted deployments only affect endpoints that have not yet received the deployment. Endpoints that have already received the deployment are not affected.
- System tasks, completed deployments, or previously aborted deployments cannot be aborted.

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.
2. Select the deployments you wish to abort.
3. Click **Abort**.

   Step Result: A confirmation message displays, asking you to confirm that you want to abort the deployment.
4. Click **OK** to confirm that you want to abort the deployment.

Result: The selected deployment is canceled.

Note: You cannot abort system tasks or Mandatory Baseline deployments.

Disabling Deployments

Disabling deployments pauses them, thus temporarily stopping the distribution of the package(s) to endpoints that have not already received a deployment. Disable deployments when you temporarily want to prevent them from installing on endpoints.

Disable deployments from the ***Deployments and Tasks*** page.

Note: You cannot disable deployments of system task packages.

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.
2. Select the deployments you want to disable.
3. Click **Disable**.

Result: The selected deployments are disabled.

Enabling Deployments

After you have disabled a deployment, reenable it to resume sending content to the deployment's assigned endpoints.

Reenable deployments from the ***Deployments and Tasks*** page.

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.
2. Select the disabled deployments you want to enable.
3. Click **Enable**.

Result: The selected deployments are enabled.

Editing Package Deployment Options

After scheduling a deployment, you can edit the package deployment options for each package assigned to the deployment. Editing a packages deployment options changes the deployment's behavior. This function is useful when you want each package in a deployment to deploy using different behavior options.

Edit package deployment behavior from the ***Deployments and Tasks*** page.

Note: System task packages are automatically assigned to endpoints, so removing an endpoint from a deployment of a system task package will have no effect (the endpoint will be re-assigned to the deployment by the Ivanti Endpoint Security).

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.
2. Expand the deployment that you want to modify.
3. Select the individual deployment package that you need to modify.

Note: If the deployment you are editing contains only one package, this list is unavailable.

4. Click the **Edit** icon.

   Step Result: The ***Package Deployment Options*** dialog opens.

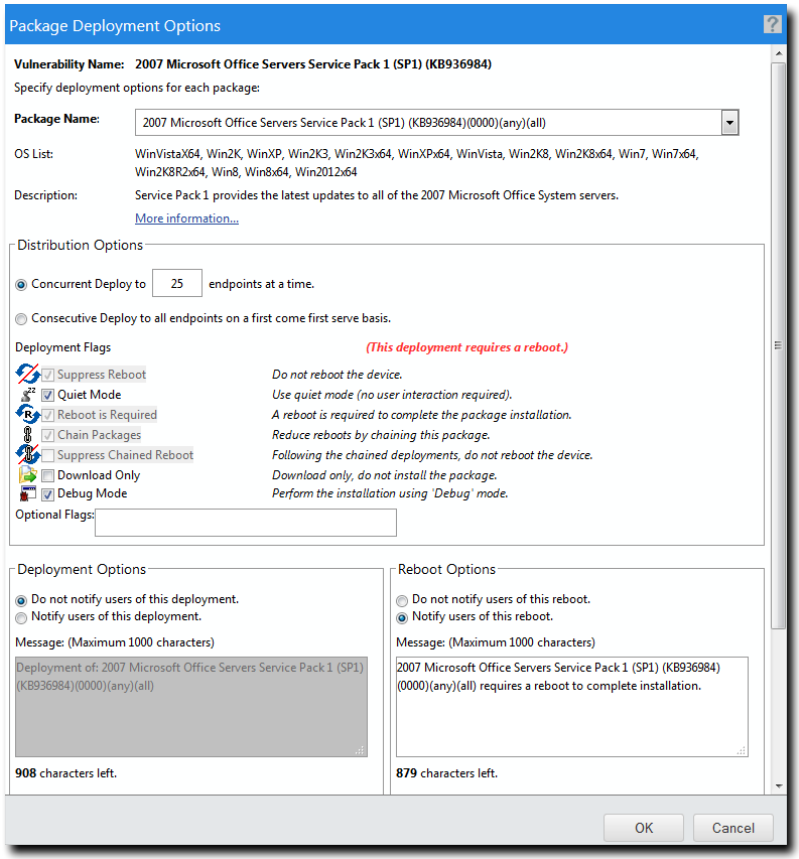


Figure 51: Package Deployment Options

5. From the **Package Name** list, ensure the desired package is selected.
6. Define **Distribution Options.**

   Choose from the following options.

Option	Steps
To deploy concurrently:	1. Select the **Concurrent** option. 2. Type the desired number of endpoints you want to deploy to at a time in the field.
To deploy consecutively:	Select the **Consecutive** option.

7. If available, select the desired **Deployment Flags**.
   For additional information, refer to Behavior Icon Definitions on page 280.
8. If needed, type additional deployment flags in the **Optional Flags** field.
   For additional information, refer to Package Flag Descriptions on page 282.
9. Define the **Deployment Options**.

Table 140: Deployment Options

Option	Description
Do not notify users of this deployment	Deploys the Mandatory Baseline package without notifying the recipients. **Note:** Selection of this option makes the remaining **Deployment Options** unavailable.
Notify users of this deployment	Deploys the Mandatory Baseline package and notifies the recipients. **Note:** Selection of this option makes the remaining **Deployment Options** available.
Message (field)	Displays a message notifying recipients of the deployment.
Use Policies (check box)	Uses the group's assigned agent policy set to define the remaining **Deployment Options**. **Note:** Selection of this option makes the remaining **Deployment Options** unavailable.
Allow user to cancel (check box and list)	Permits the recipient of the deployment to cancel. Either select the **Use Agent Policy** check box or define the **Setting** list.
Allow user to snooze (check box and list)	Permits the recipient of the deployment to delay the deployment. Either select the **Use Agent Policy** check box or define the **Setting** list.
Notification on top (check box and list)	Displays the ***Agent Deployment*** dialog when notifying a deployment recipient. Either select the **Use Agent Policy** check box or define the **Setting** list.
Deploy within (check box, field, and list)	Defines the time between the deployment creation and the deployment deadline. If **Allow user to snooze** is enabled, this value is also the maximum deployment snooze duration. Either select the **Use Agent Policy** check box or define the **Setting** field and list.

10. Define the **Reboot Options**.

Table 141: Reboot Options

Option	Description
Do not notify users of this reboot	Reboots following installation of the Mandatory Baseline package without notifying recipients. **Note:** Selection of this option makes the remaining **Reboot Options** unavailable.
Notify users of this reboot	Reboots following installation of the Mandatory Baseline package and notifies the recipients. **Note:** Selection of this option makes the remaining **Reboot Options** available.
Message (field)	Displays a message notifying recipients of the reboot.
Use Policies (check box)	Uses the applicable agent policy set to define the remaining **Deployment** options. **Note:** Selection of this option makes the remaining **Reboot Options** unavailable.
Allow user to cancel (check box and list)	Permits the recipient of the deployment to cancel the reboot. Either select the **Use Agent Policy** check box or define the **Setting** list.
Allow user to snooze (check box and list)	Permits the recipient of the deployment to delay the reboot. Either select the **Use Agent Policy** check box or define the **Setting** list.
Reboot within (check box and list)	Defines the time between the deployment creation and the reboot deadline. If **Allow user to snooze** is enabled, this value is also the maximum reboot snooze duration. Either select the **Use Agent Policy** check box or define the **Setting** field and list.

11. Click **OK**.

Result: The ***Package Deployment Options*** dialog closes and the deployment is modified.

Deleting Deployments

Deleting deployments removes the deployments from the Ivanti Endpoint Security. You can delete entire deployments or individual packages within a deployment.

Delete completed deployments, aborted deployments, or deployment packages from the ***Deployments and Tasks*** page.

Note:

- Deleting deployments has no effect on endpoints that have already received the deployments.
- You cannot delete system tasks.
- Scheduled deployments cannot be deleted until they are aborted.

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.
2. Delete deployments. You can either delete an entire deployments, or you can delete individual packages included in a deployment.

   Complete one of the following substep sets based on whether you want to partially or fully delete a deployment.

Option	Steps
To delete entire deployment(s):	1. Select the completed or aborted deployments you want to delete. 2. From the toolbar, click **Delete**.
To delete individual packages in a deployment (partial deletion):	1. Expand the deployment containing packages you want to delete by clicking the rotating chevron (**>**). 2. Click the **Delete** icon (✘) for the package you want to delete. **Tip:** Repeat this process for each package you want to delete.

3. Click **OK** to delete the deployment(s) or package.

Deploying Content (Deployments and Tasks Page)

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including the ***Deployments and Tasks*** page. Deploying content remotely installs different types of software on your network endpoints.

You can deploy content from the ***Deployments and Tasks*** page. For additional information about deployments, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.

2. Click **Deploy**.

Result: The ***Deployment Wizard*** opens.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Explaining Deployment Deadlines

Deadlines determine when a deployment or reboot should occur. A deadline can be calculated based upon the agent's group policy or defined by you as a specific date and time.

When using deadlines, define the deadline using the following parameters:

- Date and time.
- Starting date and time.
- Ability to snooze the deployment or reboot, as many times as desired, up to the defined deadline.

Using the Deployment Wizard

The ***Deployment Wizard*** is the dialog used to create or edit deployment schedules for multiple endpoints and multiple packages. The wizard assists in selecting endpoints, scheduling the deployment, and if needed, setting recurring deployments.

The following table describes the scenarios for a deployment. These options are selected prior to starting the ***Deployment Wizard***.

Table 142: Deployment Actions

Deployment Selection	Result
Endpoint	The ***Deployment Wizard*** deploys only to the selected endpoint.
Content	The ***Deployment Wizard*** automatically selects all the endpoints and packages required for the content.
Package	The ***Deployment Wizard*** deploys the selected package to the selected groups or endpoints selected within the wizard.
Group	The ***Deployment Wizard*** deploys the applicable packages to the selected group members.

For additional information on configuring a deployment, refer to Introduction Page on page 260.

Introduction Page

The ***Introduction*** page of the ***Deployment Wizard*** explains the purpose and capabilities of the wizard.

This page can be hidden during future deployments by selecting the **Do not display this page in the future** checkbox.

If this page displays, click **Next** to continue to the Available Endpoints/Groups Page on page 261.

Available Endpoints/Groups Page

When scheduling a deployment, you must choose endpoints and groups for patching.

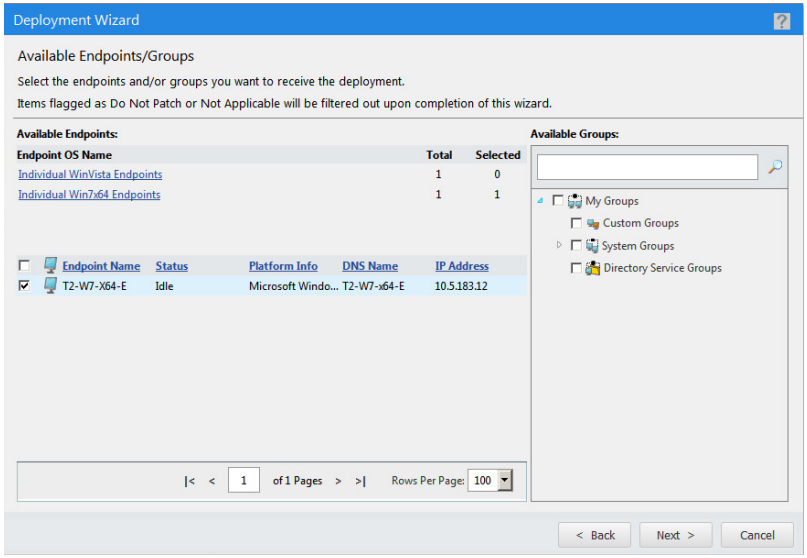


Figure 52: Available Endpoints/Groups Page

Endpoint Notes

- You can select endpoints, groups, or a combination of the two.

  Note: If you select endpoints or groups before initiating a deployment with the toolbar, those endpoints are preselected when you get to the ***Available Endpoints/Groups*** page.

- Endpoints are categorized by operating system. Click a link to display all the endpoints using that operating system.
- Groups are organized into a tree of custom groups, system groups, and directory service groups.
  - Use the search field to find specific groups quickly.
  - Wildcard searches are not supported.

Patch Notes

If you selected patches for deployment before opening the ***Deployment Wizard***, there are a few things you should know:

- The ***Deployment Wizard*** only lists endpoints that the patches apply to. For example:
  - If you select a Windows 8.1 patch for deployment, only Windows 8.1 endpoints are available for deployment.
  - If you select a patch that requires other software to be installed, endpoints that do not meet the prerequisites are unlisted.
- The ***Deployment Wizard*** only lists groups that the patches apply to.
  - If the group contains one or more endpoint that the patch applies to, it's listed.
- If you are deploying a *single* patch that is marked *Do Not Patch*:
  - **Available Endpoints** does not list endpoints that are *Do Not Patch*.
- If you are deploying multiple patches, and one or more of those patches are marked *Do Not Patch*:
  - **Available Endpoints** or **Available Groups** marked *Do Not Patch* are automatically selected because the other patches selected for deployment still apply. However, the patch marked *Do Not Patch* does not deploy to the marked endpoints and groups.

After choosing endpoints and groups, click **Next** to proceed to the Available Packages Page on page 263.

Creating an Endpoint Deployment
When creating deployments, you can define deployment recipients by selecting individual endpoints, regardless of group membership.

Select endpoints as deployment recipients from the ***Available Endpoints/Groups*** page.

1. From the **Available Endpoint** list, select the **Endpoint OS Name** required.

   Step Result: The list of endpoints within that operating system display.

2. Select an endpoint (or endpoints) from the list.

   Step Result: The endpoint(s) are highlighted.

Result: Endpoints are targeted as deployment recipients.

Creating a Group Deployment
You can select single groups, multiple groups, and group hierarchies as deployment recipients using the **Available Groups** directory tree. This method of selecting recipients lets you select multiple groups for a deployment without having to create deployments for each individual group.

Select endpoints as deployment recipients from the ***Available Endpoints/Groups*** page.

Note: If endpoints are added to a group after a deployment is created but before the time the deployment occurs, the newly-added endpoints will receive the deployment.

From the **Available Groups** directory tree, select the group or groups requiring the deployment.

Selecting a parent group also selects its child hierarchy. If you do not want to deploy to a parent's child group hierarchy, cancel the deployment for the desired groups by clearing the applicable check boxes.

Result: Groups are targeted as deployment recipients.

Available Packages Page

While completing the ***Deployment Wizard***, packages must be selected for installation on target endpoints. These packages are selected from the ***Available Packages*** page.

When selecting packages for deployment, remember the following helpful information:

- Only vendors and packages applicable to the selected endpoint(s) display. Inapplicable content is hidden.
- If you opened the ***Deployment Wizard*** from one of the ***Content*** pages after selecting content items from the page list, those items are preselected in the wizard. Finding the packages you want to deploy is unnecessary (although you can select more packages if desired).

  Note: If you pre-selected vulnerabilities for deployment, the ***Available Packages*** page may display more packages selected for deployment that the number of vulnerabilities you selected. This discrepancy is because a vulnerability may contain more than one package.

- An icon in the listed packages indicates if the package your want to deploy is already cached. If you already have the package cached, you can deploy it more quickly. Ivanti recommends caching packages before deployment.

After defining the ***Available Packages*** page, click **Next** to proceed to the Licenses Page on page 265.

For additional information of selecting packages, refer to Selecting Deployment Packages on page 263.

Selecting Deployment Packages

Selecting packages to deploy to selected endpoint remediates endpoint vulnerabilities.

Select packages for deployment from the ***Available Packages*** page.

1. Select the ***Vendor*** link containing the package(s) you want to deploy.

   Step Result: A list of the vendor's packages for the selected deployment recipients opens.

2. Select the package(s) needed.

   Step Result: The packages are selected.

3. [Optional] Repeat the selection process for additional vendors.
4. [Optional] Click a **Package Name** link to open the ***Associated Vulnerability Analysis*** page. For additional information, refer to Associated Vulnerability Analysis Page on page 264.

5. Click **Next** to proceed to the ***Licenses*** page.

   When using the ***Deployment Wizard***, the wizard will not necessarily install service packs first. Verify that all relevant service packs have deployed successfully before creating deployments using the ***Deployment Wizard***.

Associated Vulnerability Analysis Page

This page lists the package status for each endpoint that it applies to (not just the endpoints included in the deployment). Viewing this page is useful to estimate how many of your selected endpoints will not receive the deployment package due to patch status (for example, the patch does not apply to the endpoint).

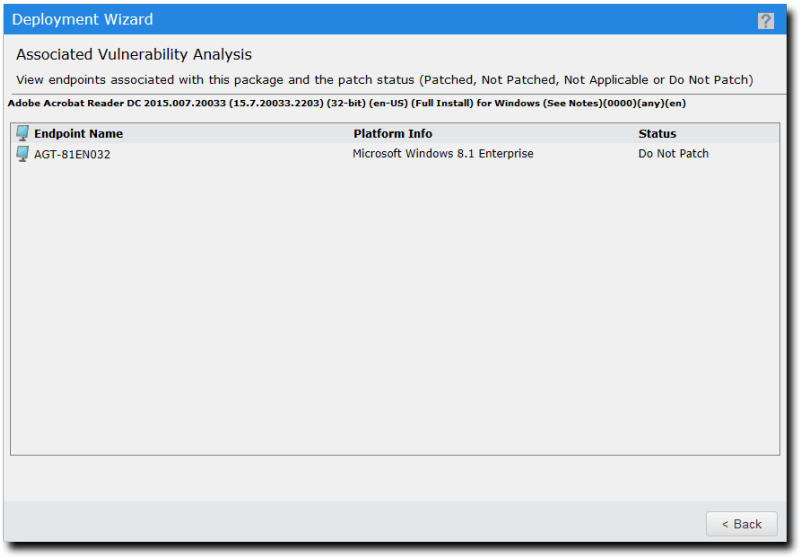


Figure 53: Associated Vulnerability Analysis Page

The following table describes the page columns.

Table 143: Associated Vulnerability Analysis Columns

Name	Description
Endpoint Name	The endpoint that the package applies to.
Platform Info	The operating system that the endpoint is using.
Status	The patch status of the package for the endpoint. Values include: • Patched • Not Patched • Not Applicable • Do Not Patch

When finished viewing the page, click **Back** to return to the Available Packages Page on page 263.

Licenses Page

To continue configuration of your deployment, you must first accept the vendor license agreement(s).

The number of different license agreements that appear depend upon how many packages you selected to install. For example, you selected four different packages for installation and these packages were created by three different vendors, you would have to agree to three different license agreements.

For additional information on accepting license agreements, refer to Accepting License Agreements on page 265.

After accepting licenses, click **Next** to proceed to the Deployment Information Page on page 266.

Accepting License Agreements

To continue configuration of your deployment, you must first accept the vendor license agreement(s).

Accept licenses from the ***Licenses Page***.

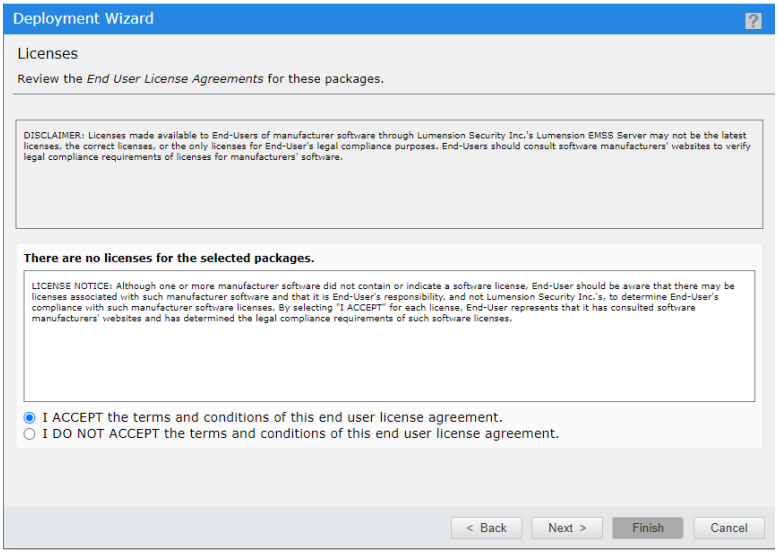


Figure 54: Licenses Page

1. Review the agreement.
2. If you accept the agreement, select the **I ACCEPT the terms and conditions of this end user license agreement** option.
3. If there are multiple agreements, repeat the previous steps.

   All agreements must be accepted before continuing.
4. [Optional] Click **Next** to proceed to the ***Deployment Information*** page.

Deployment Information Page

You can control the user notification options associated with a deployment using the ***Deployment Information*** page. You can set the deployment job name, start time, manner, and add notes.

The following information may be useful when completing this page:

- Job and task names will later be used to identify deployment results.
- Deploying using Agent Local Time is useful in geographically dispersed networks. This deployment method helps ensure deployments complete off peak business hours.
- Deploying using UTC time is useful when you want to deploy content at one specific time.
- Concurrent deployments ensure endpoint receive packages near simultaneously, but may consume excessive network bandwidth.
- Consecutive deployments reduces network bandwidth consumption, but endpoints may receive deployment at different times.

After defining deployment information, click **Next** to proceed to the Package Deployment Order and Behavior Page on page 277.

For additional information of defining deployment information, refer to Configuring Deployment Information on page 266.

Configuring Deployment Information

The deployment information contains controls for naming and configuring your deployment. You can use this page to choose a start time and the manner in which it deploys.

Configure deployment information from the ***Deployment Information*** page.

1. [Optional] Edit the **Job name** and **Task name** fields.

Field	Description
Job name	The name of the job. By default, jobs are named `Remediation`, followed by the date and time at the time of deployment creation.
Task name	The task name for the job. Use this name to describe the purpose of the deployment. By default, tasks are named `Deployment of {Package Name}`.

Tip: Upon completion of the ***Deployment Wizard***, use the **Job name** and **Task name** to identify your deployment. The **Job name** displays on the ***Deployment and Tasks*** page, and the **Task name** displays when you expand your deployment.

Use the **Start time** options to configure the deployment start time and start date. You can also use these options to schedule a recurring deployment or select deployment time zone options.

2. [Optional] Schedule the deployment **Start Time**, which is the date and time that the deployment begins. Edit the **Start time** by clicking **Change**. By default, the **Start time** is set to the date and time the ***Deployment Wizard*** was opened.

   For additional information on start times and configuring recurring deployments, refer to Schedule Configuration Page on page 269.

3. Select the desired **Deployment time zone** option.

   Use this option to configure which time zone setting is used to trigger a deployment. The following table defines the options.

Option	Description
Agent Local Time	The deployment begins according to the local time zone on each endpoint.
Agent UTC Time	The deployment begins according to UTC (coordinated universal time) on each endpoint.

Note: If you deploy to a group using **Agent Local Time**, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.

Use the **Manner** options to configure how endpoints receive the deployment in relation to one another. The **Manner** options also include:

- A feature to disable the entire deployment should deployment to an individual endpoint fail.
- A feature to redeploy packages to an endpoint, even if the package has been previously installed.

4. Select a **Manner** deployment option.

   The following table describes each manner deployment option and how to use them.

Option	Description and Instructions
Concurrent	This option deploys the package(s) to a defined number of endpoints simultaneously. New deployments are distributed when agents report back after completing the previous deployment. If an endpoint takes longer than four hours to complete the deployment, it is no longer counted against the concurrent deployment limit. To deploy to endpoints concurrently, complete the following steps: 1. Select the **Concurrent** option. 2. Type a number in the **Deploy to <*x*> nodes at a time** field.
Consecutive	This option deploys the packages simultaneously to all endpoints. However, the global deployment limit will always take precedence over the defined distribution options defined. To deploy to endpoints consecutively, select the **Consecutive** option.

5. [Optional] Define the remaining **Manner** options. Enable or disabled the options by selecting or clear each option checkbox.

   The following table describes the remaining **Manner** options.

Option	Description
Suspend the deployment of this package if it fails to deploy to one or more nodes.	This option suspends all subsequent deployments following any deployment failure.
Deploy package even if the computer has been previously patched.	This option deploys the package(s) to all selected endpoints regardless of patch status.

Finally, the ***Deployment Information*** page features a **Notes** field to type text about the deployment. You can view this text after you complete the ***Deployment Wizard*** by viewing the deployment details on various Ivanti Endpoint Security pages.

6. [Optional] Type notes and comments in the **Notes** field.

Tip: After completing the ***Deployment Wizard***, you can view deployment notes by expanding the deployment from an ***Endpoint Details*** page ***Deployment and Tasks*** tab.

Result: Deployment information is defined. Click **Next** to continue to the ***Package Deployment Order and Behavior*** page.

Schedule Configuration Page

You can set the timing and frequency of a deployment using the ***Schedule Configuration*** page. Deployments can be defined as one-time or recurring. Additional schedule configuration options are also available.

Note: If endpoints are added to a group after a deployment is created but before the deployment occurs, the newly-added endpoints will receive the deployment.

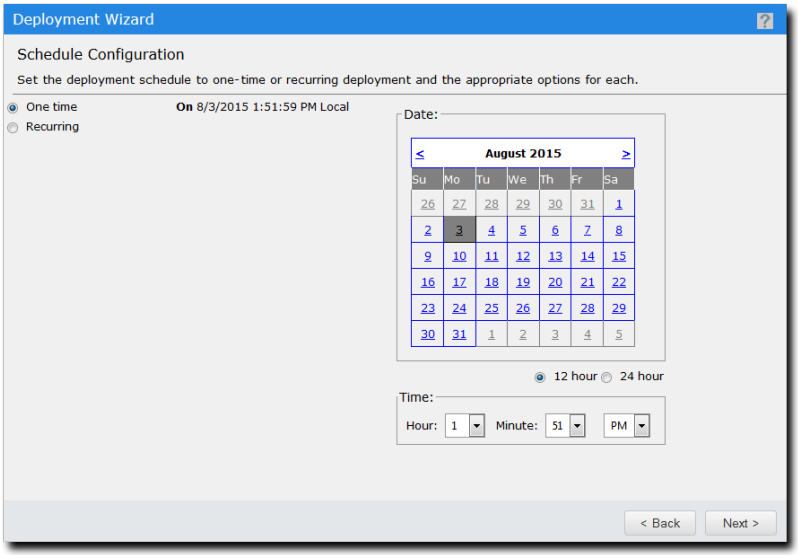


Figure 55: Schedule Configuration Page

Complete one of the following tasks based on how you want to schedule the deployment:

- If you want to run the deployment once, complete Scheduling a One Time Deployment on page 270.
- If you want to run the deployment on a recurring basis, complete Scheduling a Recurring Deployment on page 271.

Scheduling a One Time Deployment
A one time deployment starts on the selected day at the selected time.

Prerequisites:

- Begin Configuring Deployment Information on page 266.

1. From the ***Deployment Wizard Schedule Configuration*** page, click **Change** located in the **Start Time** option.
2. Ensure **One Time** is selected.

   Step Result: The deployment will start on the selected day at the defined time.
3. [Optional] Select a date from the calendar. This is the date that the deployment will begin.
4. Define a **Time**. This is the time that the deployment will begin.

   Tip: Select from the **12 hour** and **24 hour** options to change time listing values. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

   a) Select a value from the **Hour** list.
   b) Select a value from the **Minute** list.
   c) Select a value from the **AM/PM** list.
5. Click **Next**.

   Step Result: The deployment is configured to start on the selected date and time, and the ***Deployment Information*** page opens. If you scheduled the deployment for a lapsed date and time, the deployment will start the next time applicable agents contact the Ivanti Endpoint Security server.

After Completing This Task:
Complete Configuring Deployment Information on page 266.

Scheduling a Recurring Deployment

A recurring schedule starts deployments on the selected day at the selected time. The deployment repeats every day, week, or month and if defined, ends on a specific date.

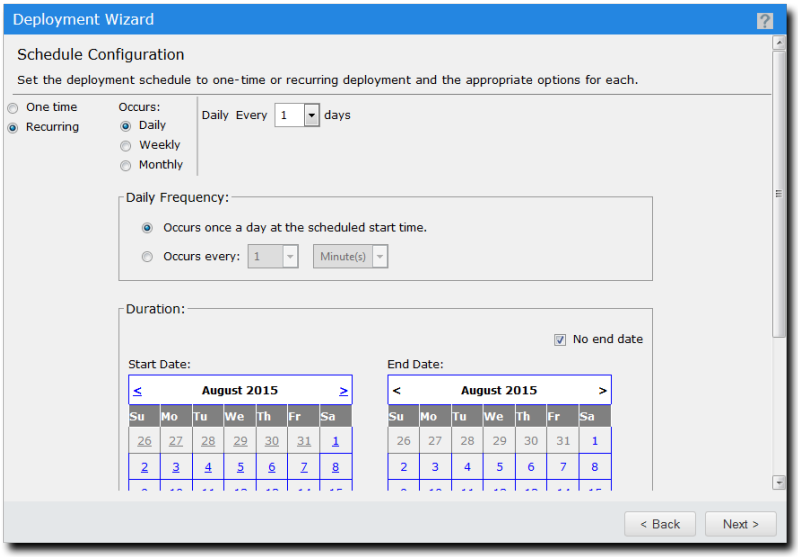


Figure 56: Schedule Configuration Page

To schedule a recurring deployment, complete one of the following tasks:

- Configuring a Daily Recurring Deployment on page 271.
- Configuring a Weekly Recurring Deployment on page 273.
- Configuring a Monthly Recurring Deployment on page 275.

Configuring a Daily Recurring Deployment

You can configure a deployment to happen every day. Recurring deployments are useful to ensure selected content remains installed on endpoints.

Prerequisites:

Begin Configuring Deployment Information on page 266.

Schedule deployments for daily recurrence from the ***Schedule Configuration*** page

1. From the ***Deployment Information*** page, click **Change**, located in the **Start Time** section of the page.

   Step Result: The ***Schedule Configuration*** page opens.

2. Select **Recurring**.

Begin configuring your daily recurring deployment by defining the occurrence options. Configure the deployment to run daily or, alternatively, configure it run it at intervals of a defined number of days.

3. Configure the **Occurs** options for a daily deployment.
   a) Select **Daily**.
   b) Select a value from the **Daily Every <*x*> days** list (1-366).

Next, select a **Daily Frequency** option. You can configure your recurring deployment to run at one time on its scheduled day, or several times on its scheduled day.

4. Select a **Daily Frequency** option.
   The following table describes each **Daily Frequency** option and lists instructions for using it.

Option	Description and Instructions
Occurs once a day at the scheduled start time	The deployment occurs as defined in the **Occurs** and **Duration** options once on the scheduled day(s). To use this option, select **Occurs once a day at the schedule start time**.
Occurs every <*x*> <*time unit*>	The deployment occurs as defined in the **Occurs** and **Durations** options at the selected interval. To use this option, complete the following steps: **1.** Select the **Occurs every <*x*> <*time unit*>** option. **2.** Select a value from the **<*x*>** list. The values available changes according to the value selected from the **<*time unit*>** list. **3.** Select a value from the **<*time unit*>** list (**Minute[s]**, **Hour[s]**).

Finally, select the duration of your recurring deployment. All recurring deployments require a start date. However, you have the option of selecting an end date for your recurring deployment or letting it run indefinitely.

5. Define a deployment **Start Date**. This is the date and time the recurring deployment will start.

Tip: Select from the **12 hour** and **24 hour** options to change time listing values for both the **Start Date** and **End Date** calendars. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

   a) Select a date from the **Start Date** calendar.
   b) Select a value from the **Hour** list.
   c) Select a value from the **Minute** list.
   d) Select a value from the **AM/PM** list.

6. Define a deployment **End Date**.

End Date Option	Instructions
To end the recurring deployment on a selected date:	1. Ensure the **No end date** checkbox is cleared. 2. Select a date from the **End Date** calender. 3. Select a value from the **Hour** list. 4. Select a value from the **Minute** list. 5. Select a value from the **AM/PM** list.
To run the recurring deployment indefinitely:	Ensure the **No end date** checkbox is selected.

7. Click **Next**.

After Completing This Task:
Complete Configuring Deployment Information on page 266.

Configuring a Weekly Recurring Deployment
You can configure a deployment that happens every week. Recurring deployments are useful to ensure selected content remains installed on endpoints.

Prerequisites:

Begin Configuring Deployment Information on page 266.

Schedule deployments for weekly recurrence from the ***Schedule Configuration*** page.

1. From the ***Deployment Information*** page, click **Change**.

   Step Result: The ***Schedule Configuration*** page opens.

2. Select **Recurring**.

Begin configuring your weekly recurring deployment by defining the occurrence options. You can configure deployments to run weekly, or you can configure it to run weekly with an interval of weeks between deployments. You can also configure the deployment to run on certain days of your weekly deployment.

3. Configure the **Occurs** options for a weekly deployment.
   a) Select the **Weekly** option.
   b) Select a value from the **Every <*x*> weeks on** list.
   c) Select the weekday checkboxes for the days of the week that you want the deployment to run (**Monday** through **Sunday**).

Next, select a **Daily Frequency** option. You can configure your recurring deployment to run at one time on its scheduled day, or several times on its scheduled day.

4. Select a **Daily Frequency** option.

   The following table describes each **Daily Frequency** option and lists instructions for using it.

Option	Description and Instructions
Occurs once a day at the scheduled start time	The deployment occurs as defined in the **Occurs** and **Duration** options once on the scheduled day(s). To use this option, select **Occurs once a day at the schedule start time**.
Occurs every <*x*> <*time unit*>	The deployment occurs as defined in the **Occurs** and **Durations** options at the selected interval. To use this option, complete the following steps: 1. Select the **Occurs every <*x*> <*time unit*>** option. 2. Select a value from the **<*x*>** list. The values available changes according to the value selected from the **<*time unit*>** list. 3. Select a value from the **<*time unit*>** list (**Minute[s]**, **Hour[s]**).

Finally, select the duration of your recurring deployment. All recurring deployments require a start date. However, you have the option of selecting an end date for your recurring deployment or letting it run indefinitely.

5. Define a deployment **Start Date**. This is the date and time the recurring deployment will start.

   Tip: Select from the **12 hour** and **24 hour** options to change time listing values for both the **Start Date** and **End Date** calendars. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

   a) Select a date from the **Start Date** calendar.
   b) Select a value from the **Hour** list.
   c) Select a value from the **Minute** list.
   d) Select a value from the **AM/PM** list.

6. Define a deployment **End Date**.

End Date Option	Instructions
To end the recurring deployment on a selected date:	1. Ensure the **No end date** checkbox is cleared. 2. Select a date from the **End Date** calender. 3. Select a value from the **Hour** list. 4. Select a value from the **Minute** list. 5. Select a value from the **AM/PM** list.

End Date Option	Instructions
To run the recurring deployment indefinitely:	Ensure the **No end date** checkbox is selected.

7. Click **Next**.

After Completing This Task:
Complete Configuring Deployment Information on page 266.

Configuring a Monthly Recurring Deployment
You can configure a deployment that happens every month. Recurring deployments are useful to ensure selected content remains installed on endpoints.

Prerequisites:

Begin Configuring Deployment Information on page 266.

Configure deployments for monthly recurrence from the ***Schedule Configuration*** page.

1. From the ***Deployment Information*** page, click **Change**, located in the **Start Time** section of the page.
2. Select **Recurring**.

Begin configuring your monthly recurring deployment by defining the occurrence options. You can configure the deployment to run monthly, or you can configure the deployment to run monthly with an interval of months between deployments. You can also schedule your monthly deployment to run on a specific date (July, 1) or a specific day (first Sunday on the month).

3. Configure the **Occurs** options for a monthly deployment.
   a) Select the **Monthly** option.
   b) Select one of the **Monthly** options that displays, and then select values from its drop-down lists.
      Select one of the following options and then define its lists.
      - **Day <*x*> of every <*x*> months**
      - **The <*x*> <*day*> of every <*x*> months**

Next, select a **Daily Frequency** option. You can configure your recurring deployment to run at one time on its scheduled day, or several times on its scheduled day.

4. Select a **Daily Frequency** option.

   The following table describes each **Daily Frequency** option and lists instructions for using it.

Option	Description and Instructions
Occurs once a day at the scheduled start time	The deployment occurs as defined in the **Occurs** and **Duration** options once on the scheduled day(s). To use this option, select **Occurs once a day at the schedule start time**.
Occurs every <*x*> <*time unit*>	The deployment occurs as defined in the **Occurs** and **Durations** options at the selected interval. To use this option, complete the following steps: 1. Select the **Occurs every <*x*> <*time unit*>** option. 2. Select a value from the **<*x*>** list. The values available changes according to the value selected from the **<*time unit*>** list. 3. Select a value from the **<*time unit*>** list (**Minute[s]**, **Hour[s]**).

Finally, select the duration of your recurring deployment. All recurring deployments require a start date. However, you have the option of selecting an end date for your recurring deployment or letting it run indefinitely.

5. Define a deployment **Start Date**. This is the date and time the recurring deployment will start.

   Tip: Select from the **12 hour** and **24 hour** options to change time listing values for both the **Start Date** and **End Date** calendars. When the **24 hour** option is selected, the **AM/PM** list is unavailable.

   a) Select a date from the **Start Date** calendar.
   b) Select a value from the **Hour** list.
   c) Select a value from the **Minute** list.
   d) Select a value from the **AM/PM** list.

6. Define a deployment **End Date**.

End Date Option	Instructions
To end the recurring deployment on a selected date:	1. Ensure the **No end date** checkbox is cleared. 2. Select a date from the **End Date** calender. 3. Select a value from the **Hour** list. 4. Select a value from the **Minute** list. 5. Select a value from the **AM/PM** list.

End Date Option	Instructions
To run the recurring deployment indefinitely:	Ensure the **No end date** checkbox is selected.

7. Click **Next**.

After Completing This Task:
Complete Configuring Deployment Information on page 266.

Package Deployment Order and Behavior Page

The packages selected for deployment can have their order and behavior edited. For instance, you may want a particular package deployed before another. Use the ***Package Deployment Order and Behavior*** page to edit order and behavior.

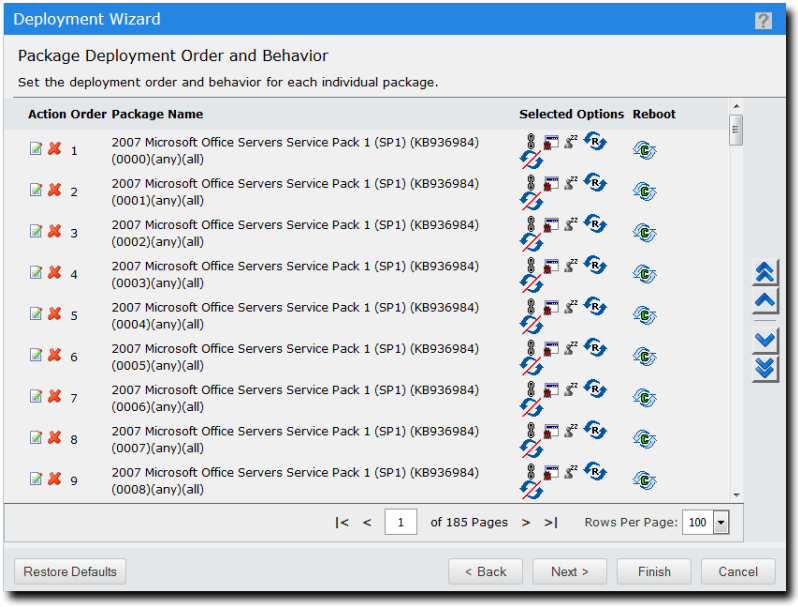


Figure 57: Package Deployment Order and Behavior Page

The following table describes each page column.

Table 144: Package Deployment Order and Behavior Columns

Column	Description
Action	Contains **Edit** and **Delete** icons. Click the **Edit** icon to open ***Package Deployment Behavior Options*** page, which you can use to change package behavior options. Click the **Delete** icon to remove the package from the deployment. For additional information on editing package behavior, refer to Selecting Deployment Behavior Options on page 279
Order	Indicates the order number of the package.
Package Name	Indicates the name of the package.
Selected Options	Displays icons that indicate behaviors selected for the package. Mouse over for a text description of the behavior. For additional information, refer to Behavior Icon Definitions on page 280.
Reboot	Displays icons that indicate whether a reboot follows the package deployment. For additional information, refer to Reboot Icon Definitions on page 281.

From this page, you can change the order that packages are deployed in using the page controls. For additional information on settings the package deployment order, refer to Selecting Deployment Behavior Options on page 279.

Note: Chained packages cannot be moved without first removing their chained status. When a package is chained, Ivanti Endpoint Security determines the deployment order. However, when no longer chained, the package can be deployed at anytime following the chained deployments.

After defining deployment order and behavior, click **Next** to proceed to the Notification Options Page on page 284.

Setting Package Deployment Order

Set the deployment order to determine which packages are installed first.

Define the deployment order from the ***Package Deployment Order and Behavior*** page.

1. Select the package(s) you want to move within the queue.

   Tip: You can remove a package from the deployment clicking its **Delete** icon (✖).

2. Move the selected packages within the queue.

   Click the following icons to move packages to desired queue position.

Icon	Description
Double Up Arrow	Moves the selected package(s) to the top of the queue.

Icon	Description
Up Arrow	Moves the selected package(s) up one queue position.
Double Down Arrow	Moves the selected package(s) to the bottom of the queue.
Down Arrow	Moves the selected package(s) down one queue position.

Tip: After editing package deployment order, you can restore the default order by clicking **Restore Defaults**.

3. [Optional] Edit deployment behavior options for packages by clicking the **Edit** icon ( ).
   For additional information, refer to Selecting Deployment Behavior Options on page 279.

Result: Package deployment order is defined. Click **Next** to proceed to the ***Notification Options*** page.

Selecting Deployment Behavior Options
Each package in a deployment can have its behavior changed by selecting behavior options.

Select deployment behavior options for a package from the ***Package Deployment Behavior Options*** page.

1. Select the check box for each behavior you want the package to use.
   The behaviors available change for each package. For a complete list of behaviors and their descriptions, refer to Behavior Icon Definitions on page 280.
2. Define additional behaviors typing entries in the **Optional Flags** field.
   For a complete listing of behavior flags, refer to Package Flag Descriptions on page 282.
3. Select a **Display** option.
   This option defines the notification that deployment recipients receive when user notifications are enabled. Select one of the following options.

Option	Description
Behavior options settings	Displays the expected deployment behavior.
Package description	Displays the package description.

Note: Modifying behavior options initiates a system reevaluation of the deployment, which may result in a change in the package order.

Result: The package enables the selected behaviors. Click **Next** to return to the ***Package Deployment Order and Behavior*** page.

Behavior Icon Definitions

Behavior icons appear on the ***Package Deployment Order and Behavior*** page and indicate the activities related to the deployment configuration.

The following table describes the deployment behavior icons and their descriptions. The icons representing the selected behaviors appear in the **Selected Options** column.

Table 145: Behavior Icon Definitions

Icon	Action	Use to
	Uninstall	Uninstall the packages.
	Force Shutdown	Force all applications to close if the package causes a reboot.
	Do Not Backup	Uninstall package without backing up files.
	Suppress Reboot	Prevent a reboot after installation.
	Quiet Mode	Suppress any user interfaces during the deployment.
	Unattended Setup	Set up packages in unattended mode.
	List Hot Fixes	Return a listing of hot fixes installed on the target devices.
	Force Reboot	Force a reboot regardless of package requirements.
	Reboot is Required	Indicate a reboot is required prior to completing the installation.
	Chain Packages	Set the package as chainable (package must support chaining).
	Suppress Chained Reboot	Suppress the reboot, so that other chained packages can be sent following this package. When creating multiple deployment jobs, this option is recommended.
	Repair File Permissions	Repair file permissions following the package installation.
	Download Only	Distribute the package without running the package installation script.
	Suppress Notification	Suppress any user notifications during installation.
	Debug Mode	Run the package installation in debug mode.

Icon	Action	Use to
	Do Not Repair Permissions	Suppress the repair of file name permissions after the reboot.
	May Reboot	Force a reboot, if required.
	Multi-User Mode	Perform the installation in multi-user mode.
	Single-User Mode	Perform the installation in single-user mode.
	Restart Service	Restart the service following the deployment.
	Do Not Restart Service	Suppress the restart of the service following the deployment.
	Reconfigure	Perform the system reconfigure task following deployment.
	Do Not Reconfigure	Suppress the system reconfigure task following deployment.

Note: When using a chained deployment, reboots are suppressed whenever possible. The final deployment is represented as `May Reboot` because Ivanti Endpoint Security determines if the agent is in a *dirty state*. If so, a `System Task - Reboot` deployment is sent before deploying the remaining packages.

Reboot Icon Definitions

Reboot icons appear on the ***Package Deployment Order and Behavior*** page and determine the reboot conditions for a deployment.

The following table describes the reboot icons.

Table 146: Reboot Icon Definitions

Icon	Name	Reboot Status
	Reboot may occur	The device may be rebooted, dependent upon the package installer requirements (at the time of install).
	Reboot may occur chained	The device may be rebooted, dependent upon the package requirements. However if a reboot is required and the device is not rebooted, the device will enter a reboot state.
	Reboot required	No other (chainable or non-chainable) packages will be installed until the device reboots.
	Reboot required chained	Only chainable packages will continue to be installed until the device has been rebooted.

Icon	Name	Reboot Status
	Reboot will occur	The device will be rebooted following the package installation.

Click **Next** to proceed to the Notification Options Page on page 284 page.

Click **Finish** to create the deployments and proceed to the Deployment Confirmation Page on page 288.

Package Flag Descriptions

You can attach behavior to package deployments using package flags.

The following table defines flag behavior and their descriptions:

Table 147: Package Flag Descriptions

Description (flag behavior)	Display Flag	Select Flag
Perform an uninstall; can be used with -mu or -q.	-yd	-y
Force other applications to close at shutdown.	-fd	-f
Do not back up files for uninstall.	-nd	-n
Do not restart the computer when the installation is done.	-zd	-z
Use quiet mode, no user interaction is required.	-qd	-q
Use unattended setup mode.	-dmu	-mu
Install in multi-user mode[1]	N/A	-su
Restart service after installation[1]	N/A	-restart
Do not restart service after installation[1]	N/A	-norestart
Reconfigure after installation[1]	N/A	-reconfig
Do not reconfigure after installation[1]	N/A	-noreconfig
Download packages to the default package cache directory for the Linux distro, but don't install them[2] Packages are downloaded to the following locations: • Redhat and CentOS: `/var/cache/yum` • SUSE: `/var/cache/zypp/packages` • Ubuntu: `/var/cache/apt`	N/A	-CACHEPACKAGES

Description (flag behavior)	Display Flag	Select Flag
Install packages cached in the `tmp` folder[2]	N/A	-INSTALLFROMCACHE
Tip: If you are patching Linux and Unix endpoints that receive content directly from vendor repositories, deployments may exceed your scheduled window because the patch content must first be downloaded, a process that may be excessively long. To reduce the likelihood of deployments that exceed maintenance schedules: **1.** Cache the content to the endpoints by completing a deployment using the -CACHEPACKAGES flag. This deployment downloads the content, but doesn't install it. **2.** Install the cached content by completing a second deployment using the -INSTALLFROMCACHE flag. The deployment skips the download of content, and installs the content already cached.		
Ignores discrepancies between libraries available in different architectures[2]	N/A	-YUM_PROTECTED_MULTILIB
Skips packages with broken dependencies when updating the endpoint[2]	N/A	-YUM_SKIP_BROKEN
Performs a trial run of the deployment with no package changes made.[3]	N/A	-TRIAL_RUN
This package is chainable and will run Qchain.exe (Windows) or (UNIX/Linux).	-dc	-c
Suppress the final chained reboot.	-dc	-sc
Repair permissions.	-dr	-r
Deploy only.	-PLD1	-PLDO
No Pop-up	-PLN1	-PLNP
Debug	-PLDG	-PLDEBUG
Suppress Repair	-dsr	-sr
Force the script to reboot when the installation is done.	-1d	-1
Reboot is required.	N/A	-2
Reboot may occur.	N/A	-3
Reboot is required, and may occur.	N/A	-4

1. This flag applies to Linux and Unix operating systems only.
2. This flag applies to only Red Hat Enterprise Linux 5.5-7.x, Oracle Enterprise Linux 5.5-7.x, and CentOS Linux 5.5-7.x.
3. This flag applies to only Oracle Solaris 10 Update 9.

Notification Options Page

You can define whether users will receive notification of deployments and/or reboots, and if so, what the notification will contain using the ***Notification Options*** page of the ***Deployment Wizard***.

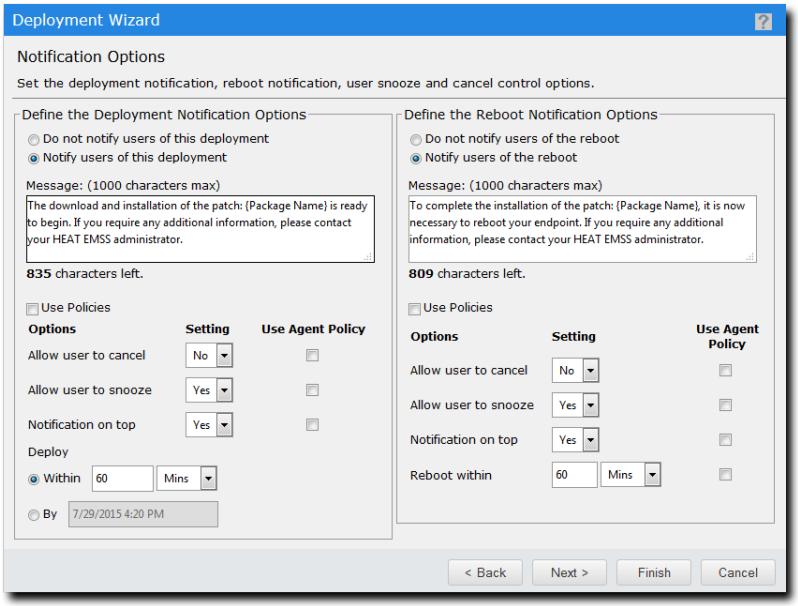


Figure 58: Notification Options Page

Note: When an agent is installed on a server where multiple users are logged in simultaneously, the deployment manager will provide each user with the ability to snooze or reject the deployment and/or reboot if snooze or reject is enabled.

For additional information on defining notification options, refer to Setting Notification Options on page 284.

After editing the ***Notifications Options*** page, click **Next** to view the Deployment Confirmation Page on page 288.

Setting Notification Options

During deployments, you can notify recipients that their endpoints are receiving a deployment or require a reboot. From the ***Notification Options*** page, you can define the message that recipients receive.

Define notification options from the ***Notification Options*** page.

1. Select a **Define the Deployment Notification Options** option.
   - **Do not notify users of this deployment**.
   - **Notify users of this deployment**.

2. If you selected the **Notify users of this deployment** option, complete the following substeps.
   a) [Optional] Type a notification in the **Message** field.
   b) Select whether you want to manually define remaining notification options or use the default settings defined in the agent policy set that applies to the target endpoints.
      - To use the default notification option settings defined in the agent policy set that applies to the target endpoints, select the **Use Policies** check box and continue to the next step.
      - To manually define the individual notification options, ensure the **Use Policies** check box is cleared. Select **Yes** or **No** from the **Setting** list for each of the following notification options:
        - **Allow user to cancel**
        - **Allow user to snooze**
        - **Notification on top**

          For additional information about this option, refer to About the Show on Top Option on page 286.

          Note: If you want to allow LUM (Linux, Unix, and Mac) endpoint users to cancel or snooze deployments, manually set the options for **Allow user to cancel** and **Allow user to snooze**. Don't select the **Use Policies** or **Use Agent Policy** check boxes. These options are for Windows endpoints only. If you select these check boxes, the system ignores their selection, and your LUM endpoint users will not receive notifications.

   c) Select and define a **Deploy** option.
      - To deploy the notification within a specific time frame, select the **Within** option and define the field and list (**Mins**, **Hours**, **Days**).
      - To deploy the notification by a specific deadline, select the **By** option and define a date and time.

        Use the calender controls that display to define the date and time, and then click **OK**.

3. Select a **Define the Reboot Notification Options** option.
   - **Do not notify users of this reboot**
   - **Notify users of this reboot**

4. If you selected the **Notify users of this reboot** option, complete the following substeps to define the remaining options.
   a) [Optional] Type a notification in the **Message** field.

b) Select whether you want to manually define remaining notification options or use the default settings defined in the agent policy set associated with the target endpoints.

- To use the default notification option settings defined in the agent policy set that applies to the target endpoints, select the **Use Policies** check box and continue to the next step.
- To manually define the individual notification options, ensure the **Use Policies** check box is cleared. Select **Yes** or **No** from the **Setting** list for each of the following notification options:
  - **Allow user to cancel**
  - **Allow user to snooze**
  - **Notification on top**

    For additional information about this option, refer to About the Show on Top Option on page 286.

Note: If you want to allow LUM (Linux, Unix, and Mac) endpoint users to cancel or snooze deployments, manually set the options for **Allow user to cancel** and **Allow user to snooze**. Don't select the **Use Policies** or **Use Agent Policy** check boxes. These options are for Windows endpoints only. If you select these check boxes, the system ignores their selection, and your LUM endpoint users will not receive notifications.

c) Define the **Reboot within** option.

- To manually define this option, enter a value in the field and select a value from the list (**Mins**, **Hours**, **Days**).
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

Result: Notification options are configured. Click **Next** to continue to the ***Deployment Confirmation*** page.

About the Show on Top Option

When creating a deployment or a Mandatory Baseline item for Windows endpoints, you can define the **Show on Top** options. These options determine whether notifications for deployments or reboots display on top or on bottom of all other open endpoint windows. These options are not available on Linux, Unix, and Mac endpoints.

There are two different ***Show on Top*** options:

- A **Show on Top** option for **Deployment Notification Options**
- A **Show on Top** option for **Reboot Notification Options**

The following table describes the notification dialog behaviors for each option setting (**Yes** or **No**).

Table 148: Always on Top Option Setting Description

Always on Top Option Setting	Notification Dialog Behaviour
Yes	The deployment or reboot notification displays as the topmost window. All other open windows display behind it.
No	The deployment or reboot notification displays as the bottommost window. All other open windows display in front of it.
	Note: When sending a deployment or reboot notification for the first time, the deployment or reboot notification displays as the topmost window (with the exception of some dialogs, such as ***Windows Task Manager***). The notifications will display as the bottommost window in subsequent notifications.

Tip:

You can configure an agent policy to define the default **Show on Top** option setting for deployments and reboots when configuring a deployment or Mandatory Baseline. For additional information, refer to the following tasks:

- Creating an Agent Policy Set on page 430
- Editing an Agent Policy Set on page 436

Deployment Confirmation Page

This page displays the options that you've selected while completing the ***Deployment Wizard***. Use this page to verify the options that you've chosen before finishing the wizard and beginning the deployment.

Deployment Confirmation Text

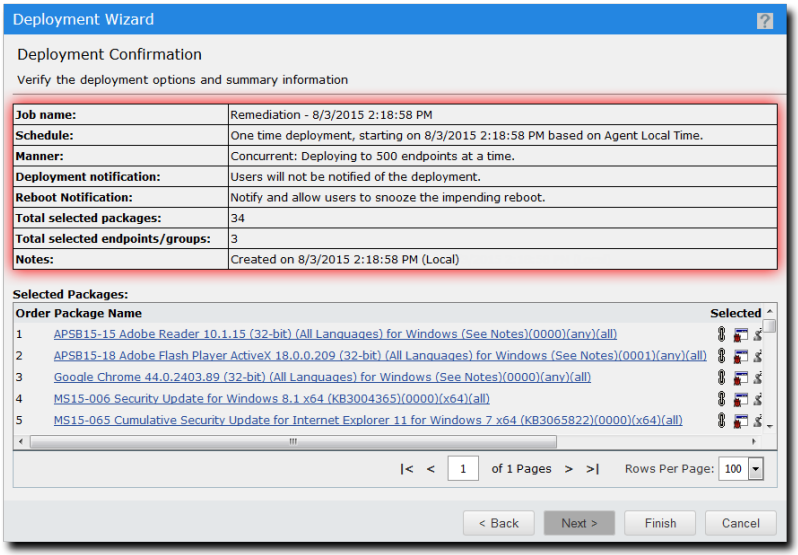


Figure 59: Deployment Confirmation Text

The upper portion of the page summarizes what options you selected while completing the ***Deployment Wizard***.

Table 149: Deployment Confirmation Text

Text	Description
Job Name	The job name that you entered.
Schedule	The deployment schedule that you chose.
Manner	The manner that the patches are deployed.
Deployment notification	The option that you selected for notifying endpoint users of deployments.
Reboot notification	The option that you selected for notifying endpoint users of deployment reboots.

Text	Description
Total selected packages	The total number of packages included in the deployment. **Note:** Some patches include more than one package. If the number of packages in the deployment exceeds the number of patches you selected for deployment, one or more package likely includes multiple packages.
Total selected endpoints/groups	The total number of endpoints and groups included in the deployment. Both endpoints and groups add a value of 1. For example, if you select 5 endpoints and 1 group of 5 endpoints, the total is 6, not 10.
Notes	Any notes that you entered to describe the deployment and its purpose.

Note: When an agent is installed on a server where multiple users are logged in simultaneously, the deployment manager will provide each user with the ability to snooze or reject the deployment and/or reboot if snooze or reject is enabled.

Selected Packages

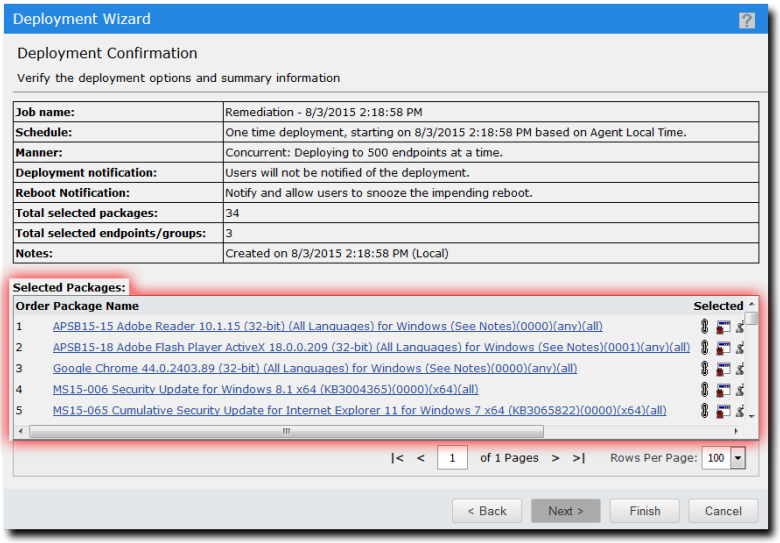


Figure 60: Selected Packages

The lower portion of the page lists the packages you chose for deployment.

Table 150: Selected Packages Column Descriptions

Column	Description
Order	The package's place in queue during the deployment. The order is optimized to minimize reboots.

Column	Description
Package Name	The name of the package being deployed.
Selected Options	The options and flags that you selected while configuring the deployment.
Reboot	Indicates if a reboot is required to complete installation of the package.
Endpoints/Groups	The number of endpoints and groups the package is deploying to.

After reviewing the ***Deployment Confirmation*** page, click **Finish** to proceed to the Deployment Summary Page on page 290.

Deployment Summary Page

This page lists all the options that you chose while completing the ***Deployment Wizard***. You can also use this page to cache packages before beginning the deployment.

All information displayed is identical to the info displayed on the Deployment Confirmation Page on page 288.

More importantly, you can use the page to *cache* packages before beginning the deployment.

What's *Caching*?

Caching is the process of commanding the Ivanti Endpoint Security Server to download selected packages to its local hard drive.

Why Should I Cache Packages Before a Deployment?

- Caching ensures that packages are installed in an optimized, predictable order.
- Starting a deployment without caching the packages first may result in unpredictable endpoint behavior. Packages are deployed as they are downloaded. For example, if deployment includes multiple packages that require a reboot, endpoints may repeatedly enter a reboot state, or (even worse) endpoints force reboots multiple times, thus interrupting employee work.

How do I Know When I Need to Cache Packages?

If you haven't already cached the packages you're deploying, the ***Selected Pages*** list includes red warning text and controls related to caching. We recommend waiting until caching completes before closing the ***Deployment Wizard***. Read about caching information in the table that follows.

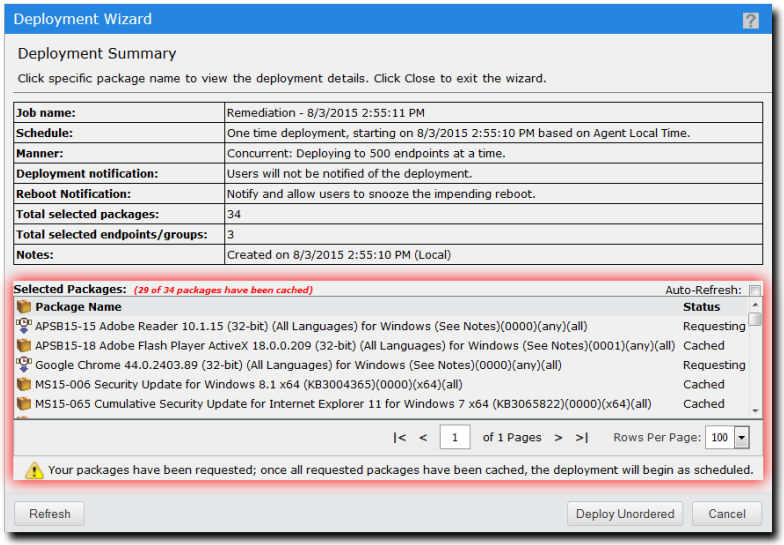


Figure 61: Deployment Summary Page - Packages Not Cached

Table 151: Selected Packages (Caching Packages)

Column	Description
Package Icon	Contains an icon that indicates if the package is cached or is being requested. Mouse over the icon for a description.
Package Name	The name of the package being deployed.
Status	Indicates the package cache status. • **Cached** • **Requesting**

If you don't see these controls, go ahead and close the wizard. You're all set because the packages are cached.

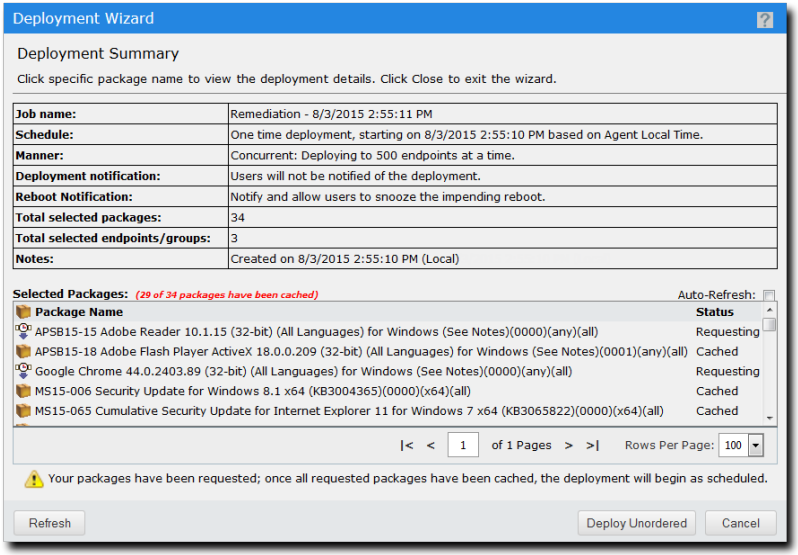


Figure 62: Deployment Summary Page - Packages Cached

After you finish reviewing the summary, click **Close** to dismiss the ***Deployment Wizard***.

The Deployment Details Page

The ***Deployment Details*** page shows targeted endpoint groups, targeted endpoints, deployment status, and deployment times for individual deployments.

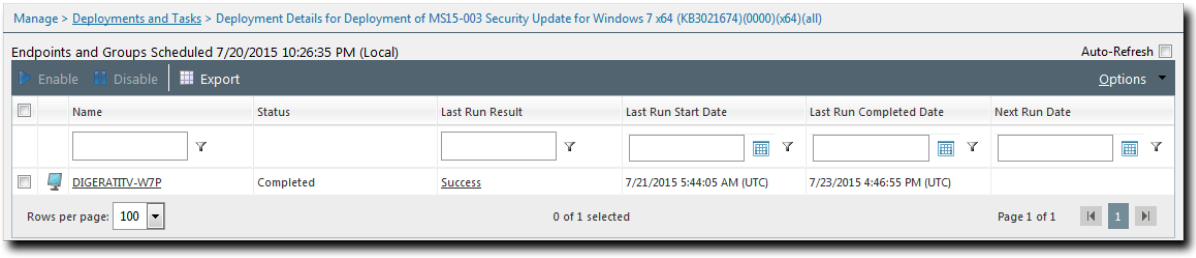


Figure 63: The Deployment Details Page

Viewing the Deployment Details

View the ***Deployment Details*** page for details about a specific deployment.

View the ***Deployment Details*** page by clicking a link from the ***Deployments and Tasks*** page.

1. From the **Navigation Menu**, select **Manage** > **Deployments and Tasks**.
2. Expand a deployment.

3. Click a package to view details about its deployment.

The Deployment Details Page Toolbar

The ***Deployment Details*** page toolbar contains functionality that you can use to enable and disable deployments and export deployment detail information.

The following table describes each toolbar button.

Table 152: Deployments Details Page Toolbar

Menu Item	Function
Enable	Enables the selected disabled deployment (Patch and Remediation only). For additional information, refer to Enabling Deployments on page 254.
Disable	Disables the selected enabled deployment (Patch and Remediation only). For additional information, refer to Disabling Deployments on page 254.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Deployment Details Page List

Details for individual deployments that you select from the ***Deployments and Tasks*** page reside in the ***Deployment Details*** page list.

Table 153: Deployment Details Column Definitions

Column	Description
Agent Status Icon	Indicates the status of the endpoint or endpoint group. For additional information, refer to Agent Module Status Icons on page 168.
Name	Indicates the name of the endpoint or endpoint group. The group name is a link; clicking the link displays the group membership and individual endpoint results.

Column	Description
Status	Indicates the current status of the deployment. Values include: • **Success** • **Not Patched** • **Not Deployed** • **Aborted** • **Failed** **Note:** A state of **Not Deployed** indicates that the patch either does not apply or has been marked *Do Not Patch*.
Last Run Result	Indicates the deployment's status when last ran. The status is a link; clicking the link displays the Package Deployment Results page.
Last Run Start Date	Indicates the date and time the deployment began.
Last Run Completed Date	Indicates the date and time the deployment completed.
Next Run Date	Indicates the next scheduled start date and time for this deployment.

Deployment Details for Package

You can view details for a package's deployment progress or outcome. This information may be helpful for troubleshooting purposes, such as if a package deployment fails.

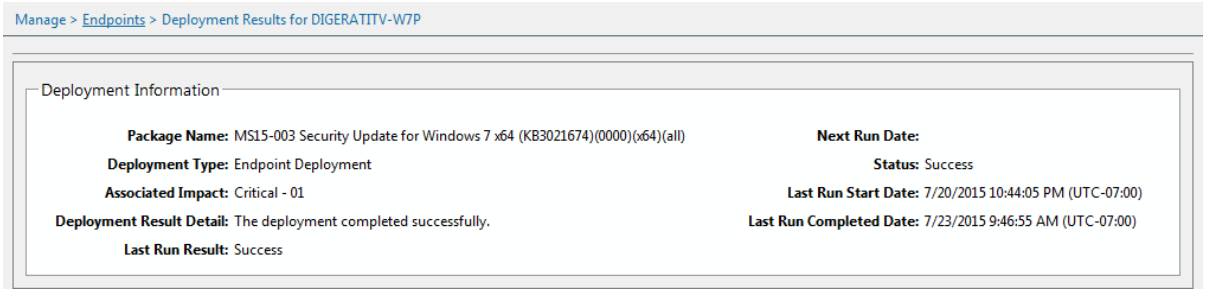


Figure 64: Deployment Results

The following table describes the text displayed in ***Deployment Information***.

Table 154: Deployment Information Fields

Field	Description
Package Name	Indicates the name of the package that was deployed.
Deployment Type	Indicates the deployment type.

Field	Description
Associated Impact	Indicates if the impact of the package.
Deployment Result Detail	Indicates the overall deployment status information.
Last Run Result	Indicates the result of the last time the endpoint performed the deployment.
Next Run Date	Indicates if the deployment is recurring and displays the date when the endpoint is to perform the deployment again.
Status	Indicates the result of the last time the endpoint performed the deployment. Values include: • **Success** • **Not Patched** • **Not Deployed** • **Aborted** • **Failed** **Note:** A state of **Not Deployed** indicates that the patch either does not apply or has been marked *Do Not Patch*.
Last Run Date	Indicates the status of the last time the endpoint performed the deployment.
Last Run Start Date	Indicates the date when the endpoint last started the deployment.
Last Run Completed Date	Indicates the date when the endpoint last finished the deployment.
Do Not Patch Reason	If a user has marked the package *Do Not Patch*, this text indicates the reason that the patch was marked for exclusion (if the user entered one).

Chapter 10

Using Groups

In this chapter:

Within Ivanti Endpoint Security, you can organize endpoints into groups, which are collections of endpoints. Organizing endpoints into a group lets you manage them as a single object.

About Groups

A *group* is a collection of endpoints that you can manage collectively. Within Ivanti Endpoint Security you can create custom groups to administer all endpoints as a single object.

Groups are organized into a tree hierarchy in which groups are nested; groups can contain other groups. This structure allows for inheritence of group members and policies, helping to minimize endpoint maintenance.

- For more information about the controls used to managed groups, see The Groups Page Browser on page 299.
- For more information about how you can use groups and their hierarchy to simplify Ivanti Endpoint Security administration, see Group Hierarchy on page 300.
- For more information about the different types of groups in Ivanti Endpoint Security, see Defining Groups on page 302.

The Groups Page

Use this page to control groups. The functions from many other Ivanti Endpoint Security pages are available from this page (the ***Endpoints*** page, the ***Users and Roles*** page, and so on). However, the functions performed on the ***Groups*** page pertain primarily to the selected group's endpoints.

Groups are selected from the **Browser**, a ***Groups*** page pane. The browser displays an expandable tree that lists parent and child groups. From this browser, you can access group information by clicking a group. Information for the selected group displays in the main pane.

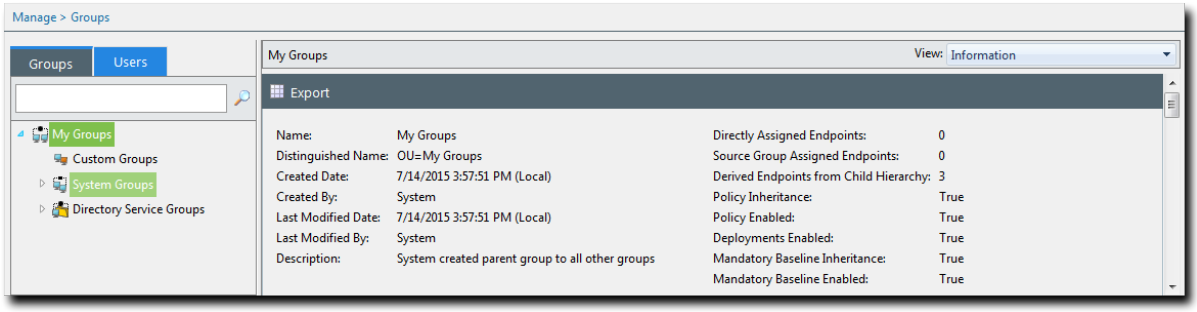


Figure 65: Groups Page

Unlike most other Ivanti Endpoint Security pages, which are organized by tabs, the ***Groups*** page is organized by views, which are selectable from the **View** list. The information displayed for a selected group changes according to view.

The views are:

- The Information View on page 303
- The Group Membership View on page 308
- The Endpoint Membership View on page 316
- The Mandatory Baseline View on page 351
- The Vulnerabilities/Patch Content View on page 371
- The Inventory View on page 378
- The Deployments and Tasks View on page 379
- The Agent Policy Sets View on page 384
- The Antivirus Policies View on page 394
- The Virus and Malware Event Alerts View on page 397
- The Compliance Summary View on page 401
- The Compliance Detail View on page 401
- The Roles View on page 401
- The Dashboard View on page 406
- The Settings View on page 409

The Groups Page Browser

Interact with all groups in Ivanti Endpoint Security by using the ***Groups*** page **Browser**, which organizes your groups into a tree hierarchy.

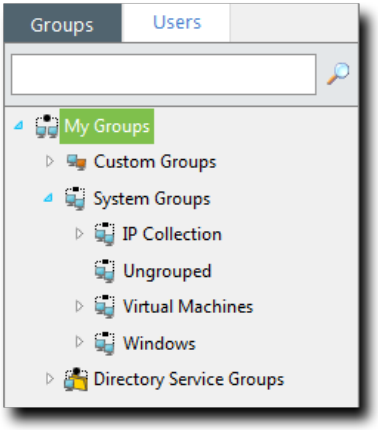


Figure 66: Browser

You can interact with the **Browser** in a variety of ways:

- You can expand the group hierarchy by clicking the **triangle**.
- You can collapse the group hierarchy by clicking click the **triangle** again.
- You can interact with a group by selecting it and using the ***Groups*** page features.
- You can create a new group, add endpoints to the selected group, or change views for the selected group by right-clicking it and making a selection from the menu.
- You can drag and drop custom groups by dragging the custom groups *icon* (not the group name) into another group.

Note: Remember a couple of thing when you are dragging and dropping groups:

- You can't drag a group down within its own child hierarchy. Groups can be moved to other group hierarchys however.
- If you drag a group with a child hierarchy into another group, the child hierachy gets moved as well.
- If the group you are moving is inheriting Agent Policy Sets, moving that group will change the policies it inherits. Before moving the group, check what Agent Policy Sets the group is inheriting, because moving a group without understanding its inherited policies can result in *big* changes to endpoint behavior!

Group Hierarchy

Within the ***Groups*** page **Browser**, groups are organized into a tree hierarchy. This hierarchy creates a structure similar to a family tree. This structure allows you to aggregate group membership and settings through inheritance. Familiarize yourself with examples of group hierarchy in this topic to understand how groups impact endpoint group membership and settings.

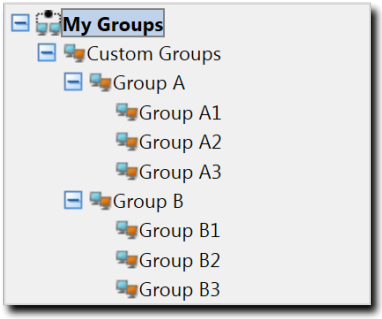


Figure 67: Group Tree Example

Root Group	In the Ivanti Endpoint Security group tree structure, the root group is the group of origin, which has no parents or ancestors. Within Ivanti Endpoint Security, **My Groups** is the root group, and all other groups are its descendent.

Parent Group	A parent group is a group that is one branch higher in the tree than the groups below it. In the figure above, **Group A** is parent of **Group A1**, **Group A2**, and **Group A3**. A parent group can have multiple child groups, and these children inherit the parent group settings.
Child Group	A child group is a group that is one branch lower in the tree than its parent. In the figure above, **Group A1** is the child of **Group A**. Each child group can only have one parent, and the child group inherits its parent settings by default.
Sibling Groups	Sibling groups are groups that share a parent group. In the figure above, **Group A** and **Group B** are siblings. Any group can have zero, one, or more siblings.
Ancestor Groups	Ancestors groups are all the groups above a group in the tree hierarchy for a single lineage. In the figure above, **Group A1** has ancestor groups of **Group A**, **Custom Groups**, and **My Groups**. **Group B** *is not* an ancestor group for **Group A1**.
Descendent Groups	Descendent groups are all the groups below a group in the tree hierarchy. In the figure above, **Customs Groups** has descendants in **Group A** (and all its child groups) and **Group B** (and all its child groups).
Leaf Group	A leaf group is a group that has no children. In the figure above, **Group A1** is a leaf group.
Inheritance	Inheritance is the mechanism that allows groups to aggregate endpoint membership and settings. • Endpoint membership is inherited *up* the tree. For example, endpoints added to **Group A3** are aggregated to with the endpoints directly assigned to **Group A**. • Settings (such as mandatory baselines and agent policies) are inherited *down* the tree. For example, an Agent Policy Set assigned to **Custom Group**s is also assigned to **Group A**, as well as groups **A1**, **A2**, and **A3**. Setting inheritance is enabled by default, but you can also disable it. Each group has its own inheritance settings. See Editing Group Settings on page 409.

Note: Within the **Browser**, `System Groups` and `Directory Service Groups` hierarchies cannot be modified. For additional information on group types, refer to Defining Groups on page 302.

Defining Groups
Within Ivanti Endpoint Security, there are several types of groups. Some groups are created by users, while others are created by the Ivanti Endpoint Security system. When working with groups, only user-created groups can be deleted.

Groups are categorized into the following classifications.

Table 155: Group Definitions

Groups	Group Type	Icon	Description
My Groups	Custom Groups	(Parent) and (Child)	Custom groups are created and managed by the user.
	System Groups[1]	(Parent) and (Child)	These groups are system created groups.
	Directory Service Groups	(Parent) and (Child)	These groups are created when an agent submits a directory service hierarchy that does not already exist in Ivanti Endpoint Security. You cannot modify **Directory Service Groups** or their hierarchies.
(1) Endpoints identified in your network are automatically assigned a group membership based on IP address, Active Directory (AD) membership, or operating system. Not all IP ranges, AD groups, or operating systems may be shown. This omission is because Ivanti Endpoint Security creates system groups based on only the endpoints present in your network.			
Note: An **Ungrouped** group is a group of endpoints that have not yet been added to a custom group. A **Virtual Machines** group is a group that is created for endpoints that are in a virtual machine environment (VMware, Citrix, etc). You cannot modify **System Groups** or their hierarchies.			

Viewing Groups

Navigate to the ***Groups*** page to work with groups. After navigating to the page, select a group and a view.

You can select this page from the navigation menu at any time.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. Expand the **Browser** tree to the desired group.
3. Select the group you want to view.

   Step Result: The selected group's information displays.

4. Select the desired view from the **View** list.

Tip: You may right-click within the **Browser** tree and select either the **Create Group** option, **Add Endpoints to Groups** option, or a specific view. You must be on **Custom Groups** to utilize the **Create Group** or **Add Endpoints to Groups** option.

Result: The selected group's information displays on the main pane. Select a different view from the **View** list to change the information displayed.

The Information View

This view includes basic information about the selected group's membership, hierarchy, agent policy sets, roles, and so on. Select this view for a comprehensive listing of group settings.

Group settings and information appear in sections. Each section displays information for each type of group settings. Empty sections indicate undefined settings.

The ***Information*** view features the following sections:

- Group Information on page 304
- Email Notification Addresses on page 305
- Child Groups on page 305
- Mandatory Baseline Items on page 306
- Agent Policy Sets on page 307
- Resultant Agent Policy Set Information on page 307
- Roles on page 308

Patch and Remediation updates **Information**:

- New fields are added to Group Information on page 304.
- A new section is added: Mandatory Baseline Items on page 306.

For additional information about unlisted sections, refer to *The Information View* in Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

The following table describes the ***Information*** view buttons.

Table 156: Information View Button

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Group Information

The first section in the ***Information*** view displays general information about the selected group's settings. These settings are controlled within the various ***Groups*** page views. Select this view when you want to see a group's settings from a single source.

The following table describes the first fields within the first section of the **Information** view.

The following table describes the new fields that are added to the ***Information*** view after Patch and Remediation is installed.

Table 157: Group Information

Field	Description
Name	Indicates the name of the group.
Distinguished Name	Indicates the system-created name based upon the group's parent hierarchy.
Created Date	Indicates the date and time the group was created.
Created By	Indicates the user who created the group.
Last Modified Date	Indicates the date and time the group was last modified.
Last Modified By	Indicates the user who last modified the group.
Description	Indicates the description of the group.
Directly Assigned Endpoints	Indicates the number of endpoints assigned to the group. Inherited endpoints are not included.
Source Group Assigned Endpoints	Indicates the number of endpoints assigned to the source group.
Derived Endpoints from Child Hierarchy	Indicates the number of endpoints inherited from child groups.
Policy Inheritance	Indicates if agent policy sets are inherited from the group's parent (`True` or `False`).
Policy Enabled	Indicates if agent policy sets can be assigned to the group (`True` or `False`).
Deployment Enabled	Indicates if deployments can be created for the group (`True` or `False`).
Mandatory Baseline Inheritance	Indicates if Mandatory Baseline settings are inherited from the group's parent (`True` or `False`).
Mandatory Baseline Enabled	Indicates if Mandatory Baseline deployments are created based upon the group's Mandatory Baseline configuration (`True` or `False`).

Email Notification Addresses

After a group is created, it can be assigned an email address. This email is intended to be attributed to the group.

Email addresses are not assigned from the ***Information*** view; this view merely displays the assigned addresses. For additional information on assigning an email address to a group, refer to Editing Group Settings on page 409.

The following reference describes the **Email Notification Addresses** table.

Table 158: Email Notification Addresses Table

Column	Description
Notification Address	The email addresses of the group owner.

Child Groups

This section lists the direct Child Groups. Only direct children are listed; deeper descendants such as grandchild groups are not listed.

Tip: This section only lists direct Child Groups; to assign direct Child Groups to a group use the ***Group Membership*** view.

Table 159: Child Groups Table

Column	Description
Type	The group type (`Custom Group`, `System Group`, or `Directory Service Group`).
Group Name	The name of the child group.
Distinguished Name	The system-created name of the group, which is based upon the group's parent hierarchy.
Description	The description of the group.

Antivirus Policies

This section lists the antivirus policies assigned, and whether or not that policy set is directly assigned or inherited from a parent. This section only shows the antivirus policies assigned; you cannot use it to assign one. Assign an antivirus policy to the selected group via the **Antivirus Policies** view.

The following reference describes the **Antivirus Policies** table.

Table 160: Antivirus Policies

Field	Description
Policy Name	Indicates the name of the antivirus policy.

Field	Description
Policy Type	Indicates if the antivirus policy type is a *Recurring Virus and Malware Scan* or a *Real-time Monitoring Policy*.
Source	Indicates if the antivirus policy is directly assigned or inherited from a parent.

Antivirus Real-time Monitoring Resultant Policy

If two or more real-time monitoring policies are assigned, their combined resultant effect is displayed in this section. The policy details can only be viewed here; you cannot change or edit them.

The following reference describes the **Antivirus Real-time Monitoring Resultant Policy** table.

Table 161: Antivirus Real-time Monitoring Resultant Policy

Field	Description
Virus Detection Action	Indicates actions to take upon virus/malware detection.
Local users	Indicates real-time scan options for local users.
Services and remote users	Indicates real-time scan options for services and remote users.
Exclude Path/ Filename	Indicates if path(s)/filename(s) will be excluded from the scan
Optional drives	Indicates if optional drives will be included in the scan.

Mandatory Baseline Items

Tip: This section only lists group Mandatory Baseline items; to assign items to a group, use the ***Mandatory Baseline*** view.

Table 162: Mandatory Baseline Items Table

Column	Description
Name	The Mandatory Baseline item name. The name doubles as a link the item's ***Review*** page.
Content Type	The content type of the Mandatory Baseline item. For a description of each impact, refer to one of the following pages based on the applicable type of Mandatory Baseline item: • Vulnerabilities on page 461 • Software Content on page 462 • Other Content on page 462

Column	Description
Vendor	The name of the vendor that created the software in the Mandatory Baseline item.
Vendor	The name of the vendor that created the software in the Mandatory Baseline item.
OS List	The operating systems that the Mandatory Baseline item applies to.

Agent Policy Sets

This section lists the Agent Policy Sets assigned to the selected group, and whether or not that policy set is directly assigned or assigned via inheritance.

Tip: This section only lists group Assigned Policy Sets; to Assign Policy Sets to the selected group use the ***Policies*** view.

Table 163: Agent Policy Sets Table

Field	Description
Policy Set Name	Indicates the name of the Agent Policy Set.
Assigned	Indicates if the Agent Policy Set is directly assigned to the group or inherited. A value of `True` indicates the Agent Policy Set is directly assigned.

Note: When a group **Policy Enabled** setting is enabled, the group will use the Global System Policy set to define undefined policies. For additional information, refer to Defining Agent Policy Inheritance Rules on page 418.

Resultant Agent Policy Set Information

When a group is assigned two or more Agent Policy Sets, some of the policies may conflict. When conflicts occur, the system applies the agent policy conflict resolution rules to determine which policy to apply. This section lists the resultant policies used when there is Agent Policy Sets conflict.

The following table describes the ***Resultant Agent Policy Set Information*** information.

Table 164: Resultant Agent Policy Set Information

Field	Description
Name	The name of the agent policy.
Value	The agent policy value. When determining the policy value, directly assigned policies supersede inherited policies. Additionally, directly assigned policies that conflict are resolved by the conflict resolution rules.

Field	Description
Description	The description of the agent policy.

Note: Only agent policies inherited or directly assigned to the group are displayed in **Resultant Agent Policy Set Information**. To see a complete listing of all policies assigned to a managed endpoint, refer to The Information Tab on page 189.

Roles

You can restrict user access to specific groups based on roles. This section lists the user roles that can access the selected group.

Tip: This section only lists the Roles that can access the group; to assign Roles to a group, use the ***Roles*** view.

Table 165: Roles Table

Field	Description
Role Name	Indicates the name of the user role that can access the group.
Role Source	Indicates the name of the group that the assigned role is inherited from. If the role source contains no value, the role is directly assigned to the selected group.
Assigned	Indicates if the role is inherited or directly assigned to the group. A value of `True` indicates the role is directly assigned to the group.

Exporting Information View Data

To export the information displayed within the ***Information*** view to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Group Membership View

This view lets you view the selected group's direct child groups. If the selected group is a custom group, you can also create new custom child groups that you can populate with the desired endpoints. Custom groups also let you edit or delete any listed preexisting child groups.

This view only lists direct child groups; you cannot manage grandchild groups or further descendants.

The Group Membership View Toolbar

This toolbar contains buttons related to the creation and management of groups.

The following table describes the toolbar functions. Some functions are common to all the ***Groups*** page views.

Table 166: Group Membership Toolbar

Button	Function
Create	Creates a new group. For additional information, refer to Creating a Group on page 310.
Delete	Deletes a group. For additional information, refer to Deleting Groups on page 311.
Move...	Assigns a group to a new parent group. For additional information, refer to Moving a Group on page 312.
Deploy...	Deploys content to selected groups. For additional information, refer to Deploying Content to Groups (Group Membership View) on page 314.
Scan Now (menu)	Opens the **Scan Now** menu.
Discover Applicable Updates... (**Scan Now** menu item)	Prompts the Discover Applicable Updates task to launch immediately and check a group for vulnerabilities. For additional information, refer to Using Scan Now to Scan Groups on page 315.
Reboot Now...	Initiates the Reboot task for endpoints in the selected group. For additional information, refer to Rebooting Groups on page 315.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Group Membership View List

This list displays the selected group's direct child groups. Each listing contains group identification information and icons used to edit identification information or delete the group altogether.

The following table displays the ***Group Membership*** view list details.

Table 167: Group Membership View

Column	Icon	Description
Action	N/A	Contains **Edit** and **Delete** icons. Use these icons to edit or delete the associated group.
Groups		Contains an icon that indicates the type of the group: • `System` () • `Custom` () • `Directory Service` ()
Name	N/A	Indicates the name of the child group.
Description	N/A	Indicates the description of the group.
Distinguished Name	N/A	Indicates the system-created name based upon the group's parent hierarchy.
Endpoints	N/A	Indicates the number of endpoints assigned to the group.

Note: ***System*** and ***Directory Service*** groups cannot have their child group or endpoint memberships edited. However, their assigned agent policy sets can be edited.

Creating a Group

Ivanti Endpoint Security provides preconfigured groups. However, you can also create custom groups. Populate custom groups with desired endpoints. You can only create custom groups within the **Browser** custom group hierarchy.

Create groups from the ***Group Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. Select the ***Custom Group*** from the directory tree that you want to create a child group for.
4. Click **Create**.

   Step Result: A new row appears on the page.
5. In the **Name** field, type a name for the group.

6. [Optional] Type a brief description about the group in the **Description** field.
7. Click the **Save** icon associated with the new group.

Result: The group is saved to the list and is added to the directory tree. A ***Distinguished Name*** is generated for the group.

After Completing This Task:
Add endpoints to the group. For additional information, refer to Adding Endpoints to a Group on page 342.

Editing Groups

You can edit the names and descriptions for custom groups.

You may edit the name and description for groups within the **Custom Groups** hierarchy. Edit groups from the ***Group Membership*** view.

Note: For **System Groups** and **Directory Service Groups** only the **Description** field can be edited, not the **Name** field.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the **Group Browser**, select a group within the **Custom Groups** hierarchy you want to edit.
4. Click the **Edit** icon ( ).

   Step Result: The **Name** and **Description** field displays.
5. [Optional] Edit the **Name** field associated with the group.
6. [Optional] Edit the **Description** field associated with the group.
7. Click the **Save** icon associated with the new group.

Result: The group changes are saved.

Note: Within the ***Group Membership*** view, you can only edit the group name and description. To edit group behavior, use the ***Groups*** page views.

Deleting Groups

Delete a group when you no longer need to manage its endpoints collectively. Only custom groups can be deleted. After deleting a group, you cannot recover it; you must recreate the group.

Delete custom groups from the ***Groups Membership*** view.

Note: Deleting a group does not prevent an endpoint within that group from rebooting, deploying, or scanning; these tasks occur at the endpoint level.

1. From the **Navigation Menu**, select **Manage** > **Groups**.

2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the parent group of the group(s) you want to delete.

Note: Only groups within the **Custom Groups** hierarchy can be deleted.

4. Delete the desired group(s).
   Use one of the following methods.

Note: If the group you want to delete has a child hierarchy, the group cannot be deleted until the child groups have been deleted or moved.

Method	Steps
To delete a single group:	Click the **Delete** icon associated with the group you want to delete.
To delete multiple groups:	1. Select the check boxes associated with the groups you want to delete. 2. From the toolbar, click **Delete**.

   Step Result: A dialog appears asking you to acknowledge the deletion.

5. Click **OK**.

Result: The selected group(s) are deleted.

Moving a Group

After creating a group, you can change its position within the **Browser** tree.

Move groups from the ***Group Membership*** view on the ***Groups*** page.

Note: When moving a group, if the group is configured to inherit agent policies, roles, or any other settings, the group inherits those values from its new parent.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the **Browser**, select the parent group of the group you want to move.
4. Select the group you want to move.

5. Click **Move**.

Note: You cannot move groups in **System Groups** or **Directory Service Groups**.

Step Result: The ***Move Groups*** dialog opens.

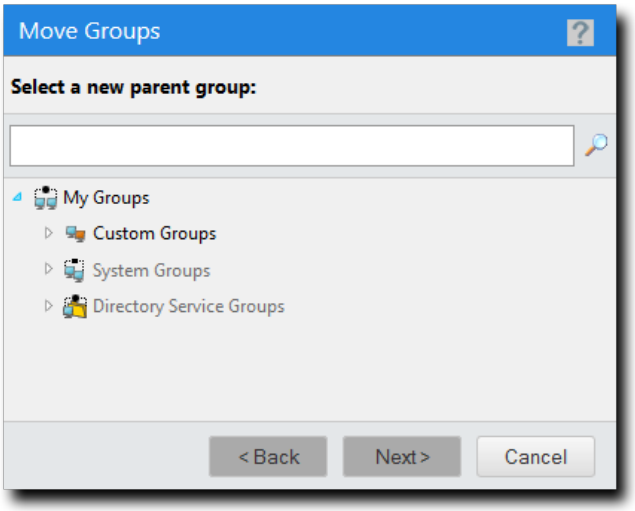


Figure 68: Move Groups Dialogs

6. Select a new parent group.

7. Click **Next**.

   Step Result: The group is moved to the new parent group.

   Note: If the group you are moving contains a child hierarchy, those groups are moved as well.

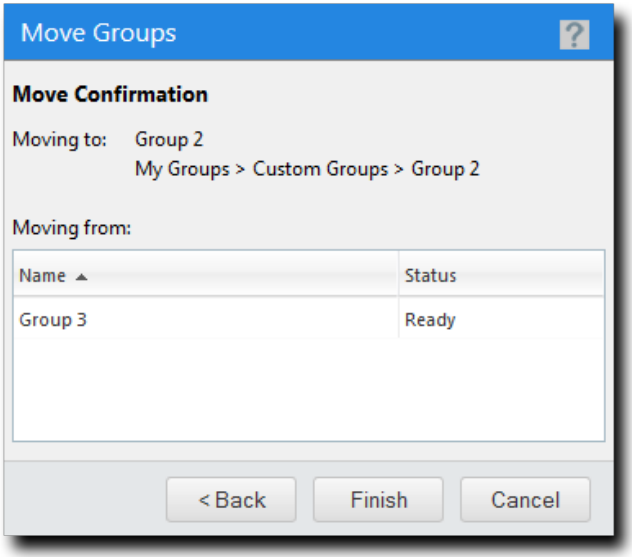


Figure 69: Move Confirmation

8. Click **Finish**.
9. Click **Close**.

Result: The select group is moved to its new place in the group hierarchy.

Deploying Content to Groups (Group Membership View)

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including the ***Groups*** page ***Group Membership*** view. When deploying from this view, the ***Deployment Wizard*** is preconfigured to deploy to the selected group.

For additional information, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the group you want to deploy content to.

4. Click **Deploy**.

Result: The ***Deployment Wizard*** opens, preconfigured to deploy to the selected group.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Using Scan Now to Scan Groups

You can initiate a Discover Applicable Updates (DAU) task for all endpoints in a selected group. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to Ivanti Endpoint Security, which you can view.

You can launch a DAU task for managed endpoints in a selected group. Perform this task from the ***Groups*** page ***Group Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the group you want to scan.
4. Click **Scan Now** > **Discover Applicable Updates**.

   Step Result: The ***Scan Now*** dialog opens.
5. Select the **Yes, scan all members of the selected group**.
6. [Optional] Select the **Include child groups in the scan**.
7. Click **Schedule**.
8. Acknowledge the scheduling by clicking **Close**.

Result: The scan is scheduled. As with all deployments, although the Discovery Applicable Updates task is scheduled for immediate execution, it will not actually occur until the next time the agent checks in.

Rebooting Groups

Within Ivanti Endpoint Security, you can reboot all endpoints within a given group.

Reboot entire groups from the ***Group Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the group you want to reboot.
4. Click **Reboot Now**.

   Step Result: The ***Reboot Now*** dialog opens.
5. Select the **Yes, reboot all members of the selected group** check box.
6. [Optional] Select the **Reboot child groups** check box.

7. Click **Reboot**.
8. Acknowledge the reboot scheduling by clicking **Close**.

Result: The reboot is scheduled. As with all deployments, although the reboot is schedule for immediate execution, it will not actually occur until the next time the agent checks in.

Exporting Group Membership View Data

To export information displayed in the ***Group Membership*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Endpoint Membership View

This view lists the endpoints that hold membership in the selected group. If the group selected is a custom group, you can also use this view to add endpoints. Use this view to manage endpoints assigned to the selected group. This view contains features similar to those available from the ***Endpoints*** page.

For additional information about this view, refer to The All Tab (Groups Page) on page 316.

A new tab is added after Patch and Remediation is installed. For additional information, refer to The Patch and Remediation Tab (Groups Page) on page 330.

The All Tab (Groups Page)

Use the ***All*** tab to perform tasks related to group endpoints.

The All Tab Toolbar (Groups Page)

The ***All*** tab toolbar contains buttons for you to perform tasks and functions for managed endpoints.

The following table describes the toolbar functions used in the ***All*** tab, available on the ***Groups*** page ***Endpoint Membership*** view.

Table 168: All Tab Toolbar (Groups Page)

Button	Description
Membership	Adds or removes managed endpoints to or from the selected group. For additional information, refer to Adding Endpoints to a Group on page 342.
Manage Agents... (menu)	Opens the Manage Agents menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 345.

Button	Description
Uninstall Agents... (**Manage Agents...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 345.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 345.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting Endpoints (Groups Page) on page 346.
Enable	Enables a disabled endpoint. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 347.
Disable	Disables an enabled endpoint. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 347.
Agent Versions...	Defines the endpoint agent version. For additional information, refer to Defining the Endpoint Agent Version (Groups Page) on page 345.
Manage Modules...	Opens the ***Add/Remove Modules*** dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Managing Endpoint Modules (Groups Page) on page 349.
Wake Now...	Wakes endpoints selected from the list. For additional information, refer to Waking Endpoints (Groups Page).
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The All Tab List (Groups Page)

The ***All*** tab lists the operating system, identification, agent, and module information for group endpoints.

The following table describes the columns within the ***All*** tab list.

Table 169: All Tab List Columns

Column	Description
Name	The name of the endpoint. Click the link to view its details.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include: **Online** — The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior. **Offline** — The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details. **Disabled** — The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.

Column	Description	
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values:	
	Started	EDS server has started and is in an operational state accepting workloads.
	Starting	EDS server is in the process of starting its service.
	Stopped	EDS server has stopped and is not accepting workloads.
	Stopping	EDS server is in the process of stopping so as to not accept workloads.
	Offline	EDS server is offline as it has not contacted the database in the configured amount of time.
Operating System	The operating system that the endpoint uses.	
Agent Version	The version of the Ivanti Endpoint Security Agent installed.	
	Note: A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.	

Column	Description	
***Module* Installed**	Indicates whether a module is installed on the endpoint. A new ***Module* Installed** column is added for each module installed on your Ivanti Endpoint Security Server. The following list defines column entry values:	
	Yes	The module is installed.
	No	The module is not installed.
	Pending Install	The module is in the process of installing.
	Pending Uninstall	The module is in the process of uninstalling.
	Pending Reboot	The module has been installed, but the endpoint needs to reboot to complete installation.
	Error	There was an error while installing or uninstalling the module. Click the for additional information about the error.
	Expired	The module license has expired.

The AntiVirus Tab (Groups Page)

Use the ***AntiVirus*** tab to perform tasks related to a selected group's endpoint.

The AntiVirus Toolbar (Groups Page)

The AntiVirus tab toolbar contains the tasks and functions that are available for you to perform for managed endpoints with AntiVirus features enabled.

The following table describes the toolbar functions used in the AntiVirus tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 170: AntiVirus Toolbar Functions

Button	Function
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.

Button	Function
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 179.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.
Enable (Menu)	Expands the **Enable** menu.
Enable Module (**Enable** menu item)	Enables the AntiVirus agent module on selected endpoints.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182. **Note:** This button is only available when an endpoint is disabled.
Disable (Menu)	Expands the **Disable** menu.
Disable Module (**Disable** menu item)	Disables the AntiVirus agent module on selected endpoints. For additional information, refer to Disabling Modules on an Endpoint on page 182.
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Manage Modules	Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions. For additional information refer to Installing Endpoint Modules on page 184.
Scan Now...	Launches the ***Virus and Malware Scan Wizard***. Use this wizard to launch an immediate anti-virus scan on the selected endpoint(s). For additional information refer to Running Scan Now on an Endpoint.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options	Opens the **Options** menu. For more information see The Options Menu on page 39.

The AntiVirus Tab List (Groups Page)
The AntiVirus tab list itemizes endpoint identification data, server connectivity, operating system, and agent information.

The following table describes the columns within the AntiVirus tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 171: AntiVirus Tab List Columns

Column	Description
Name	The name of the endpoint. Click the link to view its details.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.

Column	Description	
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:	
	Online	The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior.
	Offline	The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.	

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
AV State	State of the AntiVirus agent module (`Enabled`, `Disabled`).
AV Definition Version	Version of the definition file currently installed on the endpoint. **Note:** If the definition version is not the latest available, a warning triangle is displayed.
Last AV Definition Update (Server)	Date and time that the anti-virus definition was last updated on the endpoint.
AV Scan Status	Status of the latest anti-virus scan to run on the endpoint (`In-progress`, `Success`).
Last AV Scan Time (Server)	Date and time that the last anti-virus scan started, shown as server time.
Operating System	Operating system the endpoint is running.
AV Running Version	Version number of the AntiVirus module component installed on the endpoint.

Column	Description
Agent Version	Indicates the version of the agent that the endpoint is currently running. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

The Application Control Tab (Groups Page)

Use the ***Application Control*** tab to perform tasks related to a selected group's endpoint. This tab is similar to the ***Endpoints*** page ***Application Control*** tab, but lets you perform tasks from a group level.

The Application Control Toolbar (Groups Page)

The Application Control tab toolbar contains the tasks and functions that are available for you to perform for managed endpoints with Application Control features enabled.

The following table describes the toolbar functions used in the ***Application Control*** tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 172: Application Control Tab Toolbar (Groups Page)

Button	Description
Membership	Adds or removes managed endpoints to or from the selected group. For additional information, refer to Adding Endpoints to a Group on page 342.
Manage Agents... (menu)	Opens the Manage Agents menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 345.
Uninstall Agents... (**Manage Agents...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 345.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 345.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting Endpoints (Groups Page) on page 346.

Button	Description
Agent Versions...	Defines the endpoint agent version. For additional information, refer to Defining the Endpoint Agent Version (Groups Page) on page 345.
Enable (Menu)	Expands the **Enable** menu.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 347.
Enable Module (**Enable** menu item)	Enables the Application Control agent module on only selected endpoints. For additional information, refer to Enabling or Disabling Endpoint Modules within a Group on page 348.
Disable (Menu)	Expands the **Disable** menu.
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 347.
Disable Module (**Disable** menu item)	Disables the Application Control agent module on only selected endpoints. For additional information, refer to Enabling or Disabling Endpoint Modules within a Group on page 348.
Manage Modules...	Opens the Add/Remove Modules dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Managing Endpoint Modules (Groups Page) on page 349.
Wake Now...	Wakes endpoints selected from the list. For additional information, refer to Waking Endpoints (Groups Page).
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Application Control Tab List (Groups Page)

The ***Application Control*** tab list itemizes identification data, operating system, agent information, and Application Control policy information for each endpoint in the selected group.

The following table describes the columns within the ***Application Control*** tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 173: Application Control Tab List Columns

Column	Description
Endpoint Name	Indicates the name of the endpoint. Clicking the ***Endpoint Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.

Column	Description
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include: **Online** — The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior. **Offline** — The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details. **Disabled** — The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
LAC State	Indicates the state of the Application Control module component on the endpoint (`Enabled` or `Disabled`).
LAC Policy Enforcement	Indicates the Application Control policy enforcement.
Operating System	The operating system that the endpoint uses.
LAC Running Version	Indicates the version of the Application Control module component installed on the endpoint.
Agent Version	The version of the Ivanti Endpoint Security Agent installed. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

The Patch and Remediation Tab (Groups Page)

Use the ***Patch and Remediation*** tab to perform tasks related to a selected group's endpoint. This tab is similar to the ***Endpoints*** page ***Patch and Remediation*** tab, but lets you perform tasks from a group level.

The Patch and Remediation Tab Toolbar (Groups Page)

The ***Patch and Remediation Tab*** toolbar contains the tasks and functions that are available for you to perform for managed endpoints with Patch and Remediation features enabled.

The following table describes the toolbar functions used in the ***Patch and Remediation*** tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 174: Patch and Remediation Tab Toolbar (Groups Page)

Button	Description
Deploy...	Launches the ***Deployment Wizard***, which allows you to create a deployment for the selected endpoints (Patch and Remediation only). For additional information, refer to Deploying Content to Endpoints (Endpoint Membership View) on page 344.
Manage Agents... (menu)	Opens the Manage Agents menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 345.
Uninstall Agents... (**Manage Agents...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 345.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 345.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting Endpoints (Groups Page) on page 346.
Enable (Menu)	Expands the **Enable** menu.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182.

Button	Description
Enable Module (**Enable** menu item)	Enables the Patch and Remediation module for selected endpoints. For additional information, refer to Enabling or Disabling Endpoint Modules within a Group on page 348.
Disable (Menu)	Expands the **Disable** menu.
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Disable Module (**Disable** menu item)	Disables the Patch and Remediation module for selected endpoints. For additional information, refer to Enabling or Disabling Endpoint Modules within a Group on page 348.
Agent Versions...	Defines the endpoint agent version. For additional information, refer to Defining the Endpoint Agent Version (Groups Page) on page 345.
Manage Modules...	Opens the Add/Remove Modules dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Managing Endpoint Modules (Groups Page) on page 349.
Scan Now...	Launches the DAU task on selected endpoints. For additional information, refer to Using Scan Now to Scan Groups on page 349.
Reboot Now...	Prompts the selected endpoint to reboot. For additional information, refer to Rebooting Group Endpoints on page 350.
Wake Now...	Wakes endpoints selected from the list. For additional information, refer to Waking Endpoints (Groups Page).
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Patch and Remediation Tab List (Groups Page)
The ***Patch and Remediation Tab*** tab list itemizes endpoint identification data, server connectivity, operating system, and agent information.

The following table describes the columns within the ***Patch and Remediation Tab*** tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 175: Patch and Remediation Tab List Columns

Column	Description
Name	The name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.
Status (icon)	The icon representing the Patch and Remediation module status. You can mouse over the icon to display description of the Patch and Remediation status. For additional information, refer to Agent Module Status Icons on page 168.

Column	Description	
Agent Status	Indicates the status of the endpoint. The following list defines column values:	
	Online	The agent is able to communicate with the Ivanti Endpoint Security server in the predefined time period. Refer to Configuring the Agents Tab on page 89 for additional information on configuring agent default behavior.
	Offline	The agent is unable to communicate with the Ivanti Endpoint Security server in the predefined time period. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status, indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is either offline or has an update required status. Click the icon to find out additional status details and EDS server information.
	Disabled	The agent will no longer enforce any module policies or complete tasks. All endpoints must show a `Disabled` status in order to delete the endpoint. Refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.	

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
PR Status	The status for Patch and Remediation module on the endpoint (`Working`, `Idle`, `Sleeping`, `Offline`, `Disabled`).
DAU Status	The status of the Discover Applicable Updates (DAU) scan when last run. The status is also a link to the applicable ***Deployment Results*** page. Status values include: `Success` or `Failure` followed by the failure code, and `Not Available`, which indicates that the endpoint has not checked in. **Note:** The `Not Available` **DAU Status** is not a hyperlink (Patch and Remediation only).
Last DAU Scan (Server)	The date and time of the last successful DAU scan (server side). A value of `Not Available` indicates the endpoint has not completed a DAU scan (Patch and Remediation only).
Operating System	The operating system the endpoint is running.
PR Running Version	The Patch and Remediation module version number running on the endpoint.
Agent Type	The type of agent that is running on the endpoint and communicating with Ivanti Endpoint Security (Ivanti Endpoint Security or Patch).

Column	Description
Agent Version	Indicates the version of the agent that the endpoint is currently running. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

The Power Management Tab (Groups Page)

Use the ***Power Management*** tab to perform tasks related to a selected group's endpoint. This tab is similar to the ***Endpoints*** page ***Power Management*** tab, but lets you perform tasks from a group level.

The Power Management Tab Toolbar

This toolbar contains buttons you can use to enable or disable the Power Management component on listed endpoints.

The toolbar includes the following buttons.

Table 176: Power Management Tab Toolbar

Button	Description
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 180. For additional information, refer to Downloading the Agent Installer in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 181.
Enable (Menu)	Expands the **Enable** menu.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 182.

Button	Description
Enable Module (**Enable** menu item)	Enables the Power Management agent module on only selected endpoints. For additional information, refer to Enabling or Disabling Endpoint Modules within a Group on page 348.
Disable (Menu)	Expands the **Disable** menu.
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 183.
Disable Module (**Disable** menu item)	Disables the Power Management agent module on only selected endpoints. For additional information, refer to \Enabling or Disabling Endpoint Modules within a Group on page 348.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 179.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to add and remove modules to or from the endpoint. For additional information, refer to Installing Endpoint Modules on page 184.
Wake Now...	Wakes endpoints selected from the list. For additional information, refer to Waking Endpoints (Groups Page).
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Power Management Tab List (Groups Page)

The ***Power Management*** tab list itemizes endpoint identification data, operating system, agent information, and Power Management policy information.

The following table describes the columns within the ***Power Management*** tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 177: Power Management Tab List Columns

Column	Description
Endpoint Name	Indicates the name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page.
IP Address	Indicates the IP address of the endpoint.
Agent Status	Indicates the status of the endpoint (`Online`, `Offline`, or `Disabled`).
Last LPM Reporting Time (Server)	Indicates the last time the Ivanti Power Managementstate was reported to the server.
PM State	Indicates the status of Ivanti Power Management (`Enabled` or `Disabled`).
Operating System	Indicates the operating system the endpoint is running.
PM Running Version	Indicates the version of Ivanti Power Management installed on the endpoint.
Agent Version	Indicates the version of the agent that the endpoint is currently running. **Note:** A icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.

The Device Control Tab (Groups Page)

Use the ***Device Control*** tab to perform tasks related to a selected group's endpoint. This tab is similar to the ***Endpoints*** page ***Device Control*** tab, but lets you perform tasks from a group level.

The Device Control Toolbar (Groups Page)

The Device Control tab toolbar contains the tasks and functions that are available for you to perform for managed endpoints with Device Control features enabled.

The following table describes the toolbar functions used in the ***Device Control*** tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 178: Device Control Tab Toolbar (Groups Page)

Button	Description
Membership	Adds or removes managed endpoints to or from the selected group. For additional information, refer to Adding Endpoints to a Group on page 342.
Manage Agents... (menu)	Opens the Manage Agents menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 345.
Uninstall Agents... (**Manage Agents...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 345.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 345.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting Endpoints (Groups Page) on page 346.
Agent Versions...	Defines the endpoint agent version. For additional information, refer to Defining the Endpoint Agent Version (Groups Page) on page 345.
Enable (Menu)	Expands the **Enable** menu.
Enable Agent (**Enable** menu item)	Enables a disabled endpoint. For additional information, refer toEnabling or Disabling Ivanti Endpoint Security Agents within a Group on page 347.
Enable Module (**Enable** menu item)	Enables the Device Control agent module on only selected endpoints. For additional information, refer to Enabling or Disabling Endpoint Modules within a Group on page 348.
Disable (Menu)	Expands the **Disable** menu.

Button	Description
Disable Agent (**Disable** menu item)	Disables an enabled endpoint. For additional information, refer toEnabling or Disabling Ivanti Endpoint Security Agents within a Group on page 347.
Disable Module (**Disable** menu item)	Disables the Device Control agent module on only selected endpoints. For additional information, refer to Enabling or Disabling Endpoint Modules within a Group on page 348.
Manage Modules...	Opens the Add/Remove Modules dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Managing Endpoint Modules (Groups Page) on page 349.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Device Control Tab List (Groups Page)
The ***Device Control*** tab list itemizes endpoint identification data, operating system, agent information, and Device Control policy information.

The following table describes the columns within the ***Device Control*** tab on the ***Groups*** page ***Endpoint Membership*** view.

Table 179: Device Control Tab List

Column	Description
Endpoint Name	The name of the endpoint. Clicking the ***Name*** link displays the applicable ***Endpoint Details*** page. See The Endpoint Details Page on page 187 for additional information.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information it can provide includes what system it belongs to, where it is located, and what it is used for. You can edit this name on the Endpoint Details page..
IP Address	The IP address of the endpoint.

Column	Description	
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:	
	Online	The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 89 for more information on configuring default agent behavior.
	Offline	The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.
	Disabled	The agent is

Column	Description
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** — EDS server has started and is in an operational state accepting workloads. **Starting** — EDS server is in the process of starting its service. **Stopped** — EDS server has stopped and is not accepting workloads. **Stopping** — EDS server is in the process of stopping so as to not accept workloads. **Offline** — EDS server is offline as it has not contacted the database in the configured amount of time.
DC State	Indicates the state of Device Control module component on the endpoint (`Enabled` or `Disabled`).
Operating System	The operating system that the endpoint uses.
DC Running Version	Indicates the version of the Device Control module component installed on the endpoint.

Column	Description
Agent Version	The version of the Ivanti Endpoint Security Agent installed. **Note:** A  icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.
Last Logged Event (Server)	Indicates the last date and time an event was recorded in the Device Control log.
Policy Up To Date	Indicates whether the Device Control policy is up to date (`True` or `False`).

Adding Endpoints to a Group

You can manage endpoints and mobile endpoints collectively by adding them to custom groups.

Add endpoints to a group from the ***Groups*** page.

1. From the **Navigation Menu**, select **Manage** > **Groups**.

2. From the **Groups** tree, right-click a group in the **Custom Groups** hierarchy and select **Add endpoints to group**.

Remember: Endpoints can only be added to custom groups.

Step Result: The ***Membership*** dialog opens.

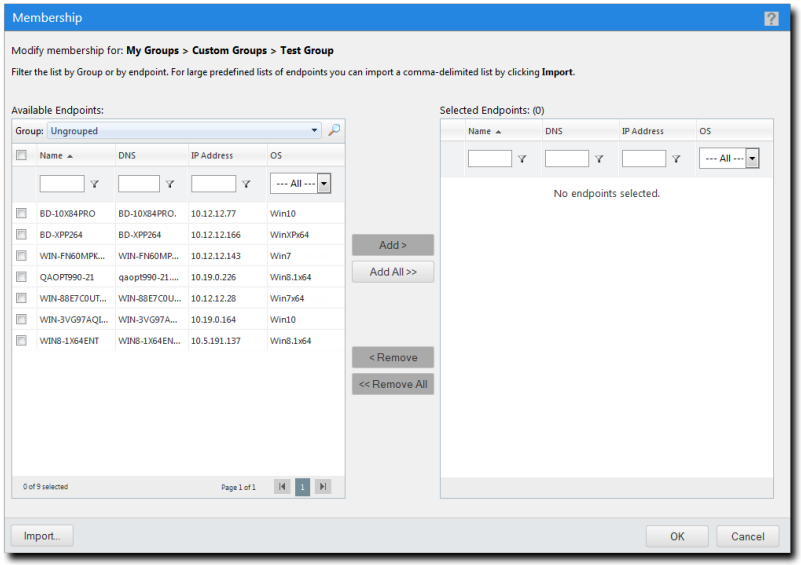


Figure 70: Membership Dialog

3. Add endpoints to the group.
   a) [Optional] To filter the endpoints that are listed down to a pre-existing group, select a **Group** from the drop-down list and click 🔍.
   b) [Optional] To filter the endpoints that are listed, type filter criteria in the table fields and click ⏷ to select an operator.
   c) Select endpoints and click **Add**.

Tip:

- Click **Add All** to include the entire list.
- You can add endpoints to the group by importing them from a list. Click **Import** to use this feature.
- Use the **Remove** and **Remove All** buttons to remove endpoints from the list.

   d) Review the list of endpoints to confirm it is correct.
4. Click **OK**.

Result: The selected endpoints are added to the group. Select **Endpoint Membership** from the **View** list to confirm they are added.

Importing Endpoints into Groups
If you are adding a large number of endpoints to a group, importing a list of endpoints can be faster than than selecting them individually within the ***Membership*** dialog.

Import Rules

- You can only import endpoints using their host names. IP Addresses cannot be imported.
- You must separate each endpoint with a comma.

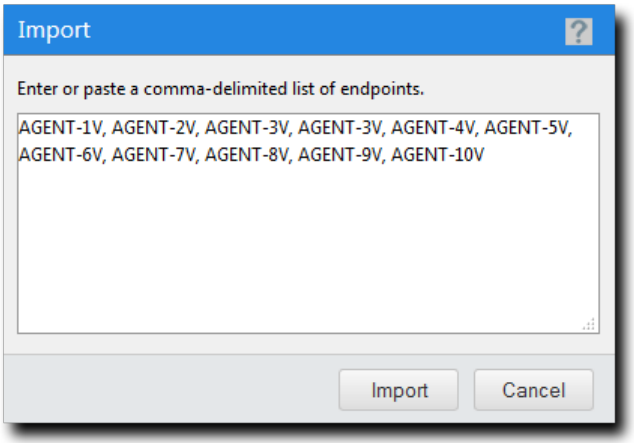


Figure 71: Import List Example

Tip: You can use Ivanti Endpoint Security to easily obtain a list of endpoints to import. To create a list:

1. Open the ***Endpoints*** page (**Manage** > **Endpoints**).
2. Using the page filters to display the endpoints you want to add to your group.
3. Click **Export**.
4. Open the exported .csv file and copy and paste the endpoint names into the **Import** dialog. Add a comma between each name.

Deploying Content to Endpoints (Endpoint Membership View)

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including the ***Groups*** page ***Endpoint Membership*** view. When deploying from this page, the ***Deployment Wizard*** is preconfigured to deploy content to selected endpoints within a selected group.

For additional information, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. From the directory tree, select the group containing endpoints you want to deploy content to.
4. Select the ***Patch and Remediation*** tab.

5. [Optional] Select endpoints to receive deployments.
6. Click **Deploy**.

Result: The ***Deployment Wizard*** opens, preconfigured to deploy to selected endpoints.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Installing Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of installing an agent on endpoints using an Agent Management Job. To create an Agent Management Job that installs agents from the ***Endpoint Membership*** view, select **Manage Agents** > **Install Agents** from the toolbar.

For additional information, refer to Installing Agents by Agent Management JobInstalling Agents by Agent Management Job.

Uninstalling Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of uninstalling an agent from endpoints using an Agent Management Job. To create an Agent Management Job that uninstalls agents from the ***Endpoint Membership*** view, select **Manage Agents** > **Uninstall Agents** from the toolbar.

To pre-populate the ***Schedule Agent Management Job - Uninstall Wizard*** **target** list, first select the desired group from the **Browser**, and then select the check box associated with the desired endpoints.

For additional information, refer to Uninstalling Agents by Agent Management Job.

Downloading the Agent Installer

You can install an agent on a local endpoint from the ***Endpoint Membership*** view.

To download an agent installer from the ***Endpoint Membership*** view, select **Manage Agents** > **Download Agent Installer** from the toolbar. For additional information, refer to Downloading the Agent Installer on page 180.

Defining the Endpoint Agent Version (Groups Page)

From the ***Groups*** page, you can upgrade your endpoints to a newer version of the agent.

Define agent version(s) for group endpoints from the ***Groups*** page ***Endpoint Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Select the endpoints on which you want to define agent version(s).
5. Click **Agent Versions**.

   Step Result: The ***Manage Agent Versions*** dialog opens.

6. Define the agent version(s).
   Use one of the following methods:

Method	Steps
To define a standard agent version for all listed endpoints:	• From the **Select One** list, select an agent version. • Click **Apply to All Agents**.
To define an agent version for each endpoint:	Select an agent version from the **Agent Version** list for each endpoint.

Note: The agent versions available for selections are defined from the ***Options*** page. For additional information, refer to Configuring the Agents Tab on page 89.

7. Click **OK**.

Result: The ***Manage Agent Versions*** dialog closes. If an agent version other than the defined version is installed on the endpoints, the defined version is installed over the previous version.

Deleting Endpoints (Groups Page)

From the ***Groups*** page, you can delete an endpoint from the Ivanti Endpoint Security database.

Prerequisites:

The endpoints you want to delete must be disabled. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 347.

Delete endpoints from the ***Endpoint Membership*** view.

Note: Deleting an endpoint removes its record from the Ivanti Endpoint Security database, but it does not remove the agent on the endpoint.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy that is disabled.

4. Select the endpoint listings you want to delete.

   Tip: You can delete endpoints from any module tab.

5. Click **Delete**.

   Step Result: A confirmation dialog opens.

6. Click **OK** to confirm the deletion.

Result: The selected endpoints are deleted.

Enabling or Disabling Ivanti Endpoint Security Agents within a Group

Disabling an agent deactivates its functionality. Disabled agents do not contact the Ivanti Endpoint Security server, use Ivanti Endpoint Security features, or occupy Ivanti Endpoint Security licenses. Disable an agent if it will be unused for a prolonged period. You can re-enable an agent at any time.

Enable or disbale an agent within a group from the ***Endpoint Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select one of the following tabs:
   - The ***All*** Tab
   - The ***Patch and Remediation*** Tab
4. From the **Browser**, select a group within either the **Custom Groups** or **Systems Groups** hierarchy.
5. If necessary, define filter criteria and click **Update View**.
6. Select the endpoints on which you want to enable or disable the agent:
   Use one of the following methods.

Method	Steps
To enable a disabled endpoint:	Click **Enable**.
To disable an enabled endpoint:	1. Click **Disable**. 2. Acknowledge the disablement by clicking **OK**.

Result: The applicable agents are enabled or disabled. The ***Endpoint Membership*** view and ***Endpoints*** page reflect your changes.

Note: Disabling an agent within a group is not limited to the group; the agent is completely disabled within the Ivanti Endpoint Security.

Enabling or Disabling Endpoint Modules within a Group

From the groups page, you can disable an agent's individual modules. Disable an endpoint's module component if it will be unused for a prolonged period. You can re-enable the endpoint module at any time.

Prerequisites:

Endpoints must have the applicable agent module installed, and the endpoint must be licensed for the agent module. For additional information, refer to Installing Endpoint Modules on page 184.

Enable or disable a module within a group from the ***Endpoint Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Select the tab for the module you want to enable or disable.

   Tip: The tabs available depend on which modules you have purchased and installed.

5. [Optional] Define filter criteria and click **Update View**.
6. Select the check box(es) for endpoint(s) with module components you want to enable or disable.
7. Enable or disable the selected endpoint module(s):
   Use one of the following methods.

Method	Steps
To enable a disabled module component:	Select **Enable** > **Enable Module**.
To disable an enabled endpoint:	1. Select **Enable** > **Enable Module**. 2. Acknowledge the disablement by clicking **OK**.

Result: The applicable endpoint module components are enabled or disabled. The ***Endpoint Membership*** view and ***Endpoints*** page reflect your changes.

Note: Disabling an endpoint module within a group is not limited to the group; the endpoint module is completely disabled within the Ivanti Endpoint Security system.

Managing Endpoint Modules (Groups Page)

You can manage endpoint module licences from the ***Groups*** page. Using this feature allows you control which modules apply to a particular endpoint.

Manage modules for individual endpoints from the ***Groups*** page ***Endpoint Membership*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select one of the following tabs:
   - The ***All*** Tab
   - The ***Patch and Remediation*** Tab
4. Select a group from the directory tree.

   Note: You may select a group that is in either the **Custom Groups** or **Systems Groups** hierarchy.

5. Select the checkbox(es) associated with the endpoints for which you want to manage modules.
6. Click **Manage Modules**.

   Step Result: The ***Add/Remove Modules*** dialog opens.

7. Manage modules for each endpoint.
   - To activate a module for a particular endpoint, select the module check box for the applicable endpoint.
   - To deactivate a module for a particular endpoint, clear the module check box for the applicable endpoint.

   Tip: Select or clear the **Select All** check boxes associated with a module to globally toggle a module for all endpoints.

8. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes. The agent features for each edit are updated during the next Discover Applicable Updates task.

Using Scan Now to Scan Groups

You can initiate a Discover Applicable Updates (DAU) task for all endpoints in a selected group or only selected endpoint within the group. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to Ivanti Endpoint Security, which you can view.

You can launch a DAU task for all endpoints in a selected group or individual endpoints in a selected group. Perform this task from the ***Groups*** page ***Endpoint Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.

2. From the **View** list, select **Endpoint Membership**.
3. Select the ***Patch and Remediation*** tab.
4. From the directory tree, select the group containing endpoints you want to schedule DAU tasks for.
5. Schedule a task for the entire group or individual endpoints.
   Use one of the following methods.

Method	Steps
To schedule a task for an entire group:	1. From the toolbar, click **Scan Now**. 2. Select **Yes, scan all members of the selected** group check box. 3. Select the **Include child groups in the scan** check box. This option schedules tasks for all groups in the selected group's child hierarchy.
To schedule a task for individual endpoints:	1. From the list, select the check boxes associated with the desired endpoint(s). 2. Click **Scan Now**. 3. Select the **Yes, scan the selected endpoint** check box.

Note: When the Patch and Remediation and Application Control modules are both installed, the **Scan Now** button is replaced with a **Scan Now** menu. When this menu is present, select **Scan Now** > **Discover Applicable Updates** from the toolbar to perform a DAU task.

6. Click **Schedule**.
7. Acknowledge the scheduling by clicking **Close**.

Result: The scan is scheduled. As with all deployments, although the Discovery Applicable Updates task is scheduled for immediate execution, it will not actually occur until the next time the agent checks in.

Rebooting Group Endpoints

From the ***Endpoint Membership*** view, you can reboot entire groups or endpoints within a group.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select the ***Patch and Remediation*** tab.
4. From the directory tree, select the group containing endpoints you want to reboot.

5. Reboot the entire group or individual endpoints.
   Use one of the following methods.

Method	Steps
To reboot an entire group	1. Click **Reboot Now**. 2. Select **Yes, reboot all members of the selected group** check box. 3. Select the **Reboot child groups** check box.
To reboot individual endpoints:	1. Select the check boxes associated with the desired endpoint(s). 2. Click **Reboot Now**. 3. Select the ***Yes, reboot the selected endpoint*** check box.

6. Click **Reboot**.
7. Acknowledge the reboot by clicking **Close**.

Result: The reboot is scheduled. As with all deployments, although the reboot is schedule for immediate execution, it will not actually occur until the next time the agent checks in.

Exporting Endpoint Membership View Data

To export information displayed in the ***Endpoint Membership*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Mandatory Baseline View

This view lets you add content to the selected group's Mandatory Baseline. It also lists each content item included in the group's Mandatory Baseline. The list also shows whether or not each endpoint within the group has that content item installed.

Use this view to define the selected group's Mandatory Baseline.

About Mandatory Baselines

A *Mandatory Baseline* is a minimum set of content that *must* be installed on a group's endpoints. Composed of user-defined content items deemed essential to the group, this baseline continually verifies that the applicable items are installed on group endpoints. If a group endpoint is found in a *non-compliant* state (does not have an item defined in the baseline installed), Ivanti Endpoint Security automatically deploys the applicable content until the endpoint is once again compliant. Mandatory Baselines ensure group endpoints are never without essential security content.

For example, you can set a Mandatory Baseline for all endpoints within a group that must have Microsoft Windows Messenger installed. If Messenger is deleted on a group member's endpoint, Ivanti Endpoint Security reinstalls Messenger.

Remember the following rules when working with Mandatory Baselines:

- Mandatory Baseline inheritance indicates that a group's endpoints (both inherited and assigned) are included by the parent group when evaluating its own baseline items and inheritance.
- If endpoints receive a Mandatory Baseline item via inheritance, the Mandatory Baseline item will also be displayed on the child group's ***Mandatory Baseline*** view. However, the inherited baseline items will be unavailable, indicating the Mandatory Baseline originates from a parent group.
- Disabling Mandatory Baseline deployments only applies to the Mandatory Baseline items that are directly assigned to the group, and will prevent those directly assigned items from being inherited by the group's child hierarchy.
- Disabling Mandatory Baseline deployments does not disable the deployments created through Mandatory Baseline inheritance. Additionally, disabling the baseline deployments will not remove the baseline items from the group's ***Mandatory Baseline*** view.

Note: Unless stringent hours of operation agent policies are in effect, do not apply Mandatory Baselines to groups of mission-critical servers or other endpoints where unscheduled reboots would disrupt daily operations.

About Mandatory Baseline Import/Export

Within Ivanti Endpoint Security, you can import or export Mandatory Baselines. Importing and Exporting Mandatory Baselines simplifies application of Baselines to different groups.

After establishing a Mandatory Baseline, you can export the baseline from Ivanti Endpoint Security. After exporting a baseline, you can then import the baseline to a different group or Ivanti Endpoint Security installation.

Ivanti recommends using the Mandatory Baseline import/export feature in the following situations:

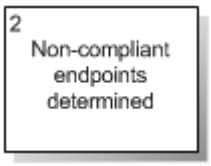
- When reinstalling Ivanti Endpoint Security. Export Mandatory Baselines before beginning reinstallation, and then import Mandatory Baselines to groups after installation. This use of import/export eliminates the manual reestablishment of baselines, easing administrative burden.
- When establishing similar or identical Mandatory Baselines for multiple groups. Rather than manually creating baselines for each group, export a Mandatory Baseline and then import it to other groups. Use this method to quickly establish baselines for multiple groups. After importing a baseline, you can then edit it to suit a group's particular requirements.

The Mandatory Baseline Process

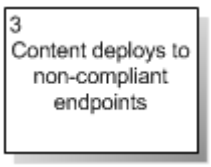
After content items are added to a group's Mandatory Baseline, Ivanti Endpoint Security schedules a series of scans and deployments until the group complies with the baseline.

The following chart depicts the Mandatory Baseline process following the addition of a content item to a baseline.

Ivanti Endpoint Security automatically schedules a Discover Applicable Updates (DAU) task for all endpoints within the applicable group.



Following the DAU, Ivanti Endpoint Security determines which endpoints are not compliant with the Mandatory Baseline.



Necessary content is deployed to non-compliant endpoints as soon as possible.

Note: Some content requires both reboots and an administrator-level log in to complete. If these or similar content items are added to a baseline, the deployment will stop until the log in occurs.

Viewing a Group Mandatory Baseline

Navigate to a group's Mandatory Baseline to see the content items that all its members must have installed.

See the Mandatory Baseline for a selected group from the ***Mandatory Baseline*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. Select the desired group from the directory tree.
3. From the **View** list, select **Mandatory Baseline**.

Result: The Mandatory Baseline associated with the group is displayed.

The Mandatory Baseline View Toolbar

This toolbar contains buttons related to the management of Mandatory Baselines. It also contains a button that lets you cache content items after adding them to the baseline. This caching process ensures swift content installations if an endpoint falls out of compliance.

The following table lists the available toolbar buttons and their functions.

Table 180: Mandatory Baseline View Toolbar

Button	Function
Manage	Adds or removes content to or from the group's Mandatory Baseline. For additional information, refer to either Adding Content to Mandatory Baselines on page 357 or Removing Content from Mandatory Baselines on page 361.
Update Cache	Caches (downloads) the package associated with the selected Mandatory Baseline item(s) (or the scripts associated with downloading the package). For additional information, refer to Updating the Mandatory Baseline Cache on page 366.
Import	Imports an Mandatory Baseline template into the group, defining Mandatory Baseline item. For additional information, refer to Importing Mandatory Baseline Templates on page 366.
Export (menu)	Opens the **Export** menu.
CSV file (**Export** menu item)	Exports the page data to a comma separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47.
Template (*.XML) (**Export** menu item)	Exports the group Mandatory Baseline as a template in `.xml` format. For additional information, refer to Exporting Mandatory Baselines Templates on page 370.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Mandatory Baseline View List

This list displays the content items included in the selected group's Mandatory Baseline. You can also filter this list to display different types of content.

The following table describes the ***Mandatory Baseline*** view list.

Table 181: Mandatory Baseline View List

Column	Icon	Description
Item Type		An icon that indicates the Mandatory Baseline item status and type. For a description of each Mandatory Baseline item icon, refer to Content Status and Type on page 474.
Mandatory Baseline Compliance		An icon that indicates compliance status for the item. For a description of each compliance icon, refer to Mandatory Baseline Item Compliance Icons on page 356. **Note:** If the Mandatory Baseline fails to deploy more than twice, it will be recorded as an error in the **Status** column. However, this notification will only show in the ***Mandatory Baseline*** view.
Mandatory Baseline Item	N/A	The Mandatory Baseline item name. The name doubles as a link the item's ***Review*** page.
Content Type	N/A	The content type of the Mandatory Baseline item. For a description of each impact, refer to one of the following pages based on the applicable type of Mandatory Baseline item: • Vulnerabilities on page 461 • Software Content on page 462 • Other Content on page 462
Vendor	N/A	The name of the vendor that created the software in the Mandatory Baseline item.
State	N/A	The state of the Mandatory Baseline item (`Enabled` or `Disabled`).
OS List	N/A	The operating systems that the Mandatory Baseline item applies to.

Note: The **Mandatory Baseline Item**, **Content Type**, **Vendor**, **State**, and **OS List** are identical to the content items that the Mandatory Baseline items represent.

Each item on the ***Mandatory Baseline*** view list can be expanded to display additional details about the item. This information lists each endpoint in the group, and whether or not these endpoints comply with the expanded Mandatory Baseline item. Click the arrow (**>**) next to a Mandatory Baseline item to view these details.

The following table describes each column within the details of a Mandatory Baseline item.

Table 182: Package Column Definitions

Column	Icon	Description
Endpoint Status Icon		Displays an icon that indicates the current status of the applicable endpoint. For additional information, refer to Agent Module Status Icons on page 168.
Mandatory Baseline Icon		Displays an icon that indicates the status of the endpoint in relation to the expanded Mandatory Baseline item. For additional information, refer to Mandatory Baseline Item Compliance Icons on page 356.
Name	N/A	Indicates the name of the endpoint within the selected group.
OS	N/A	Indicates the operating system that runs on the endpoint.
Compliance	N/A	Indicates whether the endpoint complies with the expanded Mandatory Baseline item. If the item is marked *Do Not Patch* for the endpoint, the endpoint is considered compliant.

Mandatory Baseline Item Compliance Icons

Each item on the ***Mandatory Baseline*** view list contains an icon that indicates if all applicable endpoints within the group have the associated content installed. Familiarizing yourself with these icons will help you understand if the selected group currently complies with its Mandatory Baseline. Additionally, after expanding a Mandatory Baseline items, compliance icons also appear for each endpoint.

The following table describes the compliance icons for Mandatory Baseline items.

Table 183: Mandatory Baseline Item Compliance Icons

Icon	Status
	Indicates one or more group members are either detecting, obtaining the package, awaiting detection, or is in a deployment-not-started state.
	Indicates one or more group members are deploying the package.
	Indicates all group members are disabled.
	Indicates all group members are either not applicable or in compliance with this package (some can also be disabled).
	Indicates one or more group members are not compliant and had an error during deployment. Error information displays in the mouseover text.

Icon	Status
	Indicates that the patch is marked *Do Not Patch* for the group.
	Note: • If a group marked *Do Not Patch* for a content item is later marked *OK to Patch*, the Mandatory Baseline automatically installs the content on that group. • If a group has content added to its Mandatory Baseline that is later marked *Do Not Patch*, that content *is not* automatically uninstalled.

The following table describes the compliance icons for endpoints (which appear when a Mandatory Baseline item is expanded).

Table 184: Endpoint Compliance Icons

Icon	Status
	Indicates the group member is either detecting, obtaining the package, awaiting detection, or is in a deployment-not-started state.
	Indicates the group member is receiving the package.
	Indicates the Mandatory Baseline item does not apply to the group member.
	Indicates the group member complies with the Mandatory Baseline item.
	Indicates the group member does not comply with the Mandatory Baseline item.
	Indicates that group member is marked *Do Not Patch* for the Mandatory Baseline item.
	Note: • If an endpoint marked *Do Not Patch* for a content item is later marked *OK to Patch*, the Mandatory Baseline automatically installs the content on that endpoint. • If an group endpoint has content added to its Mandatory Baseline that is later marked *Do Not Patch*, that content *is not* automatically uninstalled.

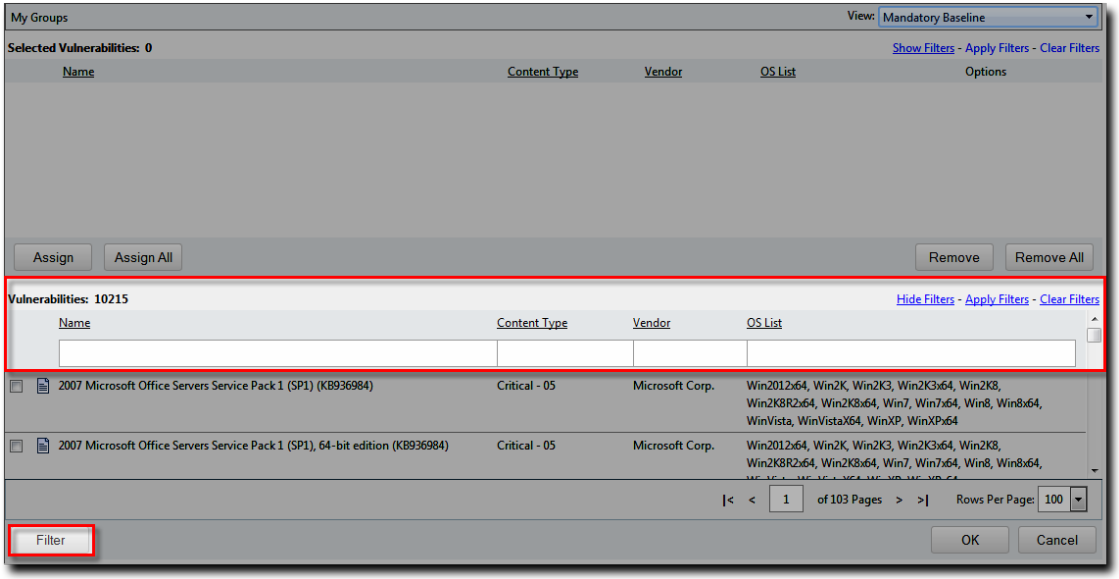
Adding Content to Mandatory Baselines

Add content to a group Mandatory Baseline to monitor the endpoints for installation of the content. If an endpoint does not have it installed, Ivanti Endpoint Security installs it following the next Discover Applicable Updates task.

Add content to a Mandatory Baseline from the ***Mandatory Baseline*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Mandatory Baseline**.

3. From the **Group Browser**, select the desired group.
4. Click **Manage**.
5. [Optional] Filter the **Vulnerabilities** table. There are two ways to filter:
   - Click the **Show/Hide Filters** link to toggle the built-in table filters.
   - Click the **Filter** button at the bottom of the table to open the ***Needed Detection Vulnerabilities*** dialog, which only shows content applicable to the group that hasn't been installed (content that's not applicable or marked *Do Not Patch* for the group aren't displayed).



6. Select the content you want to add to the baseline and click the **Assign** button.

Note:

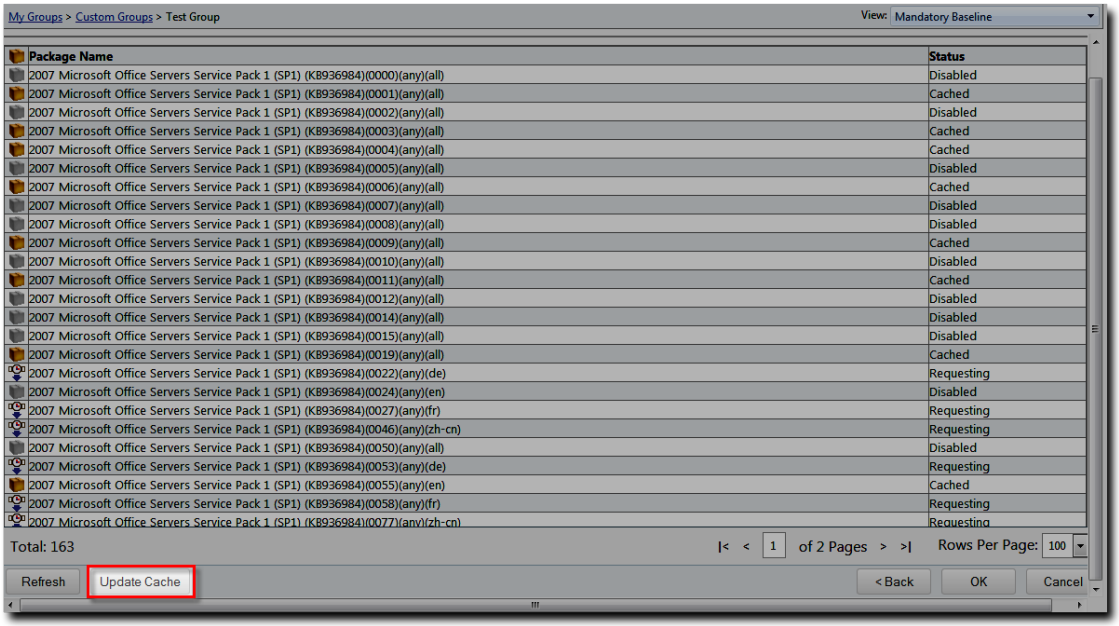
- Don't use the **Assign All** button until you've filtered the **Vulnerabilities** table. Adding all the available content creates excessive network traffic.
- Don't add locally created packages to the baseline. They don't contain the fingerprint files that the baseline requires to monitor for packages.

Step Result: Your content is added to the **Selected Vulnerabilities** table.

7. Click **OK**.
8. If vendor license agreements are displayed, select the **I ACCEPT the terms and conditions of this end user license agreement** option and click **OK**.

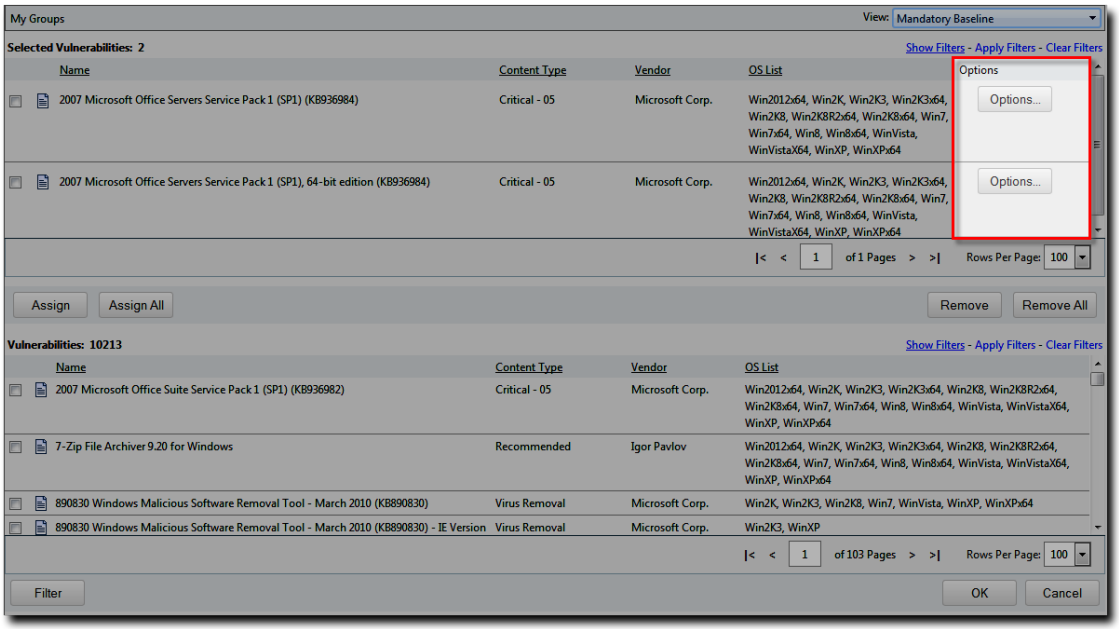
9. [Recommended] Click the **Update Cache** button to download the content.

Note: Skipping the cache update may result in endpoint reboots that interrupt employee work. Cache the content now to optimize package installation order. While caching, click **Refresh** to check for progress.



10. [Optional] From the **Select Vulnerabilities** table, click the **Option** button to set deployment options for a content item.

You can do this for each content item added to the baseline.



11. Click **OK**.

Result: The content is added to the group Mandatory Baseline.

> **Note:** To deploy Mandatory Baseline items, the group **Mandatory Baselines enabled** setting must be set to `True`. For additional information, refer to Editing Group Settings on page 409.

Filtering the Vulnerabilities Table for Applicable Content
When adding content to a Mandatory Baseline, click the filter button to open the ***Needed Detection Vulnerabilities*** dialog. This dialog filters the default the Vulnerabilities table to show only content that applies to the group that hasn't been installed yet.

Prerequisites:

Start Adding Content to Mandatory Baselines on page 357 and complete up to step 5.

1. Click the **Filter** button.

   Step Result: The ***Needed Detection Vulnerabilities*** dialog opens.

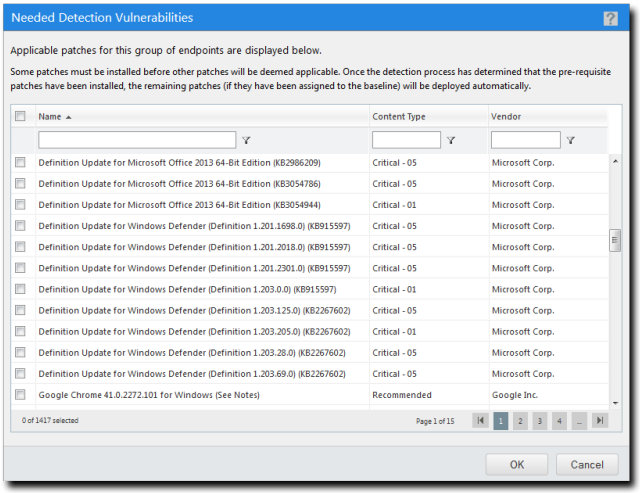


   Figure 72: Needed Detection Vulnerabilities Dialog

2. [Optional] Use the column filters to narrow down content.

   Only applicable content is listed. Content that is not applicable or marked *Do Not Patch* for the group isn't displayed.

3. Select the content items you want to add to the Mandatory Baseline and then click **OK**.

Result: The ***Needed Detection Vulnerabilities*** dialog closes and the selected content items are added to the **Selected Vulnerabilities** table.

Removing Content from Mandatory Baselines

When a group of endpoints no longer requires the constant presence of specific content, remove the applicable content items from that group's Mandatory Baseline. Removing content from a Mandatory Baseline does not remove it from the group's endpoints.

Remove content from Mandatory Baselines from the ***Mandatory Baseline*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Mandatory Baseline**.
3. From the directory tree, select the desired group.
4. Click **Manage**.

5. Remove content from the Mandatory Baseline.
   Use one of the following methods.

Method	Steps
To remove individual content items:	1. From the **Selected Vulnerabilities** table, select the check boxes associated with the content items you want to remove from the Mandatory Baseline. 2. Click **Remove**.
To remove all content items:	Click **Remove All**.

   Step Result: Content items are removed from the **Selected Vulnerabilities** table according to your input.

6. Click **OK**.

Result: The selected content is removed from the selected group's Mandatory Baseline. The ***Groups*** page reflects your changes.

Setting Mandatory Baseline Deployment Options

Like other deployments, automated Mandatory Baseline deployments also have customizable options. After adding content items to a group's Mandatory Baseline, you can set deployment options for each item. Configuring these options defines the manner in which Mandatory Baseline packages are deployed.

Prerequisites:

- A content item must be added to a group Mandatory Baseline.

Configure Mandatory Baseline package deployment options from the ***Mandatory Baseline*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. Select the desired group from the directory tree.
3. From the **View** list, select **Mandatory Baseline**.
4. Click **Manage**.

5. Click the **Options** button associated with the Mandatory Baseline item for which you want to define deployment options.

   Step Result: The ***Package Deployment Options*** dialog opens.

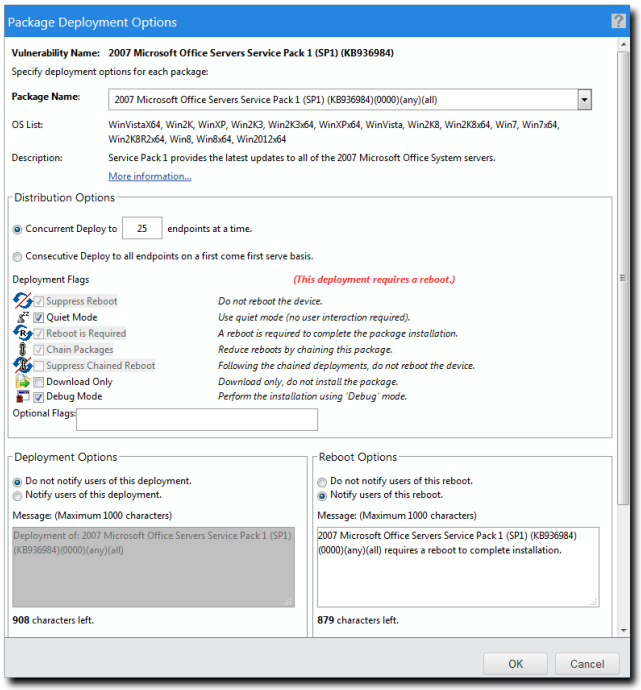


Figure 73: Package Deployment Options Dialog

6. From the **Package Name** list, ensure the desired package is selected.
7. Define **Distribution Options**.
   Choose from the following options.

Option	Steps
To deploy concurrently:	1. Select the **Concurrent** option. 2. In the field, type the desired number of endpoints to receive simultaneous deployments.
To deploy consecutively:	Select the **Consecutive** option.

8. If available, select the desired **Deployment Flags**.
   For additional information, refer to Behavior Icon Definitions on page 280.
9. If needed, type additional deployment flags in the **Optional Flags** field.
   For additional information, refer to Package Flag Descriptions on page 282.

10. Select a **Deployment Option**.

- **Do not notify users of this reboot**.
- **Notify users of this reboot**.

11. If you selected **Notify users of this deployment** option, complete the following substeps.

a) [Optional] Type a notification in the **Message** field.
b) Define the **Deploy within** option.

- To manually define this option, type a value in the field and select a value from the list (***minutes***, ***hours***, ***days***).
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

12. Select a **Reboot Option**.

- **Do not notify users of this reboot**.
- **Notify users of this reboot**.

13. If you selected **Notify users of this reboot** option, complete the following substeps.

a) [Optional] Type a notification in the **Message** field.
b) Define the **Reboot within** option.

- To manually define this option, define the field and list (***minutes***, ***hours***, ***days***).
- To use the default notification option setting defined in the agent policy set associated with the target endpoints, select the **Use Agent Policy** check box.

Result: The ***Package Deployment Options*** dialog closes. Repeat these instructions for additional Mandatory Baseline items if necessary.

Removing Deployments Created by Mandatory Baselines

Occasionally, deployments associated with a Mandatory Baseline may need to be stopped. However, how you stop the deployment will change based on context; in some instances, you may want to stop the deployment for all endpoints within the group; in others, you may only want to stop the deployment for specific endpoints within the group.

Mandatory Baseline deployments can be stopped one of two ways: either stop the deployment itself or disable the endpoints receiving the deployment.

The removal of Mandatory Baseline deployments does not take place within the ***Mandatory Baselines*** view. Rather, it takes place within the ***Deployments and Tasks*** view.

Note: If the Mandatory Baseline still applies, the deployment will be recreated.

Removing a Mandatory Baseline Deployment from a Group
In the event that a Mandatory Baseline deployment needs to be removed for all endpoints within a group, delete the deployment itself. Using this method prevents packages associated with the baseline from being installed on all endpoints within the group.

Stop Mandatory Baseline deployments using this method from the ***Deployments and Tasks*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Deployments and Tasks**.
3. Select the applicable group from the directory tree.
4. Select the check box associated with the Mandatory Baseline deployment you want to delete.
5. Click **Delete**.

   Step Result: A dialog displays, asking you to acknowledge the deletion.
6. Click **OK** to acknowledge the deletion.

Note: If the Mandatory Baseline(s) still applies, the deployment(s) is recreated.

Result: The Mandatory Baseline deployment is stopped. It no longer appears in the ***Deployments and Tasks*** view.

Stopping a Deployment for Specific Endpoints
In the event that a Mandatory Baseline deployment needs to be stopped for specific endpoints within a group, disable those endpoints. Using this method prevents packages associated with the baseline from being installed on specific endpoints within the group rather than all endpoints within the group.

Stop Mandatory Baseline deployments using this method from the ***Deployments and Tasks*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Deployments and Tasks**.
3. Select a group from the directory tree.
4. Click the desired deployment name link.
5. Select the check box(es) associated with the desired endpoint(s).
6. Click **Disable** to disable the deployment(s) for the selected endpoint(s).

Note: If the Mandatory Baseline still applies, the deployment is recreated.

Result: The selected endpoints are disabled, preventing them from receiving the Mandatory Baseline deployment. Remember to re-enable the endpoints to resume vulnerability management activities following management of the Mandatory Baseline.

Updating the Mandatory Baseline Cache

You can cache content that you have included in a group's Mandatory Baseline. Updating the cache for content items downloads the packages (or the scripts that will download the packages) associated with those items. Cached content items can be deployed immediately.

Cache content for Mandatory Baseline items from the ***Mandatory Baseline*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the ***View*** list, select **Mandatory Baseline**.
3. From the directory tree, select the group with Mandatory Baseline items (content items) that you want to cache.
4. If necessary, designate filter criteria for the desired Mandatory Baseline item and click **Update View**.
5. Select the check boxes associated with the Mandatory Baseline item you want to cache.
6. Click **Update Cache**.

Result: The selected content begins caching.

Importing Mandatory Baseline Templates

After a Mandatory Baseline template has been exported, import the template and apply it to a new group. Importing a Mandatory Baseline template is faster than creating a new, identical Mandatory Baseline.

Import Mandatory Baseline templates from the ***Mandatory Baseline*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Mandatory Baseline**.
3. From the directory tree, expand to the group with which you want to import a Mandatory Baseline template.

4. From the toolbar, click **Import**.

   Step Result: The ***Import Mandatory Baseline Wizard*** opens to the ***Welcome to the Import Mandatory Baseline Wizard*** page.

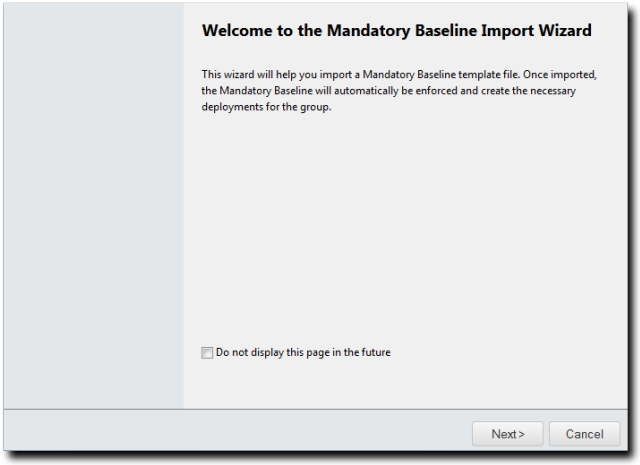


Figure 74: Welcome Page

5. Click **Next**.

   Step Result: The ***Import Mandatory Baseline*** page opens.

6. Define the Mandatory Baseline template that you want to import.

   a) Click **Browse**.

      Step Result: The ***Choose file*** dialog opens.

   b) Browse to the Mandatory Baseline template you want to import.
   c) Click **Open**.

   Step Result: The Mandatory Baseline template name displays in the **Mandatory Baseline template (*.XML)** field.

7. If you do not want to import the deployment options associated with the Mandatory Baseline and use the system defaults defined on your Ivanti Patch and Remediation server, select the **Import without deployment options and use system default** check box.
8. Click **Next**.

9. Based upon the page or dialog that opens, complete the applicable steps.

Page/Dialog	Steps
If the *This group already has Mandatory Baseline items assigned* dialog opens:	1. Select either the **Append to the list of existing items and replace duplicates** option or the **Replace all existing items with new items** 2. Click **OK**.
If the *One or more of the Mandatory Baseline items are not available because they are not included in the server's content subscription* dialog displays:	Click **OK** to proceed with the import or **Cancel** to cancel the import.
If the *Review Mandatory Baseline Items* page opens:	Proceed to the next step.

10. Review the Mandatory Baseline items and edit them as needed.

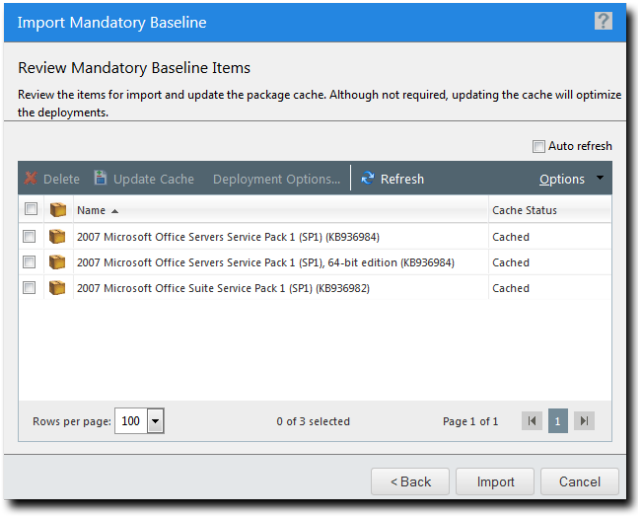


Figure 75: Review Mandatory Baseline Items Page

The following table describes each page column.

Column	Description
Mandatory Baseline Icon	Displays an icon that indicates the cache status of the Mandatory Baseline item. For additional information, refer to Content Icons and Descriptions on page 475.

Column	Description
Name	Lists the name of the Mandatory Baseline item. The Mandatory Baseline item name is identical to the content item.
Cache Status	The cache status of the Mandatory Baseline item. The cache status indicates whether the content item has been downloaded to your Ivanti Patch and Remediation server (`Cached` or `Not Cached`).

11. [Optional] Edit the list.

Edit the list according to the following task steps.

Task	Steps
To delete items:	**1.** Select the check box(es) associated with the applicable Mandatory Baseline item(s). **2.** Click **Delete**.
To update the cache for items:	**Important:** Updating the cache for Mandatory Baseline items ensures they are deployed in the proper chain sequence. Failure to cache Mandatory Baseline items may result in multiple deployment recipient endpoint reboots. **1.** Select the check box(es) associated with the applicable Mandatory Baseline item(s). **2.** Click **Update Cache**.
To configure deployment options for an item:	**1.** Select the check box associated with the applicable Mandatory Baseline item. **2.** Click **Deployment Options**. **3.** Complete Setting Mandatory Baseline Deployment Options on page 362 from step 6.
To refresh item cache statuses:	Click **Refresh**. **Tip:** If the **Auto Refresh** check box is selected, Mandatory Baseline item cache statuses will periodically refresh automatically.

12. Click **Next**.

Step Result: The ***License Agreement*** page opens.

13. Review the license agreement for each mandatory basline item and select **I ACCEPT the terms and condition of the end user license agreement** option.

    Scrolling may be necessary to review and accept all license agreements.

14. Click **Finish**.

    Step Result: The import process begins. A bar indicates progress.

15. Click **Close**

Result: The Mandatory Baseline is imported to the selected group. List items for applicable Mandatory Baseline items appear within the ***Mandatory Baseline*** view. All endpoints within the group are now subject to the Mandatory Baseline.

Exporting Mandatory Baselines Templates

You can export Mandatory Baseline templates in an XML format. This feature is useful for setting up Mandatory Baselines across multiple groups and Ivanti Endpoint Securitys via importation.

Export Mandatory Baselines templates from the ***Mandatory Baseline*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Mandatory Baseline**.

   Step Result: The ***Mandatory Baseline*** view displays.

3. From the directory tree, select the group assigned the Mandatory Baseline you want to export.

   Expand the tree as necessary.
4. From the toolbar, select **Export** > **Template (*.XML)**.

   Step Result: The ***File Download*** dialog opens.

   Note: If using Mozilla Firefox, the procedure to export the Mandatory Baseline will differ slightly.

5. Click **Save**.

   Step Result: The ***Save As*** dialog opens.

6. Define the filepath where you want to save the Mandatory Baseline.
7. [Optional] Edit the **File name** field.
8. Click **Save**.
9. If you want to export Mandatory Baselines for additional groups, repeat the Mandatory Baseline exportation process from step 4.

Result: Your Mandatory Baseline(s) are exported.

Exporting Mandatory Baseline View Data

To export information displayed in the ***Mandatory Baseline*** view list to a comma separated value (`.csv`) file, select **Export** > **CSV File** from the toolbar. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Vulnerabilities/Patch Content View

The ***Groups*** page view contains identical functionality to ***Patch Content*** page, but from this view, you can apply patch content to the endpoint groups you have created. Unlike the ***Patch Content*** page, this view will display only patch content applicable to the selected group.

The Patch Content Broswer

When working within the ***Patch Content*** view, you can browse through content using the **Patch Content Browser**.

For more information, see The Patch Content Browser on page 466.

The Vulnerabilities/Patch Content View Toolbar

This toolbar contains buttons related to the management of content. You can also launch deployments using this toolbar.

The following table describes the ***Vulnerabilities/Patch Content*** view toolbar functions.

Table 185: Vulnerabilities/Patch Content View Toolbar

Button	Function
Enable	Enables the selected disabled content item(s). For additional information, refer to Enabling Content within a Group on page 376. **Note:** This button is only available when a disabled item is selected.
Disable	Disables the selected enabled content item(s). For additional information, refer to Disabling Content Globally on page 479. **Note:** This button is only available when a enabled item is selected.
Do Not Patch...	Disables the selected patch for specific groups and endpoint that you select. For more information, see Disabling Content for Groups/Endpoints on page 480.
Add to List...	Adds content selected from the page list to a Custom Patch List. For additional information, refer to Adding Content to a Custom Patch List on page 485.
Remove	Removes content selected from a Custom Patch List. For additional information, refer to Removing Content from a Custom Patch List on page 487.

Button	Function
Update Cache	Caches (downloads or re-downloads) the package associated with the selected content item(s) (or the scripts associated with downloading the package(s). For additional information, refer to Updating the Cache on page 485.
Deploy...	Deploys selected content. For additional information, refer to Deploying Selected Content (Vulnerabilities View) on page 377.
Scan Now (Menu)	Opens the **Scan Now** menu.
Discover Applicable Updates... (**Scan Now** Menu Item)	Prompts the Discover Applicable Updates task to immediately check the endpoints (Patch and Remediation only). For additional information, refer to Using Scan Now (Endpoint Details Page) on page 226.
Virus and Malware Scan... (**Scan Now** Menu Item)	Prompts Ivanti Endpoint Security to immediately scan endpoints for virus and malware. For additional information, refer to Using the Virus and Malware Scan Wizard.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Add to Mandatory Baseline	Adds patches you select from the grid to a group's Mandatory Baseline
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Vulnerabiliites/Patch Content View List

This list displays content that applies to the selected group. You can also filter this list to display specific content items. Additionally, each item lists identification information and endpoint statistics.

Note: You can filter the list by using Patch Content filters.

Table 186: Column Definitions

Column	Icon	Definition
Status		The content item status, which indicates when the server downloaded the content item metadata. For additional information, refer to Content Status and Type on page 474.
Package Status		The cache status for the content item, which indicates if the server downloaded the content item packages. For additional information, refer to Content Icons and Descriptions on page 475.
Name	N/A	The content item name, which links to the ***Patch Status*** of the item. For additional information, refer to The Patch Status Page on page 489.
Content Type	N/A	Indicates the content item type. For more information, see one of the following topics: • Vulnerabilities on page 461 • Software Content on page 462 • Other Content on page 462
Vendor	N/A	The name of the vendor that created the software in the content item.
Vendor Release Date	N/A	The date and time that the vendor released the software in the content item.
Number of endpoints which came up Patched		The number of endpoints patched with the content item.
Number of endpoints which came up Not Patched		The number of endpoints not patched with the content item.
Total Applicable		The number of endpoints that the content item applies to.
Number of endpoints which came up Do Not Patch		The number of endpoints that administrators have created a patch exception for.

Column	Icon	Definition
Percent Patched	%	The the percentage of applicable endpoints patched with the content item.

Additionally, you can expand each content item by clicking its arrow (**>**). The following table describes each field that displays when you expand a content item.

The following detail information appears on this page.

Table 187: Content Item Field Descriptions

Name	Description
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Associated packages	The number of packages associated with the content item.
Packages status	The cache status for the content item packages.
Ivanti Endpoint Security ID	The Ivanti Endpoint Security identifier for the content item.
Custom Patch Lists	A listing of all Custom Patch Lists that the content item is included in.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The Ivanti Endpoint Security user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/time (UTC)	The date and time the vendor released the software in the content item.
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.

Name	Description
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

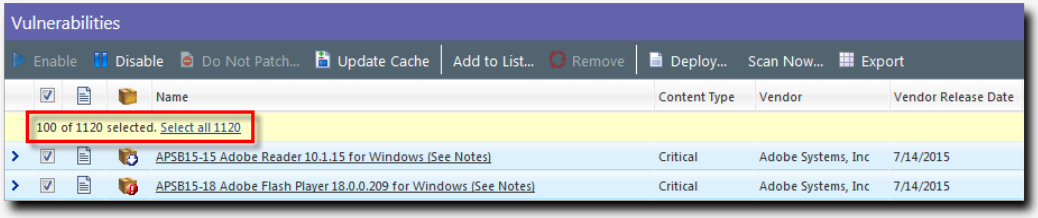
Disabling Content within a Group

You can disable content items from the ***Groups*** page as well as the content pages. Disabled content moves to the bottom of the list and is noted with a disabled status icon. Disable content to prevent it from being deployed.

Note: Disabling content within the ***Vulnerabilities*** view also disables it on all content pages.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Vulnerabilities**.
3. Select a group from the **Group Browser**.
4. If necessary, define filter criteria and click **Update View**.
5. Select one or more content items that you want to disable.

Note: If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.



6. Click **Disable**.

Note: If you disable a content item that's already been cached, the package will not be updated if a new version of the content item is released.

Result: The selected content is disabled.

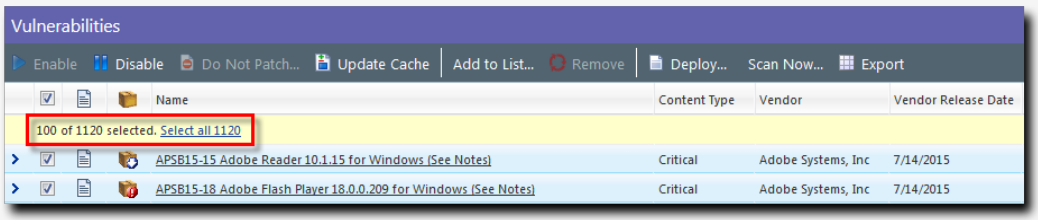
Enabling Content within a Group

After disabling a content item, re-enable it for deployment availability. You can re-enable content from the ***Vulnerability*** view regardless of where it was disabled. Enabled content is noted with an enabled status icon.

Note: Re-enabling a content item from the ***Vulnerabilities*** also re-enables it on all content pages.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Vulnerabilities**.
3. Select a group from the **Group Browser**.
4. If necessary, define filter criteria and click **Update View**.
5. Select the disabled content items you want to enable.

Note: If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.



6. Click **Enable**.

Result: The selected content is re-enabled.

Updating the Groups Cache

From the ***Vulnerabilities*** view, you can update the cache for selected content items. Updating the cache for content items downloads the packages (or the scripts that will download the packages) associated with those items so you can deploy them immediately.

You can update the cache for content from the ***Vulnerabilities*** view, not just other content pages.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Vulnerabilities**.
3. From the directory tree, select the group with applicable vulnerabilities that you want to cache.
4. If necessary, designate filter criteria for the desired content and click **Update View**.
5. Select the check boxes associated with the content you want to cache.

6. Click **Update Cache**.

   Step Result: The ***Warning*** dialog opens, informing you that the update request and this action may take an extended period of time.

   Note: The cache will not be updated for disabled content items that have had a new version released.

7. Click **OK**.

Result: The selected content begins caching.

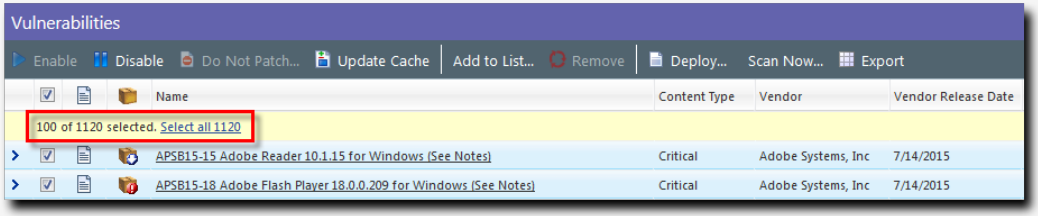
Deploying Selected Content (Vulnerabilities View)

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including the ***Groups*** page ***Vulnerabilities*** view. When deploying from this page, the ***Deployment Wizard*** is preconfigured to deploy your selected content to the selected group.

For additional information, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Vulnerabilities**.
3. From the **Group Browser**, select the group you want to deploy content to.
4. Select the content you want to deploy.

   Note: If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.



5. Click **Deploy**.

Result: The ***Deployment Wizard*** opens, preconfigured to deploy selected content to the selected group.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Exporting Vulnerability View Data

To export information displayed in the ***Vulnerability*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Inventory View

The ***Inventory*** view displays the software, hardware, services, and operating systems detected on the endpoints in the group. This view is identical to the ***Inventory*** page but only displays the inventory of the selected group.

The Inventory View Toolbar

This toolbar contains only basic options related to data exportation and page viewing. It offers no functionality related to endpoint inventory.

The following table describes buttons available from the ***Inventory*** view toolbar.

Table 188: Inventory View Toolbar

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

Exporting Inventory View Data

To export information displayed in the ***Inventory*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Deployments and Tasks View

The ***Deployments and Tasks*** view is similar to the ***Deployments and Tasks*** page because it lists pending, active, and completed deployments or tasks. However, unlike the ***Deployments and Tasks*** page (which lists all deployments), this view only lists the deployments that apply to the selected group. Additionally, you can use this view to manage and create deployments.

Note: This view does not display the deployments and tasks for each member; only the group's assigned deployments.

The Deployments and Tasks View Toolbar

This toolbar contains buttons that offer functionality related to the management and creation of deployments. Selection of list items associated with deployments may be necessary to use some buttons.

The following table describes the ***Deployments and Tasks*** view toolbar.

Table 189: Deployments and Tasks View Toolbar

Button	Function
Enable	Enables the selected disabled deployment or task. For additional information, refer to Enabling Group Deployments on page 381.
Disable	Disables the selected enabled deployment or tasks. For additional information, refer to Deleting Group Deployments on page 382.
Abort	Cancels the selected deployment or tasks for any endpoints that are yet to receive the deployment. For additional information, refer to Aborting Group Deployments on page 381.
Delete	Removes the deployment or tasks from Ivanti Patch and Remediation. For additional information, refer to Deleting Group Deployments on page 382.
Deploy...	Deploys the selected packages. For additional information, refer to Deploying Content (Deployments and Tasks View) on page 382.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Deployments and Tasks View List

This list itemizes all deployments and deployment details applicable to the selected group.

View the ***Deployments and Tasks View*** list from the ***Groups*** page. The following table describes each ***Deployments and Tasks View*** list columns.

Table 190: Deployment and Tasks View List

Column	Icon	Description
Name	N/A	The name of the deployment.
Scheduled Date	N/A	The date and time the deployment was created.
Number of Successful Endpoints		The total number of endpoints and groups that finished the deployment successfully.
Number of Failed Endpoints		The total number of endpoints and groups that finished the deployment unsuccessfully.
Number of Endpoints Assigned to the Deployment		The total number of endpoints and groups that are assigned to the deployment.
Number of In Progress Endpoints		The total number of endpoints and groups that are receiving the deployment. **Note:** If you deploy to a group using Agent Local Time, the deployment remains in progress until all time zones have passed. This behavior ensures any endpoints added to the group following deployment start also receive content. This behavior does not occur when using Agent UTC Time.
Total Not Deployed		The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, or marked *Do Not Patch*).
Number of Endpoints That Have Completed the Deployment		The total number of endpoints and groups that finished the deployment.
The Percentage of Completed Endpoints		The percentage of endpoints and groups that finished the deployment. Percentage = [Total Finished endpoints / Total Assigned endpoints]

Enabling Group Deployments

Within Ivanti Patch and Remediation, you can re-enable paused, group-specific deployments from the ***Deployments and Tasks*** view.

Enable group deployments from the ***Deployments and Tasks*** view, *not* the ***Deployments and Tasks*** page.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Deployments and Tasks**.
3. From the directory tree, select the group containing the deployment you want to enable.
4. Select the select the check box associated with the disabled deployment you want to enable.
5. Click **Enable**.

Result: The selected deployment is enabled.

Disabling Group Deployments

Within Ivanti Endpoint Security, you can pause group-specific deployments from the ***Deployments and Tasks*** view.

Disable group deployments from the ***Deployments and Tasks*** view, *not* the ***Deployments and Tasks*** page.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Deployments and Tasks**.
3. From the directory tree, select the group containing the deployment you to disable.
4. Select the deployment you want to disable.
5. Click **Disable**.

Result: The selected deployment is disabled.

Aborting Group Deployments

Within Ivanti Endpoint Security, you can abort group-specific deployments from the ***Deployments and Tasks*** view.

Abort group deployments from the ***Deployments and Tasks*** view, *not* the ***Deployments and Tasks*** page.

Note: The endpoints that have already received the deployment will not be affected. Only the endpoints that have not yet received the deployment will have the deployment aborted.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Deployments and Tasks**.
3. From the directory tree, select the group containing the deployment you want to abort.

4. Select the check box associated with the deployment you want to abort.
5. Click **Abort**.

Result: The selected deployment is aborted.

Note: You cannot abort system tasks or Mandatory Baseline deployments.

Deleting Group Deployments

Within Ivanti Endpoint Security, you can delete group-specific deployments from the ***Deployments and Tasks*** view.

Delete group deployments from the ***Deployments and Tasks*** view, *not* the ***Deployments and Tasks*** page.

Note: Deleting a deployment will have no effect on endpoints that have already received the deployment. You cannot delete system task deployments.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Deployments and Tasks**.
3. From the directory tree, select the group containing the deployment you want to delete.
4. Select the check box associated with the deployment you want to delete.
5. Click **Delete**.

Result: The selected deployment is deleted.

Deploying Content (Deployments and Tasks View)

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including the ***Groups*** page ***Deployments and Tasks*** view.

For additional information, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Deployments and Tasks**.
3. From the directory tree, select the group deploy content to.
4. Click **Deploy**.

Result: The ***Deployment Wizard*** opens.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Adding Content to a Mandatory Baseline from the Vulnerabilities/Patch Content View

You can add content from a Custom Patch List or any of the other view options.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Vulnerabilities/Patch Content**.
3. From the **Group Browser**, select the desired group.
4. [Optional] From the ***Patch Content Browser***, select a **Custom Patch List** (recommended) or any of the view options.

   Tip: A Custom Patch List is an object that you can add patches to and then deploy to your endpoints. These lists are a great way to keep a history of patches you've deployed each Patch Tuesday.

   While creating a Custom Patch List, understand the applicability and impact of deploying these patches to your environment, especially critical machines. When making this assessment, consider:

   - Threat Level
   - Known Active Exploits in the Wild
   - Risk of Compromise
   - Consequences of Compromise

   For more information, see Creating Custom Patch Lists on page 476 and Adding Content to a Custom Patch List on page 485
5. [Optional] If necessary, designate filter criteria for the desired content and click **Update View**.
6. Select the content you want to add to the baseline.
7. Click **Add to Mandatory Baseline**.

   Step Result: Your content is added to the Group's Mandatory Baseline. A window appears withd details on the number of new items added and which were existing.
8. [Optional] Click **Set Options** to set the individual deploment options for items selected from the Mandatory Baseline view. For additional information, refer to Setting Mandatory Baseline Deployment Options on page 362.

Result: The content is added to the group Mandatory Baseline.

Exporting Deployments View Data

To export information displayed in the ***Deployments and Tasks*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Agent Policy Sets View

After creating agent policy sets, you can apply them to a group using the ***Agent Policy Sets*** view. From this view you can add or remove existing agent policy sets to or from the selected group. Additionally, you can create policy sets from this view. However, this view, unlike the ***Agent Policy Sets*** page, does not let you edit policy sets or view their details. This view is only applicable to agent policy sets.

For additional information about agent policy sets, refer to About Agent Policies and Agent Policy Sets on page 415.

The Agent Policy Sets View Toolbar

This toolbar allows you to manage Agent Policy Sets for groups.

Table 191: Agent Policy Sets View Toolbar

Button	Function
Assign	Assigns an Agent Policy Set to the selected group and its child groups. For additional information, refer to Assigning an Agent Policy Set to a Group on page 385.
Unassign	Unassigns an Agent Policy Set to the selected group and its child groups. For additional information, refer to Unassigning an Agent Policy Set from a Group on page 386.
Create...	Creates an Agent Policy Set. For additional information, refer to Creating an Agent Policy Set (Groups Page) on page 387.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Agent Policy Sets View List

This list itemizes all agent policy sets and policy details assigned to the selected group.

View the ***Agent Policy Sets View*** list from the ***Groups*** page. The following table describes ***Agent Policy Sets View*** list.

Column	Description
Action	The **Unassign** icon indicates the Agent Policy Set may be unassigned. **Note:** You may use the **Unassign** icon to remove a policy set from the selected group. For additional information, refer to Unassigning an Agent Policy Set from a Group on page 386. The **Unassign Disabled** icon indicates the Agent Policy Set cannot be unassigned. **Note:** The **Unassign Disabled** icon indicates the policy is inherited. An inherited Agent Policy Set can not be unassigned from the group.
Name	The name of the Agent Policy Set. **Note:** You may select the **Name** column to sort the Agent Policy Set list.

Assigning an Agent Policy Set to a Group

Assigning an Agent Policy Set to a group defines functional rules for the group.

Prerequisites:

Create an Agent Policy Set. Refer to Creating an Agent Policy Set (Groups Page) on page 387 for details.

Assign Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 415 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Assign**.

   Step Result: The **Select a Policy Set** list becomes active.

5. Select an agent policy set from the **Select a Policy Set** list.

6. Click the **Save** icon ( ) to save your changes.

   Step Result: The **Select a Policy Set** list closes and your policy is assigned.

   Note: The **Cancel** icon ( ) cancels your changes and any edits are not saved.

Result: The policy set is saved and associated with the group.

Unassigning an Agent Policy Set from a Group

When desired, you can unassign an Agent Policy Set from a group.

Prerequisites:

An Agent Policy Set is assigned. Refer to Assigning an Agent Policy Set to a Group on page 385 for details.

Unassign the Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 415 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Remove the desired policy sets.

   Use one of the following methods.

Method	Steps
To remove one Agent Policy Set:	Click the **Unassign** icon ( ) associated with the Agent Policy Set you want to remove.
To remove multiple Agent Policy Sets:	1. Select the check boxes associated with the Agent Policy Sets you want to remove. 2. From the toolbar, click the **Unassign** button.

Note: An **Unassign Disabled** icon indicates you cannot remove an inherited Agent Policy Set. Instead, you must change the group policy inheritance setting or remove the inherited policy set from the parent group. Refer to *Policy Inheritance* in Editing Group Settings on page 409 for additional information.

Step Result: A dialog appears, prompting you to acknowledge the removal.

5. Click **OK**.

   Step Result: The selected policy set(s) are removed and the dialog closes.

Result: The Agent Policy Set(s) are no longer associated with the group.

Creating an Agent Policy Set (Groups Page)

You can create agent policy sets from the ***Agent Policy Set*** view. Agent policy sets are collections of values that can be assigned to groups to regulate how agents behave.

Note: When creating an agent policy set from the ***Agent Policy Set*** view, the created policy set will be immediately applied to the group selected in the directory tree.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Set**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Create**.

   Step Result: The ***Create Agent Policy Set*** dialog opens.

5. Type the applicable information in the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

6. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 417.

Option	Description
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.

7. Define the **Agent Logging** options.
   The following table describes each option.

Option	Step
Logging level (button)	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 446.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

8. Define the **Ivanti Endpoint Security Agent Communication** options.
   The following table describes each option.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *True*.
Send interval (list)	Select the amount of time that the agent should wait before sending an event to the Ivanti Endpoint Security server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval (field and list)	Type and select the amount of time that the agent should delay before reattaching events from the Ivanti Endpoint Security Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.
Timeout interval (field and list)	Type and select the amount of time the agent should stay attached to the Ivanti Endpoint Security server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval (field and list)	Type and select the amount of time between agent check-ins with the Ivanti Endpoint Security server (1 minute-1 day). A value of *15 minutes* is the default setting.

9. Define the **Ivanti Endpoint Security Agent Notification Defaults** options.
   The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the ***Agent Control Panel*** (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**). **Note:** • This policy will not take effect until the agent is restarted. • This policy can hide only the Ivanti Endpoint Security Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***. • This policy cannot hide the Patch Agent or the Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the ***Agent Control Panel*** are hidden or accessible to an endpoint user after logging on (**True** or **False**).

10. Define the **Reboot Behavior Defaults** option.
    An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.
    a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.
Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

11. Define the **Patch Agent Communication** options.

The following table describes each option.

Option	Step
Use SSL for agent to server communication (list)	Select whether the Patch Agent uses HTTPS when communicating with the Ivanti Endpoint Security server.
Use HTTP for package download (list)	Select whether files are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *False*.
Agent Listener Port (field)	Select the agent listener port number. When the agent is contacted using this port, it responds with the agent version number and initiates communication with Ivanti Endpoint Security. The default value of *0* disables the agent listener.
Agent Scan Mode (list)	Select the mode that the Discover Applicable Updates (DAU) task runs in. These modes include: **Normal** — Performs the DAU task normally, which uses the least amount of resources. **Initial Only** — Performs the first DAU task in fast mode, but subsequent DAU tasks in normal mode. **Fast Scan** — Performs the DAU task faster, but uses more resources. The default value is *Normal*.
Communication Interval (field and list)	Type and select the interval (in minutes, hours, or days) between agent and Ivanti Endpoint Security communication (1 minute-1 day). The default value is *15 minutes*.
Inventory Collection Options (button)	Click to open the ***Select Inventory Collection*** dialog. Use this dialog to select the inventory values for recording during agent scanning. For additional information, refer to Defining Inventory Collection Options on page 448.
Resume Interrupted Downloads (list)	Select whether the agent resumes interrupted downloads at the point of interruption (*True* or *False*). The default value is *True*.

Option	Step
Hours of Operation (button)	Click to open the ***Edit Agent Hours of Operation*** dialog. Hours of operation are based on agent local time, allowing for further definition of the agent start and end times. For additional information, refer to Defining Agent Hours of Operation on page 450.

12.[Optional] Define the **Configuration Policies** option according to context.

Context	Step
If defining this option for the first time:	Click the **Define** button adjacent to **Security Configuration management**.
If editing this option after it has been defined:	Click the **Modify** button adjacent to **Security Configuration management**.

Step Result: The ***Configuration Policy Management*** dialog opens. For more information regarding defining configuration policies, see Uploading and Applying a Benchmark to a New Agent Policy Set.

13. Define the **Ivanti Patch and Remediation Deployment Notification Defaults** options.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the deployment (**True** or **False**). The default value is **False**.
User May Snooze (list)	Select whether the deployment recipient can snooze the deployment (**True** or **False**). The default value is **True**.
Deploy Within (field)	Select the default time (in minutes) between the creation of the deployment and the deployment deadline (1-1440). The default value is **5 minutes**.
Always On Top (list)	Select whether deployment notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 286.

14. Define the **Ivanti Patch and Remediation Reboot Notification Defaults**.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the reboot (**True** or **False**). The default value is *True*.
User May Snooze (list)	Select whether the deployment recipient can snooze the reboot (**True** or **False**). The default value is *True*.
Reboot Within (field)	Type the default time (in minutes) between the creation of the deployment and the reboot deadline (1-1440). The default value is **5 minutes**.
Always on Top (list)	Select whether reboot notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 286.

15. Define the **Discover Applicable Updates (DAU)** option.

Option	Step
Scheduling Frequency (field)	Type the frequency (in hours) of the DAU task (1-8760). The default value is *26 hours*.

16. Define the **FastPath Servers** options.

For additional information, refer to About FastPath on page 453.

Option	Step
Interval (field and list)	Type the time interval (in minutes, hours, or days) between FastPath server validations (0 minutes-7 days). The default value of *0* disables the option.
Servers (button)	Click **Define** to open the ***Edit FastPath Servers*** dialog. Use this dialog to add FastPath servers. For additional information, refer to Adding/Editing FastPath Servers on page 453.

17. Define the **Bandwidth Throttling** options.

Option	Step
Maximum Transfer Rate (field)	Type the maximum amount of network bandwidth (in kilobytes per second), per endpoint that can be used by the agent for content download (0-1024). The default value of *0* disables bandwidth throttling.
Minimum File Size (field)	Type the threshold (in KB) at which a file will be managed by bandwidth throttling (0-1024). Files smaller than the defined value will not be managed by bandwidth throttling. The default value is *100*.

18. Define the **Power Management** options (Ivanti Power Management only).

For additional information, refer to Power Management Policies.

19. Define the **Device Control** options .

Option	Description
DC install SK-NDIS driver (list)	Indicates whether Ivanti Endpoint Security installs a SK-NDIS on endpoints assigned the policy (**Do not install** or **Install Enabled**).
DC detection interval (field)	Indicates the detection interval (in minutes) that determines how often the endpoint verifies installation.
DC device event upload interval (field)	Indicates the reporting interval (in minutes) that determines how other the endpoint reports device events back to the server.
DC agent reboot behavior (Read-only text)	Indicates how reboots are performed following installation of the Device Control endpoint module. This behavior is defined using the **Reboot behavior** option. For additional information, refer to 8 on page 432.

20. Define the **AntiVirus** option:

Option	Description
Delay AV definition distribution by (field)	Type the time interval (in hours, up to 23 hours) that the Ivanti Endpoint Security Agent is to delay requesting a new AntiVirus definitions file from the Application Server. The default value of *0* hours disables the option. Use this option to make time to test a new definitions file in a test environment before distributing it to agents (for example, to check for false positives that can negatively affect system functionality). **Important:** Delaying the download of important updates can make your environment vulnerable to new viruses or malware.

21. Click **Save**.

Result: Your agent policy set is saved and assigned to the selected group. You can also assign the agent policy set to other endpoint groups or edit the set.

Exporting Agent Policy Sets View Data

To export information displayed in the ***Agent Policy Sets*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Antivirus Policies View

The ***Antivirus Policies*** view on the ***Groups*** page provides a centralized view of the antivirus policies assigned to a selected group. Resultant Policies are compiled by combining the criteria of policies listed.

Antivirus Policies View Toolbar

The ***Antivirus Policies*** view toolbar on the ***Groups*** page enables you to create, edit, and manage group antivirus policies.

Table 192: Antivirus Policies Toolbar Buttons

Button	Function
Create	Enables you to create a *Recurring Virus and Malware Scan* policy or a *Real-time Monitoring Policy*.
Assign	Assigns the selected policy to one or more endpoints or groups.

Button	Function
Un-assign	Un-assigns the selected policy from one or more endpoints or groups.
Export	Exports the selected policy to a comma separated value (`.csv`) file. See Exporting Data on page 47 for more information.
Options	Features options to set page views, filter data, and enable clipboard copy. See The Options Menu on page 39 for more information.

Antivirus Policies View List

The ***Antivirus Policies*** view list on the ***Groups*** page provides information on existing group antivirus policies.

Table 193: Antivirus Policies List Columns

Column	Description
Select check box	Select this check box to perform an action on the policy.
Action	Actions that can be performed on the selected policy.
Status	An icon representing whether the policy is enabled or disabled.
Policy Name	The name given by the policy creator.
Policy Type	• Recurring Virus and Malware Scan • Real-time Monitoring Policy
Source	• Assigned • Inherited
Assigned Date (Server)	The date in server time when the policy was assigned to the group. For inherited policies, the date/time displayed is when the policy was assigned to the parent group.

The Application Control Policies View

The ***Application Control Policies*** view on the ***Groups*** page provides a centralized view of the application control policies assigned to a selected group. Resultant Policies are compiled by combining the criteria of policies listed.

Application Control Policies View Toolbar

The ***Application Control Policies*** view toolbar on the ***Groups*** page enables you to create, edit, and manage group application control policies.

Table 194: Application Control Policies Toolbar Buttons

Button	Function
Create	Enables you to create the following policy types: Memory Injection, Trusted Publisher, Trusted Updater, Easy Auditor, Easy Lockdown.
Assign	Assigns the selected policy to one or more endpoints or groups.
Un-assign	Un-assigns the selected policy from one or more endpoints or groups.
Export	Exports the selected policy to a comma separated value (`.csv`) file. See Exporting Data on page 47 for more information.
Options	Features options to set page views, filter data, and enable clipboard copy. See The Options Menu on page 39 for more information.

Application Control Policies View List

The ***Application Control Policies*** view list on the ***Groups*** page provides information on existing group applicaion control policies.

Table 195: Applicaion Control Policies List Columns

Column	Description
Select check box	Select this check box to perform an action on the policy.
Action	Actions that can be performed on the selected policy.
Status	An icon representing whether the policy is enabled or disabled.

Column	Description
Policy Name	The name given by the policy creator.
Policy Type	• Memory Injection • Trusted Publisher • Trusted Updater • Easy Auditor • Easy Lockdown
Source	• Assigned • Inherited
Assigned Date (Server)	The date in server time when the policy was assigned to the group. For inherited policies, the date/time displayed is when the policy was assigned to the parent group.

The Virus and Malware Event Alerts View

The ***Virus and Malware Event Alerts*** view on the ***Groups*** page provides a centralized view of all alerts generated by virus and malware scans performed on a selected group.

Table 196: Virus and Malware Event Alerts Features

Feature	Function
Filters	Filters list of event alerts.
Toolbar	Manages event alerts and launches ***Virus and Malware Scan Wizard***.
Group By row	Groups the list of event alerts.
Event Alerts list	Lists event alerts generated by virus scans.

The information and features enable you to:

Review current status	You can see the types of malware that have been detected and the endpoints that have been infected. This information will help you to determine how the infection originated and the best way to handle it.
Take remedial action	You can use Scan Now to launch the ***Virus and Malware Scan Wizard***, configuring it to perform specific actions that will reduce the threat to the network. See Using the Virus and Malware Scan Wizard for more information.

Virus and Malware Event Alerts View Toolbar

The ***Virus and Malware Event Alerts*** toolbar on the ***Groups*** page enables you to perform functions on the group event alerts listed, and run an on-demand scan.

Table 197: Virus and Malware Event Alerts Toolbar

Button	Function
Scan Now	Opens the ***Virus and Malware Scan Wizard***. This enables an administrator to react to incoming alerts with an immediate scan. When configured appropriately, this scan can eliminate the problem by cleaning or deleting the infected files. For more information on running these scans, see Using the Virus and Malware Scan Wizard.
Remove	Removes the selected event alert(s) from the list.
Export	Exports the event alerts list to a comma separated value (`.csv`) file.

Note: Only event alerts from the previous 90 days are displayed. If there are a large number of event alerts and you no longer need to view all of them, you can use the **Remove** button to remove unwanted alerts from the list. This does not delete them from the database, however, so you can always view these removed alerts by generating an appropriate report.

Virus and Malware Event Alerts View List

The ***Virus and Malware Event Alerts*** view on the ***Groups*** page provides a comprehensive and constantly updated list of all event alerts generated by virus and malware scans performed on a selected group.

Table 198: Virus and Malware Event Alerts List

Column	Description
Virus/Malware Name	The name of the virus or malware detected. Each example links to the relevant entry in the ***Virus/Malware Details*** page.
Endpoint Name	The name of the endpoint where the virus or malware was detected. **Note:** Each example links to the relevant entry in the endpoint's ***Details*** page.
IP Address	The IP address of the endpoint where the virus or malware was detected.
Alert Source	The type of scan that generated the alert: • Real-time Monitoring Policy • Recurring Virus and Malware Scan • Scan Now

Column	Description
Status	The alert status: •  (Cleaned) •  (Deleted) •  (Not Cleaned) •  (Quarantined) **Note:** Both the *Cleaned* status and *Deleted* status use the same icon because in both cases the malicious code has been removed and no longer presents a danger.
Alert Message	The message related to the alert status: • Cleaned • Deleted • Not Cleaned • Quarantined
File Name	The name of the file in which the malware was detected.
File Path	The file path of the file in which the malware was detected.
Last Detected Date (Server)	The date and time the alert was generated (server time).

Tip: You can use the **Group By** row, available above the list, to sort list items into groups based on column headers. This feature (along with the filters above the toolbar) is useful when you need to examine a large number of event alerts.

The Device Control Policies View

This view displays the Device Control policies assigned to the selected group. It also contains controls you can use to assign additional policies to the group.

The Device Control View Tab Toolbar

The ***Device Control Policies*** view toolbar contains buttons you can use to create and manage Device Control policies for the selected endpoint.

The following table describes each toolbar button.

Table 199: Device Control Policies View Toolbar

Button	Description
Create	Displays a drop-down menu that allows you to select the type of policy to create. **Note:** A user should have **Manage Centralized DC Policies** access rights to access this functionality.
Assign	Opens the ***Assigned Users and Endpoints*** dialog for the selected policy. **Note:** This button is enabled only if the user has **Assign Centralized DC Policies** access rights and a policy is selected from the list.
Unassign	Allows you to unassign the selected policy. **Note:** This button is enabled only if the user has **Assign Centralized DC Policies** access rights and an assigned policy is selected from the list.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Device Control Policies View List

The ***Device Control Policies*** tab contains a listing of Device Control policies assigned to the endpoint.

The following table describes each list column.

Table 200: Device Control Policies View List

Column	Description
Status	The enabled or disabled status of the policy.
Policy Name	The name of the policy.

Column	Description
Assigned	The assigned or unassigned status of the policy.
Device Class	The device class to which the policy applies.
Device Collection	The device collection to which the policy applies.
Source	The policy source.
Last Update (Server)	The date the policy was modified last.

The Compliance Summary View

From this view, you can view policy compliance summary information for a selected group. This view will not display useful information until you apply a security configuration benchmark via an agent policy set.

For more information on this view and its contents, refer to Viewing Group Policy Compliance Summary Information.

The Compliance Detail View

From this view, you can view policy compliance detail information for a selected group. This view will not display useful information until you apply a security configuration benchmark via an agent policy set.

For additional information on this view and its contents, refer to Viewing Group Policy Compliance Detail Information.

The Roles View

This view lists the user roles that can access the selected group. This view is similar to the ***Roles*** page, but applies only to the selected group rather than the entire system. From this view, you can manage which roles have access to the selected group.

The Roles View Toolbar

This toolbar contains buttons that let you add (or remove) roles that can access the selected group. You can also use it to create new user roles.

The following table describes the functionality of each **Roles** view toolbar button.

Table 201: Roles View Toolbar

Button	Function
Add	Adds a role to the group. For additional information, refer to Adding a Role to a Group on page 403.
Remove	Removes a role from the group. For additional information, refer to Removing a Role from a Group on page 403.
Create...	Creates a new user role. For additional information, refer to Creating User Roles (Roles View) on page 404.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Roles View List

This list displays the roles that can access the selected group. Use the **Action** column to remove user roles. Additionally, you can filter this table using the filter row.

The following table describes each **Roles** view list column.

Table 202: Roles View List

Column	Description
Action	Contains a **Remove** icon. Use this icon to remove a role from the associated group.
Status	Contains an icon that indicates the type of role. For additional information, refer to one of the following topics: • Predefined System Roles • Custom Roles

Column	Description
Name	Indicates the name of the user role.
Source Group	Indicates the group from which the role was created.

Adding a Role to a Group

Add a user role to a group to grant it group access. If the selected group's **Policy inheritance** setting is set to **true**, the added user role will also be able to access the selected group's descendant groups.

Add roles to a group from the ***Roles*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.
4. Click **Add**.
5. Select a role from the **Select a Role** list.
   Select from the following roles:
   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

   Note: ***Custom Role(s)*** are only available if a custom role has been created.
6. Click the **Save** icon.

Result: The role is saved and associated with the group.

Removing a Role from a Group

Remove a user role from a group to deny its associated users group access. If the selected group has **policy inheritance** set to **true**, removing a role will remove the role from the selected group's descendant groups as well.

Remove user roles from a group using the ***Roles*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.

4. Remove roles from the group.
   Use one of the following methods.

Method	Steps
To remove a single role:	Click the **Remove** icon associated with the role you want to remove from the group.
To remove multiple roles:	1. Select the check boxes associated with the roles you want to remove from the group. 2. From the toolbar, click **Remove**.

Note: Inherited roles cannot be removed. To remove inherited roles, either edit the group's inheritence policy or remove the roles from the applicable parent group. To understand group policy inheritance and its effects, refer to Defining Agent Policy Inheritance Rules on page 418.

Step Result: A dialog displays, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

Result: The role is removed and is no longer associated with the group.

Creating User Roles (Roles View)

Custom roles let you select individual access rights, accessible groups, and accessible endpoints for that role. Create a custom role when predefined system roles do not contain the access rights needed for a particular user. Creating a custom role is also useful when you require a role that can only access specific groups or endpoints.

You can create roles from the ***Roles*** view as well as the ***Roles*** tab.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Create**.

   Step Result: The ***Create Role*** dialog appears with the ***Information*** tab selected by default.

5. Type a name in the **Name** field.
6. Type a description in the **Description** field.
7. Select a role template from the **Role Template** list.
   Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.

8. Select the ***Access Rights*** tab.
9. Select or clear the desired access rights.
   For additional information, refer to Predefined System Roles.

Tip: Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

10. Select the ***Groups*** tab.
11. Assign the desired accessible endpoint groups to the role.
    Use one of the following methods to assign groups.

Method	Steps
To assign individual groups:	1. From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign. 2. Click **Assign**.
To assign all groups:	Click **Assign All**.

Tip: Remove groups using **Remove** and **Remove All**.

12. Select the ***Endpoints*** tab.
13. Assign the desired accessible endpoints to the role.
    Use one of the following methods to assign endpoints.

Method	Steps
To assign individual endpoints:	1. From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign. 2. Click **Assign**.
To assign all endpoints:	Click **Assign All**.

Tip: Remove endpoints using **Remove** and **Remove All**.

14. Click **OK**.

Result: The new role is saved and assigned to the selected group.

Note: A created role can be edited from the ***Users and Roles*** page ***Roles*** tab. Refer to Editing User Roles.

In addition, a new role can be assigned to users. Refer to Editing Users.

Exporting Roles View Data

To export information displayed in the ***Roles*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Dashboard View

Similar to the ***Home*** page dashboard, the ***Dashboard*** view displays widgets depicting Ivanti Endpoint Security activity. However, unlike the ***Home*** page dashboard, the ***Dashboard*** view widgets include only information about endpoints within the selected group and its child hierarchy.

Widgets graphs and information are generated based on the latest Ivanti Endpoint Security server and agent data available.

Note: The widgets displayed in the ***Dashboard*** view include data from the selected group's child hierarchy. Configuration changes made to the dashboard settings apply to all groups; not just the selected group.

Group Dashboard Widgets

Most widgets available on the ***Home*** page dashboard are also available from the ***Dashboard*** view. The data depicted on each dashboard changes according to which group is selected.

The following table describes the available widgets.

Table 203: Group Dashboard Widgets

Widget	Description
Agent Module Installation Status	Displays the installation and licensing statistic of each agent module.
Agent Status	Displays all agents grouped by status.
Applicable Content Updates	Displays applicable content updates grouped by content updates.
Critical Patch Status by Endpoint	Displays the patch status of all endpoints with applicable vulnerabilities grouped by when they were released.
Discovery Scan Results: Agents	Displays the total number of agent-supported endpoints discovered in the last-run Discovery Scan Job and identifies how many have an agent installed.
Endpoints with Unresolved AntiVirus Alerts	Displays all endpoints with AntiVirus alerts that require further action, grouped by alert message.

Widget	Description
Endpoints with Unresolved Updates	Displays all endpoints with applicable content updates that have not yet been applied, grouped by content type.
Estimated Energy Savings: Daily	Displays your daily dollar savings and power usages compared with an *always on* state.
Estimated Energy Savings: Monthly	Displays your monthly dollar savings and power usages compared with an *always on* state.
Estimated Energy Savings: Weekly	Displays your weekly dollar savings and power usages compared with an *always on* state.
Incomplete Deployments	Displays all deployments with elapsed start dates and a status of not started or in progress.
Mandatory Baseline Compliance	Displays the percentage of endpoints grouped by Mandatory Baseline compliance.
Offline Patch Agents	Displays all offline agents grouped by the amount of time since they last checked in.
Patch Agent Module Status Widget	Displays all agents with the Patch and Remediation modules installed, which are grouped by Patch and Remediation status.
Scheduled Deployments	Displays endpoints with applicable content updates grouped by content type and the deployment status within each category.
Time Since Last DAU Scan	Displays all active agents (not including disabled or offline) grouped by the amount of time since their last Discover Applicable Updates task.
Top 10 Virus/Malware Threats	Displays a list of the 10 virus/malware threats within your environment ranked by exposure to endpoints.
Top 10 Infected Endpoints	Displays a list of the 10 most infected endpoints currently within your environment.
Un-remediated Critical Vulnerabilities	Displays the total number of un-remediated critical vulnerabilities that are applicable to your environment grouped by age.

Tip: For information about how to edit the group dashboard, refer to Editing the Dashboard on page 67.

Widget Setting and Behavior Icons

Setting and behavior icons are user interface controls that let you manage widgets and the dashboard within the ***Groups*** view. Click these controls to maximize, minimize, hide, and refresh widgets.

The following table describes each icon action.

Table 204: Widget Setting and Behavior Icons

Icon	Action
	Opens the ***Dashboard Settings*** dialog.
	Opens the dashboard in print preview mode.
	Collapses the associated widget.
	Expands the associated collapsed widget.
	Hides the associated widget.
	Refreshes the associated widget (or the entire dashboard).

Note: Not all widgets contain **Refresh** icons.

Previewing and Printing the Dashboard

As with the ***Home*** page dashboard, you can preview and print the ***Group*** page ***Dashboard*** view. ***Dashboard*** view widgets display data that applies only to the selected group.

To preview the ***Dashboard*** view, select the applicable group from the **Browser** and click the print icon.

For additional information, refer to Previewing and Printing the Dashboard on page 67.

Editing the Dashboard

Just as with the ***Home*** page dashboard, you can edit the widgets displayed on the ***Group*** page ***Dashboard*** view. ***Dashboard*** view widgets display data that only applies to the selected group.

To edit the widgets displayed within the ***Dashboard*** view, select the applicable group from the **Browser** and click the edit icon.

For additional information, refer to Editing the Dashboard on page 67.

The Settings View

This view lets you edit various basic settings for the selected group. The settings in this view are miscellaneous settings that cannot be grouped with other settings.

The following table describes ***Settings*** view button functions.

Table 205: Settings View Toolbar

Button	Function
Save	Saves the settings defined in the page.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Editing Group Settings

If different settings are required, you can edit the default settings for a group. Modifying group settings not only modifies settings for the selected group, but also potentially determines settings for descendant groups.

Modify group settings from the ***Settings*** view. For additional information on the remain settings, refer to *Editing Group Settings* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/)

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Settings**.
3. Select the desired group from the directory tree.
4. [Optional] Under **General**, edit the following as necessary.

Option	Description
Group Name (field)	The group name.
	Note: Only `Custom` group names can be edited.
Distinguished Name	A system-created group name that represents the group's parent hierarchy.
	Note: The **Distinguished Name** cannot be edited.

Option	Description
Group Description (field)	The group description.
Q Chain Mode (list)	Defines chain behavior during Mandatory Baseline deployments. Select from the following options: • **Standard -- Set Individually** • **Auto QChain with Manual Reboots** • **Auto QChain with Automatic Reboots**
Deployments Enabled (list)	Defines whether deployments may be created for the group. A `True` value allows authorized users to create deployments for the group.

Note: The **Deployments Enabled** list only impacts the ability to create deployments for a group. Deployments created prior to disabling group deployments will still occur as scheduled. Additionally, any deployments created for the endpoint will occur as scheduled.

5. [Optional] Under **Mandatory Baseline**, edit the following as necessary (Patch and Remediation only).

List	Description
Mandatory Baseline Inheritance	Defines whether the group inherits the agent policies assigned to the group's parent hierarchy. A `True` value sets the group to inherit its parent hierarchy's Mandatory Baseline settings.
Mandatory Baseline Enabled	Defines whether Mandatory Baselines may be assigned to the group. A `True` value allows users to create Mandatory Baseline deployments for the group.

Important: The **Mandatory Baselines enabled** setting applies only to the selected group. Therefore, if the selected group has a parent group with a **Mandatory Baselines enabled** setting of `True`, the selected group will receive its parent group Mandatory Baseline items regardless of its own **Mandatory Baselines enabled** setting.

6. Under **Policy**, edit the following lists as necessary.

List	Description
Policy Inheritance	Defines whether the group inherits the agent policies assigned to the group's parent hierarchy. A `True` value sets the group to inherit its parent hierarchy's agent policy settings. **Note:** To understand agent policy inheritance and its effects, refer to Defining Agent Policy Inheritance Rules on page 418.
Policies Enabled	Defines whether agent policies may be assigned to the group. A `True` value allows users to assign agent policies directly to the group.

7. Under **Other**, edit the following fields as necessary.

Field	Description
Group Owners	User-defined email addresses indicating the owners of the group.
Source Groups (button)	User-defined group or groups whose agents are dynamically assigned to the group. For additional information, refer to Assigning a Source Group to a Custom Group on page 413.

8. Click **Save**.

Result: The new settings are saved and applied to the group.

Defining Source Groups

Source groups are groups that automatically assign managed endpoints to a associated custom group. Use a source group to maintain multiple endpoint memberships by editing only a single group. This feature simplifies maintenance of endpoint membership among groups.

When working within the ***Groups*** page ***Settings*** view, you can assign the selected view a source group. By assigning the selected group a source group, the selected group will be modified when the source

group has endpoints added or removed. Source groups only affect endpoint membership, not group agent policies and settings.

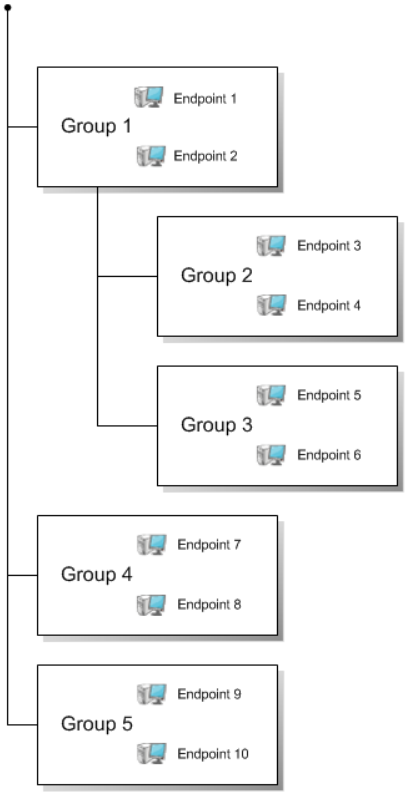


Figure 76: Source Group Diagram

When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. Source groups can only be assigned to custom groups.

The preceding diagram and the following bullets clarify how group sources operates.

- If group 3 uses group 5 as a source group, then group 3 would include endpoints 9 and 10, as well as endpoints 5 and 6.
- Because group 3 is in group 1's hierarchy, group 1 also includes endpoints 9 and 10.
- If group 4 uses group 1 as a source group, group 4 would include endpoints 7 and 8 (through direct assignment), endpoints 1 and 2 (through a directly assigned source group), endpoints 3, 4, 5, and 6 (through group 1's hierarchy), and endpoints 9 and 10 (through an indirectly assigned source group for [group 5 is a source group for group 3]).

Assigning a Source Group to a Custom Group

When a custom group is created, you can assign it a *source group*, which is a group that automatically assigns managed endpoints to associated groups. For example, if you assign *Group 1* as a source group to *Group 2*, any agents assigned to *Group 1* are automatically assigned to *Group 2*.

Assign a group a source group from the ***Settings*** view.

Note: Source groups can only be assigned to custom groups.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Settings**.
3. Select a custom group from the directory tree.
4. Under **Other**, click **Modify**.

   If necessary, scroll to the button.

   Step Result: The ***Edit Source Groups*** dialog opens.

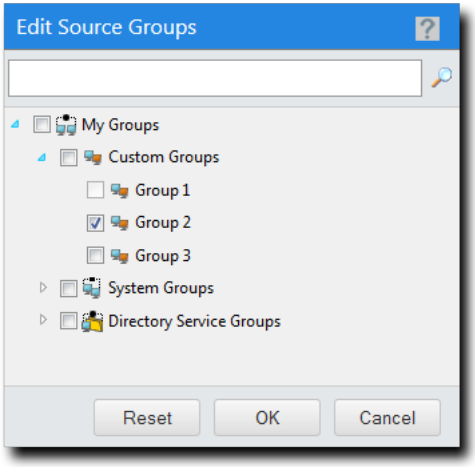


Figure 77: Edit Source Groups Dialog

5. Expand the directory tree or use the search field to locate the group you want to use as a source.
6. Select the groups you want to use as sources.

Note: When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. For additional information, refer to Defining Source Groups on page 411.

7. Click **OK**.

Result: The custom group now uses the selected groups as sources. As new agents are added to (or removed from) the source group, they are also added to (or removed from) the custom group.

Exporting Settings View Data

To export information displayed in the ***Settings*** view to a comma separated value (`.csv`) file, click **Export**. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

Chapter 11

Managing Agent Policy Sets

In this chapter:

- The Agent Policy Sets Page
- Working with Agent Policy Sets

Use *Agent Policy Sets* to control agent behavior. Agent Policy Sets are basic rules which define how agents behave.

Apply the *Agent Policy Sets* to groups to implement your policies to groups. There is a policy for every agent function.

The Agent Policy Sets Page

You can control agent behavior by creating and assigning Agent Policy Sets. Use the ***Agent Policy Sets*** page to define agent rules of behavior.

You can access this page at any time from the navigation menu.

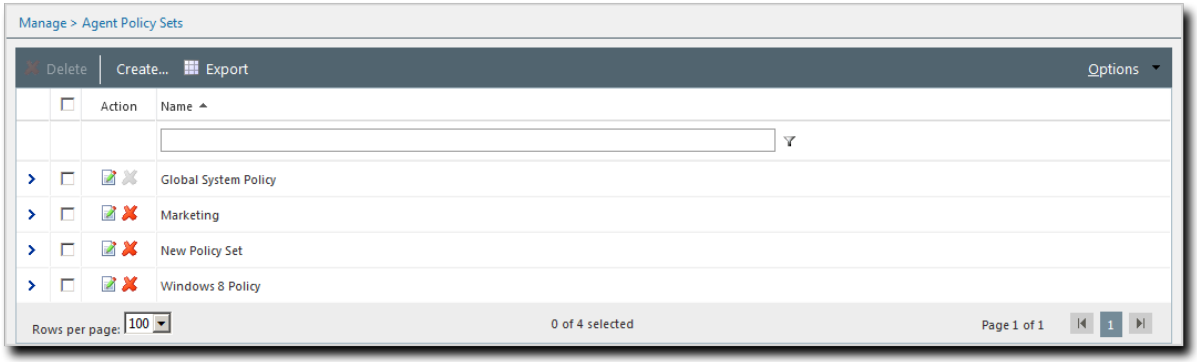


Figure 78: Agent Policy Sets Page

About Agent Policies and Agent Policy Sets

Agent Policies are rules that govern agent behavior. Agent Policy Sets are a collections of agent policy values.

Assign agent policies to groups using the *Agent Policy Sets* view. Based on group membership, agents operate according to the values in assigned Agent Policy Sets. Assignment of Agent Policy Sets is optional.

Groups without assigned Agent Policy Sets have their behavior defined by the **Global System Policy**. The **Global System Policy** does the following:

- Defines behavior for groups with no assigned policy set.
- Defines policy values for incomplete agent policy sets.

When agents holding multiple group memberships are assigned conflicting agent policy values, they are resolved with conflict resolution rules. These rules are a set of protocols that determine which policy value an agent uses when conflicts occur. For additional information, refer to Defining Agent Policy Conflict Resolution on page 418.

About Agent Hardening

Agent Policy Sets include **Agent Hardening** policies, which are policies used to prevent unauthorized Ivanti Endpoint Security Agent removal.

Agent Hardening (when set to On)	• It prevents the Ivanti Endpoint Security Agent installation location (`C:\Program Files\HEAT\EMSSAgent` by default) from being renamed, edited, or deleted. • The Agent is *hardened*, meaning the agent cannot be intentionally or unintentionally modified. • When hardening is in place, you can still upgrade or uninstall the agent after entering the **agent uninstall password** or the **global uninstall password**, which is only necessary when modifying the agent locally from the endpoint. For additional information about defining **Agent Hardening** policies, refer to the following topics: • Creating an Agent Policy Set on page 430 • Editing an Agent Policy Set on page 436
Global uninstall password	**Important:** The **Global uninstall password** option is only available when editing the **Global System Policy** agent policy set. Refer to Changing the Global Uninstall Password on page 444 for additional information. The **Global uninstall password** is a universal password that temporarily disables agent uninstall protection. This password works on all network endpoints. You are prompted for this password when manually upgrading or uninstalling hardened agents. **Note:** • Ivanti *does not* recommend providing end users with the global uninstall password in uninstall scenarios. The **Global uninstall password** should be used by the Ivanti Endpoint Security Administrator only. • In the event an end user needs to uninstall the Ivanti Endpoint Security Agent, provide them with the **Agent uninstall password**, a password that works only for their endpoint. For additional information, refer to Viewing the Agent Uninstall Password on page 218.

Viewing the Agent Policy Sets Page

Navigate to this page to view Agent Policy Sets and their policy settings. Expand policy sets to view the individual policy settings.

You can access this page any time using the navigation menu.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. [Optional] Complete a task listed in Working with Agent Policy Sets on page 429.

Defining Agent Policy Inheritance Rules

You can configure a group to inherit policies from its parent hierarchy using the **Policy inheritance** setting.

Because a group can inherit policies and have them directly assigned, policy conflicts may arise. The following rules apply when a group has **Policy Inheritance** set to `True`:

1. Any conflicting policies are assigned to the parent, but not the child. Conflicting policies are resolved at the parent level using the conflict policy resolution rules.
2. Agent Policy Set values directly assigned to a group supersede inherited Agent Policy Set values.
3. Any conflicting policies that are assigned directly to the child group are resolved by conflict resolution rules.
4. Any Agent Policy Set values that are undefined by the group's directly assigned policy are defined by the parent's group policy.
5. Policy values still undefined are defined by the **Global System Policy** set.

For more information on how to enable a group's *Policy Inheritance* setting, refer to Editing Group Settings on page 409.

For more information on *Conflict Policy Resolution* rules, refer to Defining Agent Policy Conflict Resolution on page 418.

Defining Agent Policy Conflict Resolution

On occasion, a group or endpoint may be assigned two different Agent Policy Sets that have conflicting policies. When this occurs, the system determines which policy to use based on the *Agent Policy Conflict Resolution* rules.

Conflicting policies are resolved in the following order.

1. **Group Policies** - Conflicting policy sets assigned to a group are resolved before conflicting policy sets assigned to an agent are resolved.

   The following rules apply if a group has **Policy Inheritance** set to `False`:

   a. The group does not inherit its parent policy set. Therefore, only policy sets assigned directly to the group require resolution.
   b. Conflicting policies are resolved according to the agent policy conflict resolution rules.

   The following rules apply if a group has **Policy Inheritance** set to `True`:

   a. The group inherits its parent policy set. Any conflicting policy sets that are resolved at the parent level prior to assignment to the child level.
   b. Conflicting policies are assigned directly to the group are resolved using the agent policy conflict resolution rules. Any policy set values assigned directly to a group supersede inherited policy set values.
   c. Finally, any policies that are undefined by direct assignment are defined by inheritance.
2. **Agent Policies** - After resolving the group policies, the conflicting policies assigned to an endpoint (using its group membership) are resolved. The following rules apply:
   a. The resultant policies of all groups the endpoint is a member are resolved according to the agent policy conflict resolution rules.
   b. Any policy values that have not been defined using the agent group membership are populated based on the policy settings defined in the **Global System Policy**.

Note: Conflict resolution rules do not apply to the **Global System Policy**.

The following table defines the rules used when resolving conflicting policy settings:

Table 206: Agent Policy Conflict Resolution Rules

Policy Setting	Resolution
Hide Agent Control Panel	The agent uses true (`Y`).
Core: Download file via HTTP	The agent uses true (`Y`).
Maximum Log File Size	The agent uses the largest log file size value.
Logging Level	The agent uses the most comprehensive logging level value (Trace [`4`] > Diagnostic [`3`] > Normal [`2`] > Error [`1`] > Critical [`0`]).
Agent uninstall protection	The agent uses `On`.
Show alerts on endpoints	The agent uses false (`N`).
Reboot behavior	The agent uses a combination of the most secure value, while still giving the user the best chance to save their work. The items are listed in the following order: • Notify user, user response required before reboot = `0` • Don't notify user, wait for next user-initiated reboot = `2` • Notify user, automatically reboot with 5 minute timer = `1`
Core: Heartbeat Interval	The agent uses the largest heartbeat interval frequency value.
Core: Receive Interval	The agent uses the largest receive interval frequency value.
Core: Timeout Interval	The agent uses the largest timeout interval frequency value.
Core: Send Interval	The agent uses the largest send interval frequency value.

Policy Setting	Resolution
Device Control	
Install and Enable SKNDIS	The agent uses the install enabled value (`1`).
DC: Reporting Interval	The agent uses the largest report interval frequency value.
DC: Monitor Interval	The agent uses the largest monitor interval frequency value.
Power Management	
PM: Enabled	The agent uses `enabled`.
PM: Detection Interval	The agent uses the smallest Power Management detection interval.
PM: Reporting Interval	The agent used the smallest Power Management report interval.
Patch and Remediation	
Maximum Transfer Rate	The agent uses the smallest maximum transfer rate value.
Minimum File Size	The agent uses the smallest minimum file size value.
Agent Scan Mode	The agent uses the fastest agent scan mode value (Fast Scan [`2`] > Initial Scan [`1`] > Normal Scan [`0`]).
Scheduling Frequency	The agent uses the shortest scheduling frequency interval value.
PR Deployment: User May Cancel	The agent uses true (`Y`).
PR Deployment: Always On Top	The agent uses true (`Y`).
PR Deployment: Deploy within	The agent uses the smallest deploy within value.
PR Deployment: User May Snooze	The agent uses false (`N`).
Resume Interrupted Downloads	The agent uses false (`N`).
Patch: FastPath Interval	The agent uses the shortest FastPath interval.
Patch: FastPath Servers	The agent uses all of the defined FastPath servers.
Patch: Download packages via HTTP	The agent uses true (`Y`).
Agent Listener Port	The agent listens on the highest defined port.
PR Reboot: User May Cancel	The agent uses false (`N`).

Policy Setting	Resolution
PR Reboot: Always On Top	The agent uses true (`Y`).
PR Reboot: Reboot within	The agent uses the smallest reboot within value.
PR Reboot: User May Snooze	The agent uses false (`N`).
Patch: Agent to Server Communication	The agent uses true (`https://`).
Patch: Communication Interval	The agent uses the shortest communication interval value.
Hours of Operation: Monday	The agent uses `Always On`.
Hours of Operation: Tuesday	The agent uses `Always On`.
Hours of Operation: Wednesday	The agent uses `Always On`.
Hours of Operation: Thursday	The agent uses `Always On`.
Hours of Operation: Friday	The agent uses `Always On`.
Hours of Operation: Saturday	The agent uses `Always On`.
Hours of Operation: Sunday	The agent uses `Always On`.
InventoryCollectionOption: BIOS	The agent `ON`.
InventoryCollectionOption: CPU	The agent `ON`.
InventoryCollectionOption: CUSTOM	The agent `ON`.
InventoryCollectionOption: DISK_DRIVE	The agent `ON`.
InventoryCollectionOption: ENABLE_WMI	The agent `ON`.
InventoryCollectionOption: HW_DEV_OTHER	The agent `ON`.

Policy Setting	Resolution
InventoryCollectionOption: HW_IDE_CONTROL	The agent ON.
InventoryCollectionOption: HW_NETWORK_ADAPT	The agent ON.
InventoryCollectionOption: HW_NON_PNP	The agent ON.
InventoryCollectionOption: HW_SND_GAME	The agent ON.
InventoryCollectionOption: HW_SYS_DEV	The agent ON.
InventoryCollectionOption: HW_USB	The agent ON.
InventoryCollectionOption: HW_USB_CONTROL	The agent ON.
InventoryCollectionOption: HW_USB_STORAGE	The agent ON.
InventoryCollectionOption: LAST_REBOOT	The agent ON.
InventoryCollectionOption: LAST_USER	The agent ON.
InventoryCollectionOption: MANUF_MODEL	The agent ON.
InventoryCollectionOption: None	The agent OFF.
InventoryCollectionOption: OS_SERIAL	The agent ON.
InventoryCollectionOption: PC_ASSET_TAG	The agent ON.
InventoryCollectionOption: PC_SERIAL	The agent ON.
InventoryCollectionOption: RAM	The agent ON.
InventoryCollectionOption: SERVICES	The agent ON.

Policy Setting	Resolution
InventoryCollectionOption: SOFTWARE	The agent ON.
InventoryCollectionOption: VIRTUAL	The agent ON.

The Agent Policy Sets Page Toolbar

This toolbar contains buttons that allow you to create and edit Agent Policy Sets.

The following table describes each toolbar button.

Table 207: Agent Policy Sets Page Toolbar

Button	Function
Delete	Deletes the selected Agent Policy Set(s). For additional information, refer to Deleting an Agent Policy Set on page 443.
Create...	Creates a new Agent Policy Set. For additional information, refer to Creating an Agent Policy Set on page 430.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Agent Policy Sets Page List

For each agent policy set that you create, an item for that set appears in the ***Agent Policy Sets*** page list. This list names each existing agent policy set and provides access to editing functionality.

Table 208: Agent Policy Sets Page List

Column	Description
Action	Contains **Edit** and **Delete** icons. Use these icons to edit and delete the associated agent policy set. For additional information, refer to the following topics: • Editing an Agent Policy Set on page 436 • Deleting an Agent Policy Set on page 443 **Note:** The **Global System Policy** cannot be deleted.

Column	Description
Name	The name of the agent policy set.

Each item listed on the ***Agent Policy Sets*** page can be expanded to list its individual policy settings. To view agent policy set details from the page list, click the **Rotating Chevron** (>) for the agent policy set, which opens a table containing additional details.

Table 209: Agent Policy Set Details Table

Name	Description
Policy Name	Indicates the unique name of the agent policy set.
Type	Indicates the type of agent policy set (`System` or `User Defined`).
Description	Indicates the description of the agent policy set.
Created By	Indicates the name of the user that created the agent policy set.
Created Date	Indicates the date and time that the agent policy set was created.
Modified By	Indicates the name of the user that last modified the agent policy set.
Modified Date	Indicates the date and time that the agent policy set was last modified.
Agent uninstall protection	Indicates whether agent uninstall protection is on.
Hide agent control panel	Indicates whether the Agent Control Panel is hidden from an endpoint user when they log on to their system. Any dialog or notification launched by the Ivanti Endpoint Security agent will also be hidden until the ***Agent Control Panel*** is started manually using ***Windows Control Panel***.
Reboot behavior	Indicates the reboot behavior. The following values indicate each reboot behavior setting: • Notify user, user response required before reboot = `0` • Notify user, automatically reboot with 5 minute timer = `1` • Don't notify user, wait for next user-initiated reboot = `2`
Download files via HTTP	Indicates whether the Ivanti Endpoint Security Agent downloads files via HTTP rather than HTTPS. All other communication occurs over HTTPS.
Maximum Log File Size	Specifies the maximum size of the Ivanti Endpoint Security agent log before it is deleted.

Name	Description
Logging Level	Indicates the level of detail recorded in the Ivanti Endpoint Security Agent. The following values indicate each logging level: Critical = `0`, Error = `1`, Normal = `2`, Diagnostic = `3`, Trace = `4`.
Show alerts on endpoints	Indicates whether alerts and notifications are shown to endpoint users.
Core: Heartbeat Interval	Indicates the interval at which the Endpoint Service sends a heartbeat to the server (in minutes).
Core: Receive Interval	Indicates the interval at which the Endpoint Service communication receive delay intervals (in seconds).
Core: Timeout Interval	Indicates the interval at which the Endpoint Service communication receive time intervals (in seconds)
Core: Send Interval	Indicates the interval at which the Endpoint Service communication send delay intervals.
Ivanti Device Control only	
Reboot: Reboot Behavior	Device Control reboot behavior option.
Install and Enable SKNDIS	Device Control enabling of SKNDIS driver is installed.
Dvc Control: Monitor Interval	Device Control installation monitor interval.
Dvc Control: Reporting Interval	Device Control status reporting interval.
Power Management Only	
Power Management: Enabled	Indicates power monitoring is enabled on endpoint.
Power Management: Detection Interval	Indicates the Power Management detection interval.
Power Management: Reporting Interval	Indicates the Power Management reporting interval.
Patch: Download packages via HTTP	Indicates if the agent downloads packages using HTTP, regardless of whether HTTPS is used for agent to server communication.
Patch: Maximum Transfer Rate	Indicates the maximum bandwidth used when an agent downloads packages. A setting of *0* disables bandwidth throttling.
Patch: Minimum File Size	Indicates the smallest file size that will be impacted by bandwidth throttling.

Name	Description
Patch: Agent Scan Mode	Indicates the agent detection scan mode (`0` = Slow, `1` = Fast the first time, `2` = Fast).
Patch DAU: Scheduling Frequency	Indicates the number of hours between regularly scheduled detection scans.
Patch Deployment: User May Cancel	Indicates whether the user can cancel a deployment (`Y`, `N`).
Patch Deployment: Always on Top	Indicates whether the notification will be the topmost window (`Y`, `N`).
Patch Deployment: Deploy Within	Indicates the defined time frame (in minutes) during which the user may snooze or cancel a reboot.
Patch Deployment: User May Snooze	Indicates whether the user can snooze a deployment.
Patch: Resume Interrupted Downloads	Indicates whether resumable downloads are enabled (0 = No, 1 = Yes).
Patch: Fast Path Interval	Indicates the interval (configurable in minutes, hours, and days) between each check by FastPath to determine the fastest communication path back to the Ivanti Endpoint Security server.
Patch: Fast Path Servers	Indicates the available Fast Path routes.
Patch Agent Listener Port	Indicates the agent listener port. When the agent is contacted on this port, it responds with its version number and initiates communication with the Ivanti Endpoint Security server. A value of 0 turns the agent listener off.
Patch Reboot: User May Cancel	Indicates whether the user can cancel a reboot (`Y`, `N`).
Patch Reboot: Always on Top	Indicates whether the notification will be the topmost window (`Y`, `N`).
Patch Reboot: Reboot Within	Indicates the defined time window (in minutes) during which the user may snooze or cancel a reboot.
Patch Reboot: User May Snooze	Indicates whether the user can snooze a reboot (`Y`, `N`).
Patch: Agent to Server Communication Protocol	Defines how the agent will communicate with the server (`http://` or `https://`).
Patch: Communication Interval	Indicates the time period between agent communication attempts.
Patch: Hours of Operation Monday	Defines the agent Hours of Operation (HOP) for Monday.

Name	Description
Patch: Hours of Operation Tuesday	Defines the agent HOP for Tuesday.
Patch: Hours of Operation Wednesday	Defines the agent HOP for Wednesday.
Patch: Hours of Operation Thursday	Defines the agent HOP for Thursday.
Patch: Hours of Operation Friday	Defines the agent HOP for Friday.
Patch: Hours of Operation Saturday	Defines the agent HOP for Saturday.
Patch: Hours of Operation Sunday	Defines the agent HOP for Sunday.
Patch: InventoryCollectionOptions: BIOS	Indicates whether BIOS data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: CPU	Indicates whether CPU data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: CUSTOM	Indicates whether custom inventory data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: DISK_DRIVES	Indicates whether data regarding the disk drives will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: ENABLE_WMI	Indicates whether WMI data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_DEV_OTHER	Indicates whether the Windows registry will be scanned for additional hardware information during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_IDE_CONTROL	Indicates whether data regarding IDE ATA/ATAPI controllers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_NETWORK_ADAPT	Indicates whether data regarding network adapters will be gathered during agent inventory collection (OFF or ON).

Name	Description
Patch: InventoryCollectionOptions: HW_NON_PNP	Indicates whether data regarding non-Plug and Play drivers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_SND_GAME	Indicates whether data regarding sound, video, and game controllers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_SYS_DEV	Indicates whether system device data will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_USB	Indicates whether data regarding USB endpoint's inventory (from \ENUM\USB) will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_USB_CONTROL	Indicates whether data regarding USB controllers will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: HW_USB_STORAGE	Indicates whether data regarding USB device inventory (from \ENUM\USBSTOR) will be gathered during agent inventory collection (OFF or ON).
InventoryCollectionOptions: LAST_REBOOT	Requires ENABLE_WMI = ON: Indicates whether the last boot time will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: LAST_USER	Indicates whether last logged in user and time will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: MANUF_MODEL	Requires ENABLE_WMI = ON: Indicates whether the computer manufacturer and model will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: OS_SERIAL	Requires ENABLE_WMI = ON: Indicates whether the OS serial number will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: PC_ASSET_TAG	Requires ENABLE_WMI = ON: Indicates whether the endpoint's asset tag will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: PC_SERIAL	Requires ENABLE_WMI = ON: Indicates whether the endpoint's serial number will be gathered during agent inventory collection (OFF or ON).

Name	Description
Patch: InventoryCollectionOptions: RAM	Indicates whether the endpoint's total physical RAM will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: SERVICES	Indicates whether a listing of Windows services (not applicable for Windows 9x or ME) will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: SOFTWARE	Indicates whether a listing of installed software will be gathered during agent inventory collection (OFF or ON).
Patch: InventoryCollectionOptions: VIRTUAL	Indicates whether the endpoint's virtualization status will be gathered during agent inventory collection (OFF or ON).
Security Configuration Management (Security Configuration Management only)	Indicates security configuration management compliance policies.

Note: This reference table does not list the **Value** contained in the agent policy set details. This column (which appears in the user interface) contains values that agent policies are set to.

Working with Agent Policy Sets

There are many tasks that you can perform from the ***Agent Policy Sets*** page related to agent policy sets. Some tasks are performed by clicking toolbar buttons, while others are performed by interacting with list items.

- Creating an Agent Policy Set on page 430
- Editing an Agent Policy Set on page 436
- Deleting an Agent Policy Set on page 443
- Changing the Global Uninstall Password on page 444
- Defining Agent Policy Logging Levels on page 446
- Defining Inventory Collection Options on page 448
- Defining Agent Hours of Operation on page 450
- The Edit FastPath Servers Dialog on page 452
- Exporting Data for Agent Policy Sets on page 455

Creating an Agent Policy Set

You can create an unlimited number of Agent Policy Sets to define how endpoints behave. Following creation, associate an Agent Policy Set with a group or endpoint to apply policy settings. After installing new modules, additional options are available when creating an Agent Policy Set.

Create an Agent Policy Sets from the ***Create Agent Policy Set*** dialog.

1. Select **Manage** > **Agent Policy Sets**.
2. Click **Create**.

   Step Result: The ***Create Agent Policy Set*** dialog opens.
3. Type the applicable information in the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

4. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 417.

Option	Description
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.

5. Define the **Agent Logging** options.

   The following table describes each option.

Option	Step
Logging level (button)	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 446.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

6. Define the **Ivanti Endpoint Security Agent Communication** options.
   The following table describes each option.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *True*.
Send interval (list)	Select the amount of time that the agent should wait before sending an event to the Ivanti Endpoint Security server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval (field and list)	Type and select the amount of time that the agent should delay before reattaching events from the Ivanti Endpoint Security Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.
Timeout interval (field and list)	Type and select the amount of time the agent should stay attached to the Ivanti Endpoint Security server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval (field and list)	Type and select the amount of time between agent check-ins with the Ivanti Endpoint Security server (1 minute-1 day). A value of *15 minutes* is the default setting.

7. Define the **Ivanti Endpoint Security Agent Notification Defaults** options.
   The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the ***Agent Control Panel*** (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**). **Note:** • This policy will not take effect until the agent is restarted. • This policy can hide only the Ivanti Endpoint Security Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***. • This policy cannot hide the Patch Agent or the Agent.

Option	Description
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the ***Agent Control Panel*** are hidden or accessible to an endpoint user after logging on (**True** or **False**).

8. Define the **Reboot Behavior Defaults** option.

   An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

   a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.
Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

9. Define the **Patch Agent Communication** options.

   The following table describes each option.

Option	Step
Use SSL for agent to server communication (list)	Select whether the Patch Agent uses HTTPS when communicating with the Ivanti Endpoint Security server.
Use HTTP for package download (list)	Select whether files are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *False*.
Agent Listener Port (field)	Select the agent listener port number. When the agent is contacted using this port, it responds with the agent version number and initiates communication with Ivanti Endpoint Security. The default value of *0* disables the agent listener.

Option	Step
Agent Scan Mode (list)	Select the mode that the Discover Applicable Updates (DAU) task runs in. These modes include: **Normal** — Performs the DAU task normally, which uses the least amount of resources. **Initial Only** — Performs the first DAU task in fast mode, but subsequent DAU tasks in normal mode. **Fast Scan** — Performs the DAU task faster, but uses more resources. The default value is *Normal*.
Communication Interval (field and list)	Type and select the interval (in minutes, hours, or days) between agent and Ivanti Endpoint Security communication (1 minute-1 day). The default value is *15 minutes*.
Inventory Collection Options (button)	Click to open the ***Select Inventory Collection*** dialog. Use this dialog to select the inventory values for recording during agent scanning. For additional information, refer to Defining Inventory Collection Options on page 448.
Resume Interrupted Downloads (list)	Select whether the agent resumes interrupted downloads at the point of interruption (*True* or *False*). The default value is *True*.
Hours of Operation (button)	Click to open the ***Edit Agent Hours of Operation*** dialog. Hours of operation are based on agent local time, allowing for further definition of the agent start and end times. For additional information, refer to Defining Agent Hours of Operation on page 450.

10.[Optional] Define the **Configuration Policies** option according to context.

Context	Step
If defining this option for the first time:	Click the **Define** button adjacent to **Security Configuration management**.

Context	Step
If editing this option after it has been defined:	Click the **Modify** button adjacent to **Security Configuration management**.

Step Result: The ***Configuration Policy Management*** dialog opens. For more information regarding defining configuration policies, see Uploading and Applying a Benchmark to a New Agent Policy Set.

11. Define the **Ivanti Patch and Remediation Deployment Notification Defaults** options.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the deployment (**True** or **False**). The default value is **False**.
User May Snooze (list)	Select whether the deployment recipient can snooze the deployment (**True** or **False**). The default value is **True**.
Deploy Within (field)	Select the default time (in minutes) between the creation of the deployment and the deployment deadline (1-1440). The default value is **5 minutes**.
Always On Top (list)	Select whether deployment notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 286.

12. Define the **Ivanti Patch and Remediation Reboot Notification Defaults**.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the reboot (**True** or **False**). The default value is *True*.
User May Snooze (list)	Select whether the deployment recipient can snooze the reboot (**True** or **False**). The default value is *True*.
Reboot Within (field)	Type the default time (in minutes) between the creation of the deployment and the reboot deadline (1-1440). The default value is **5 minutes**.
Always on Top (list)	Select whether reboot notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 286.

13. Define the **Discover Applicable Updates (DAU)** option.

Option	Step
Scheduling Frequency (field)	Type the frequency (in hours) of the DAU task (1-8760). The default value is *26 hours*.

14. Define the **FastPath Servers** options.

For additional information, refer to About FastPath on page 453.

Option	Step
Interval (field and list)	Type the time interval (in minutes, hours, or days) between FastPath server validations (0 minutes-7 days). The default value of *0* disables the option.
Servers (button)	Click **Define** to open the ***Edit FastPath Servers*** dialog. Use this dialog to add FastPath servers. For additional information, refer to Adding/Editing FastPath Servers on page 453.

15. Define the **Bandwidth Throttling** options.

Option	Step
Maximum Transfer Rate (field)	Type the maximum amount of network bandwidth (in kilobytes per second), per endpoint that can be used by the agent for content download (0-1024). The default value of *0* disables bandwidth throttling.
Minimum File Size (field)	Type the threshold (in KB) at which a file will be managed by bandwidth throttling (0-1024). Files smaller than the defined value will not be managed by bandwidth throttling. The default value is *100*.

16. Define the **Power Management** options (Ivanti Power Management only).

For additional information, refer to Power Management Policies.

17. Define the **Device Control** options .

Option	Description
DC install SK-NDIS driver (list)	Indicates whether Ivanti Endpoint Security installs a SK-NDIS on endpoints assigned the policy (**Do not install** or **Install Enabled**).
DC detection interval (field)	Indicates the detection interval (in minutes) that determines how often the endpoint verifies installation.

Option	Description
DC device event upload interval (field)	Indicates the reporting interval (in minutes) that determines how other the endpoint reports device events back to the server.
DC agent reboot behavior (Read-only text)	Indicates how reboots are performed following installation of the Device Control endpoint module. This behavior is defined using the **Reboot behavior** option. For additional information, refer to 8 on page 432.

18. Define the **AntiVirus** option:

Option	Description
Delay AV definition distribution by (field)	Type the time interval (in hours, up to 23 hours) that the Ivanti Endpoint Security Agent is to delay requesting a new AntiVirus definitions file from the Application Server. The default value of *0* hours disables the option. Use this option to make time to test a new definitions file in a test environment before distributing it to agents (for example, to check for false positives that can negatively affect system functionality). **Important:** Delaying the download of important updates can make your environment vulnerable to new viruses or malware.

19. Click **Save**.

Result: Your Agent Policy Set is saved. You can now assign the Agent Policy Set to endpoint groups or edit the set.

After Completing This Task:
To assign an Agent Policy Set to a group, complete Assigning an Agent Policy Set to a Group on page 385.

Editing an Agent Policy Set

Following the creation of an Agent Policy Set, you can modify it to accommodate network environment changes.

The ***Edit A Policy Set*** dialog allows you to modify an agent policy set.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Click the **Edit** icon associated with the policy set you want to edit.

   Step Result: The ***Edit a Policy Set*** dialog opens.

3. [Optional] Edit the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

4. [Optional] Edit the **Agent Hardening** options.
   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 417.

Option	Step
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.
Global Uninstall Password (button)	Click **Modify** to open the ***Global Uninstall Password*** dialog. Use this dialog to define a password for manually uninstalling the agent. For additional information, refer to Changing the Global Uninstall Password on page 444. **Note:** This option only available when editing the Global System Policy agent policy set. Only users assigned to the built-in Administrator role may view or modify the global uninstall password.

5. [Optional] Edit the **Agent Logging** options.

Option	Step
Logging level (button)	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 446.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

6. [Optional] Edit the **Ivanti Endpoint Security Agent Communication** options.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *True*.

Options	Step
Send interval (list)	Select the amount of time that the agent should wait before sending an event to the Ivanti Endpoint Security server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval (field and list)	Type and select the amount of time that the agent should delay before reattaching events from the Ivanti Endpoint Security Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.
Timeout interval (field and list)	Type and select the amount of time the agent should stay attached to the Ivanti Endpoint Security server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval (field and list)	Type and select the amount of time between agent check-ins with the Ivanti Endpoint Security server (1 minute-1 day). A value of *15 minutes* is the default setting.

7. [Optional] Define the **Ivanti Endpoint Security Agent Notification Defaults** options.
   The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the ***Agent Control Panel*** (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**). **Note:** • This policy will not take effect until the agent is restarted. • This policy can hide only the Ivanti Endpoint Security Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***. • This policy cannot hide the Patch Agent or the Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the ***Agent Control Panel*** are hidden or accessible to an endpoint user after logging on (**True** or **False**).

8. [Optional] Edit the **Reboot Behavior Defaults**.

   An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

   a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.
Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

9. [Optional] Edit the **Patch Agent Communication** options.

Option	Step
Use SSL for agent to server communication (list)	Select whether the Patch Agent uses HTTPS when communicating with the Ivanti Endpoint Security server.
Use HTTP for package download (list)	Select whether files are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *False*.
Agent Listener Port (field)	Select the agent listener port number. When the agent is contacted using this port, it responds with the agent version number and initiates communication with Ivanti Endpoint Security. The default value of *0* disables the agent listener.

Option	Step
Agent Scan Mode (list)	Select the mode that the Discover Applicable Updates (DAU) task runs in. These modes include: **Normal** — Performs the DAU task normally, which uses the least amount of resources. **Initial Only** — Performs the first DAU task in fast mode, but subsequent DAU tasks in normal mode. **Fast Scan** — Performs the DAU task faster, but uses more resources. The default value is *Normal*.
Communication Interval (field and list)	Type and select the interval (in minutes, hours, or days) between agent and Ivanti Endpoint Security communication (1 minute-1 day). The default value is *15 minutes*.
Inventory Collection Options (button)	Click to open the ***Select Inventory Collection*** dialog. Use this dialog to select the inventory values for recording during agent scanning. For additional information, refer to Defining Inventory Collection Options on page 448.
Resume Interrupted Downloads (list)	Select whether the agent resumes interrupted downloads at the point of interruption (*True* or *False*). The default value is *True*.
Hours of Operation (button)	Click to open the ***Edit Agent Hours of Operation*** dialog. Hours of operation are based on agent local time, allowing for further definition of the agent start and end times. For additional information, refer to Defining Agent Hours of Operation on page 450.

10.[Optional] Edit the **Configuration Policies** option.

Context	Step
If defining this option for the first time:	Click the **Define** button adjacent to **Security Configuration management**.

Context	Step
If editing this option after it has been defined:	Click the **Modify** button adjacent to **Security Configuration management**.

Step Result: The ***Configuration Policy Management*** dialog opens. For more information regarding defining configuration policies, see Uploading and Applying a Benchmark to a New Agent Policy Set.

11. [Optional] Edit the **Ivanti Patch and Remediation Deployment Notification Defaults** options.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the deployment (**True** or **False**). The default value is **False**.
User May Snooze (list)	Select whether the deployment recipient can snooze the deployment (**True** or **False**). The default value is **True**.
Deploy Within (field)	Select the default time (in minutes) between the creation of the deployment and the deployment deadline (1-1440). The default value is **5 minutes**.
Always On Top (list)	Select whether deployment notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 286.

12. [Optional] Edit the **Ivanti Patch and Remediation Reboot Notification Defaults**.

Option	Step
User May Cancel (list)	Select whether the deployment recipient can cancel the reboot (**True** or **False**). The default value is *True*.
User May Snooze (list)	Select whether the deployment recipient can snooze the reboot (**True** or **False**). The default value is *True*.
Reboot Within (field)	Type the default time (in minutes) between the creation of the deployment and the reboot deadline (1-1440). The default value is **5 minutes**.
Always on Top (list)	Select whether reboot notifications display as the topmost window (**True** or **False**). The default value is **True**. For additional information about the **Always on Top** policy, refer to About the Show on Top Option on page 286.

13.[Optional] Edit the **Discover Applicable Updates (DAU)** option.

Option	Step
Scheduling Frequency (field)	Type the frequency (in hours) of the DAU task (1-8760). The default value is *26 hours*.

14.[Optional] Edit the **FastPath Servers** options.

Option	Step
Interval (field and list)	Type the time interval (in minutes, hours, or days) between FastPath server validations (0 minutes-7 days). The default value of *0* disables the option.
Servers (button)	Click **Define** to open the ***Edit FastPath Servers*** dialog. Use this dialog to add FastPath servers. For additional information, refer to Adding/Editing FastPath Servers on page 453.

15.[Optional] Edit the **Bandwidth Throttling** options.

Option	Step
Maximum Transfer Rate (field)	Type the maximum amount of network bandwidth (in kilobytes per second), per endpoint that can be used by the agent for content download (0-1024). The default value of *0* disables bandwidth throttling.
Minimum File Size (field)	Type the threshold (in KB) at which a file will be managed by bandwidth throttling (0-1024). Files smaller than the defined value will not be managed by bandwidth throttling. The default value is *100*.

16.[Optional] Edit the **Power Management** options (Ivanti Power Management only).
For additional information, refer to Power Management Policies.

17. Edit the **Device Control** options (Device Control only).

Option	Step
DC install SK-NDIS driver (list)	Indicates whether Ivanti Endpoint Security installs a SK-NDIS on endpoints assigned the policy (**Do not install** or **Install Enabled**).
DC detection interval (field)	Indicates the detection interval (in minutes) that determines how often the endpoint verifies installation.

Option	Step
DC device event upload interval (field)	Indicates the reporting interval (in minutes) that determines how other the endpoint reports device events back to the server.
DC agent reboot behavior (Read-only text)	Indicates how reboots are performed following installation of the Device Control endpoint module. This behavior is defined using the **Reboot behavior** option. For additional information, refer to 8 on page 439.

18. Define the **AntiVirus** option:

Option	Description
Delay AV definition distribution by (field)	Type the time interval (in hours, up to 23 hours) that the Ivanti Endpoint Security Agent is to delay requesting a new AntiVirus definitions file from the Application Server. The default value of *0* hours disables the option. Use this option to make time to test a new definitions file in a test environment before distributing it to agents (for example, to check for false positives that can negatively affect system functionality). **Important:** Delaying the download of important updates can make your environment vulnerable to new viruses or malware.

19. Click **Save**.

Result: Your edits are saved. The new policy values take effect the next time the applicable agents communicate with the Ivanti Endpoint Security server.

Deleting an Agent Policy Set

As your network environment changes, Agent Policy Sets may no longer be applicable. When this event occurs, you may delete the unnecessary Agent Policy Set.

You can delete Agent Policy Sets at any time from the ***Agent Policy Sets*** page.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.

2. Delete one or more Agent Policy Sets.
   Use one of the following methods.

Method	Steps
To delete one Agent Policy Set:	Click the **Delete** icon associated with an Agent Policy Set.
To delete multiple Agent Policy Sets:	1. Select the check boxes associated with the Agent Policy Sets you want to delete. 2. From the toolbar, click the **Delete** button.

Note: Assigned agent policy sets and the **Global System Policy** cannot be deleted.

Step Result: A dialog displays, asking you to acknowledge the deletion.

3. Acknowledge the deletion by clicking **OK**.

Result: The Agent Policy Set(s) is deleted.

Changing the Global Uninstall Password

Change the Global Uninstall Password associated with the **Global System Policy** set. to uninstall any agent in your network.

Note: To uninstall an agent from its host endpoint, you must enter one of two passwords: *Endpoint Uninstall Password* or the *Global Uninstall Password*. The Global Uninstall Password feature ensures that endpoint users cannot uninstall the agent without the knowledge and permission of the administrator.

Define the Global Uninstall Password when editing the **Global System Policy**.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Click the edit icon ( ) for the **Global System Policy** set.
   Step Result: The ***Edit a Policy Set*** dialog opens.

3. Under the ***Agent Hardening*** section, click the **Modify** button adjacent to the **Global uninstall password** field.

   Step Result: The ***Global Uninstall Password*** dialog opens.

Figure 79: Global Uninstall Password Dialog

4. Type the desired password in the **New password** field.

   Tip: The password must be at least 8 characters in length.

5. Retype the password in the **Confirm new password** field.
6. Click **Save**.

   Note: Password edits are not saved until the agent policy set itself is saved.

7. Finish any desired edits to the **Global System Policy** set and click **Save**.

   Note: Password edits are not saved until the **Global System Policy** set is saved.

Result: The ***Global Uninstall Password*** dialog closes. Your edits take effect the next time Ivanti Endpoint Security and the applicable agents communicate.

Tip: The password required to uninstall the agent from the endpoint locally can be found. Refer to Viewing the Agent Uninstall Password on page 218 for additional information.

Defining Agent Policy Logging Levels

All Ivanti Endpoint Security Agents record a log of events that transpire on the endpoint. An Agent Policy Set logging level setting controls how much memory an agent's host endpoint allocates for event logs.

Note: A defined logging level can help troubleshoot agent policy behavior. Define logging levels carefully: a low logging level may not record enough information to be useful; however, a high logging level may record verbose information at the cost of higher disk space.

Define logging levels when creating or editing an Agent Policy Set.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

Step Result: Either the ***Create an Agent Policy Set*** or the ***Edit a Policy Set*** dialog opens.

3. Under the ***Agent Logging*** section perform one of the following procedures based on your context.

Context	Procedure
If you are defining the logging level for the first time:	Click the **Define** button adjacent to the **Logging level** field.

Context	Procedure
If you are modifying the logging level:	Click the **Modify** button adjacent to the **Logging level** field.

Step Result: The ***Logging Level*** dialog opens.

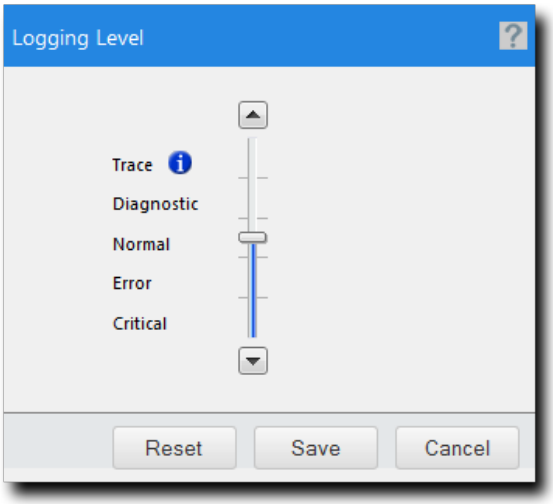


Figure 80: Logging Level Dialog

4. Move the slider to the desired logging level.
   The following table describes each logging level.

Logging Level	Description
Trace	Logs all errors and system actions. **Note:** This highest level logging level should be used only when necessary, as it will consume a large amount of resources on the endpoint.
Diagnostic	Logs all errors and major system actions.
Normal	Logs all errors and basic system action and usage information.
Error	Logs only errors.
Critical	Logs only critical events.

5. Click **Save**.

6. Finish any additional edits to the Agent Policy Set and click **Save**.

Note: Logging level edits are not saved until the Agent Policy Set is saved.

Result: The ***Logging Level*** dialog closes. Your edits take effect the next time the Ivanti Endpoint Security server and the applicable agents communicate.

Defining Inventory Collection Options

Each Ivanti Endpoint Security agent compiles a list of hardware and software present on its host endpoint. However, you can control how detailed this inventory is; you can configure what hardware and software items the agent should scan for. Selecting fewer items from the list requires fewer system resources, but the resulting inventory is not as robust.

Perform this task from ***Select Inventory Collection*** dialog when editing or creating an agent policy set.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

Step Result: Either the ***Create Agent Policy Set*** or the ***Edit a Policy Set*** dialog opens.

3. Under the ***Patch Agent Communication*** section perform one of the following procedure based on your context.

Context	Procedure
If you defining inventory collection options for the first time:	Click the **Define** button adjacent to the **Inventory Collection Options** field.
If you modifying inventory collection options:	Click the **Modify** button adjacent to the **Inventory Collection Options** field.

Step Result: The ***Select Inventory Collection*** dialog opens.

4. Select or clear the check boxes associated with the desired inventory collection options.
   The following table describes each option.

Tip: Selecting an option with child options automatically selects the child options as well.

Option	Description
Allow use of WMI during inventory collection	Required if Windows Management Instrument (WMI) data will be gathered.
Hardware	Selects or clears all options grouped under **Hardware**.
USB controllers	Scans for data regarding USB device inventory (from `HKEY_LOCAL_MACHINE\Enum\USB`).
IDE ATA/ATAPI controllers	Scans for data regarding IDE ATA/ATAPI controllers.
Other hardware devices	Scans for system device data.
Processors	Scans for processor data.
USB Storage Devices	Scans for data regarding USB device inventory (from `HKEY_LOCAL_MACHINE\Enum\USBSTOR`).
Network adapters and MAC address (may use WMI)	Scans for data regarding network adapters.
Physical RAM - amount	Scans for the endpoint's total physical RAM.
System devices	Scans the Windows registry for additional hardware information.
Non-Plug and Play drivers	Scans for data regarding non plug-and-play drivers.
Locally attached drives, total, and free space	Scans for data regarding the disk drives.
USB devices	Scans for data regarding USB controllers.
BIOS information	Scans for BIOS data.
Sound, video, and game controllers	Scans for data regarding sound, video, and game controllers.
Services	Scans for a listing of Windows services (not applicable for Windows 9x or ME).
Software	Scans for a listing of installed software.
Other	Selects or clears all child options grouped under **Other**.
OS serial number (requires WMI)	Scans for the OS serial number (requires WMI).
Virtual Machines	Scans to determine if the endpoint is a virtual machine.

Option	Description
Endpoint serial number (requires WMI)	Scans for the endpoint's serial number (requires WMI).
Endpoint manufacturer and model (may use WMI)	Scans for the computer manufacturer and model.
Endpoint asset tag (requires WMI)	Scans for the endpoint's asset tag (requires WMI).
User - last logged on	Scans for last logged in user and time.
System uptime (may use WMI)	Scans for and returns the time since last reboot (system uptime).
Custom import from file (may use WMI)	Scans for files containing custom inventory data.

5. Click **OK**.
6. Finish any desired edits in the agent policy set dialog and click **Save**.

Note: Edits to the **Inventory Collection Options** are not saved until you click **Save** in the agent policy set dialog.

Result: Your edits are saved. These edits take effect the next time Ivanti Endpoint Security and the applicable agents communicate.

Defining Agent Hours of Operation

Agent hours of operations determine when a patch agent is active on its host endpoint. In other words, this setting restricts agent operations to a specific time range. By applying a specific hours of operation setting, you can configure the agents to operate at optimal hours. For example, setting your agents to only work during the weekend will ensure bandwidth remains open during operation hours, helping to maintain worker efficiency. Optimal agent hours of operation vary by network.

Edit agent hours of operation when creating or editing an agent policy set.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.

Context	Procedure
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

Step Result: Either the ***Create Agent Policy Set*** or the ***Edit a Policy Set*** dialog opens.

3. Under ***Patch Agent Communication*** perform one of the following procedure based on your context.

Context	Procedure
If you are creating an agent policy set:	Click the **Define** button adjacent to the **Hours of Operation** field.
If you are editing an agent policy set:	Click the **Modify** button adjacent to the **Hours of Operation** field.

Step Result: The ***Edit Agent Hours of Operation*** dialog opens.

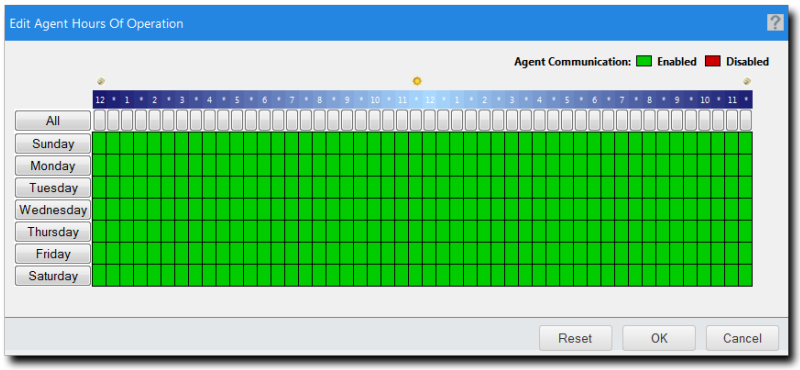


Figure 81: Edit Agent Hours of Operation Dialog

4. Click time units to define agent hours of operation.

   Green units indicate days and times of enablement, while red units indicate days and times of disablement.

   - Click **All** to toggle all ***Time*** units on or off.
   - Click ***Day*** to toggle time units for a day on or off.
   - Click ***Time*** units to toggle individual units on or off.

5. Click **OK**.

6. Finish any desired edits in the dialog and click **Save**.

Note: Changes made to the **Hours of Operation** schedule will not be saved until you have clicked **Save** in the **agent policy set dialog**.

Result: Your edits are saved. These edits take effect the next time Ivanti Endpoint Security and the applicable agents communicate.

The Edit FastPath Servers Dialog

Use this dialog to leverage caching proxies in your network, also known as *FastPath Servers*, to store content and reroute your server and agent communications.

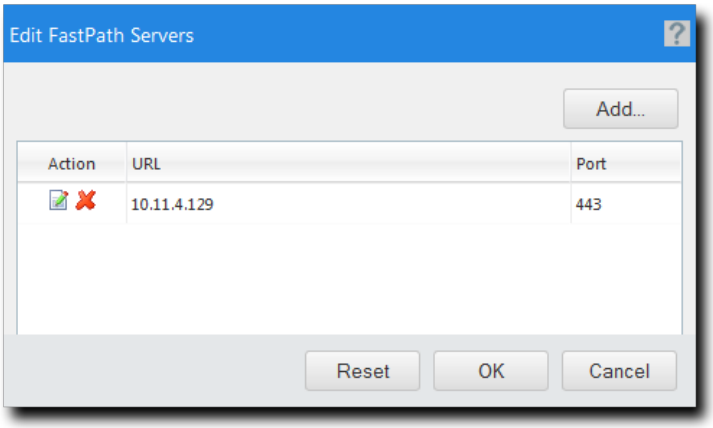


Figure 82: Edit FastPath Servers Dialog

To access this dialog, click the **Define/Modify** next to **Servers** field within the ***Create/Edit A Policy Set*** dialog.

Table 210: Edit FastPath Servers Dialog Columns

Column	Description
Action	Contains action icons (and). Use these to edit and delete FastPath servers.
URL	The URL of the FastPath server.
Port	The port number the FastPath server uses to route communication between the server and agents.

The following table describes the buttons specific to the ***Create/Edit FastPath Servers*** dialog.

Table 211: Edit FastPath Servers Dialog Buttons

Button	Description
Add	Opens the ***Add/Modify FastPath Server*** dialog. For additional information, refer to Adding/Editing FastPath Servers on page 453.

About FastPath

In large networks, you can configuring caching proxies, or FastPath servers, to increase deployment speed and reroute server and agent communications.

This practice provides several benefits:

- Endpoints download deployment content from FastPath servers instead of your Ivanti Endpoint Security server. This action reduces bandwidth consumed during large deployments.
- You can assign FastPath servers to endpoints by applying policies to groups, rather than assigning them directly to the endpoint.
- You can assign fallback FastPath servers, in case the primary FastPath server fails.

Periodically, agents validate the FastPath servers you have assigned to a group. During this process, agents determine the FastPath server used by contacting each one. The FastPath server with the shortest path to the agent is used for deployments and communications.

Add FastPath servers and a FastPath communication interval to a policy by defining the **FastPath Server** policies.

Adding/Editing FastPath Servers

Use of FastPath servers, or caching proxies, optimizes communication routes between your server and agents.

You can add or edit FastPath servers from the ***Add/Modify FastPath Server*** dialog when creating or editing agent policy sets.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Perform one of the following procedures based on your context.

Context	Procedure
To create an agent policy set:	Click **Create**.
To edit an agent policy set:	Click for the policy you want to edit.

Step Result: A dialog for creating or editing an agent policy set opens.

3. Under ***FastPath Servers*** perform one of the following procedures based on context.

Context	Procedure
If adding FastPath servers for the first time:	Click **Define** next to the **Servers** field.
If modifying FastPath servers that have already been defined:	Click **Modify** next to the **Servers** field.

Step Result: The ***Edit FastPath Servers*** dialog opens.

4. Click **Add**.

Tip: If you want to edit existing FastPath server settings, click for the server.

Step Result: The ***Add/Modify Server*** dialog opens.

5. Define the FastPath server information.
   Type the FastPath server information in the following fields.

Field	Description
URL	The FastPath server URL in the following format: `http://<FastPathURL>`.
Port	The FastPath server port number used to route server and agent communication.

6. If using a FastPath server that requires authentication, select the **Authenticated** check box and type the applicable information in the following fields.
   Ivanti Endpoint Security validates the credentials that you enter.

Field	Description
User Name	A local or domain user account that authenticates with the FastPath server.
Password	The password for the user name.
Confirm Password	The password retyped.

7. Click **OK**.

Step Result: The ***Add/Modify Fastpath Server*** dialog closes.

8. [Optional] Repeat the previous step to add another FastPath server.

Tip:
Ivanti recommends the following practices when assigning FastPath servers:

- Add the Ivanti Endpoint Security server itself as a FastPath server. This practice ensures that if all other FastPath servers cannot be validated, the agent can still communicate with the server.
- Because FastPath servers do not share cache directories with each other, do not add more than three servers per policy. Adding more servers negates bandwidth conservation.
- Assign FastPath servers to groups based on geographical location.

9. Click **OK** to close the ***Edit FastPath Servers*** dialog.
10. Finish any desired edits in the agent policy set dialog and click **Save**.

Note: Added FastPath servers are not saved until its parent agent policy set is saved.

Result: Your edits are saved. Your FastPath servers are validated immediately.

Deleting FastPath Servers
When you no longer want to use a FastPath server, delete its entry from the ***Edit FastPath Servers*** dialog.

Delete FastPath Servers from the ***Edit FastPath Servers*** dialog. You can delete FastPath servers when creating or editing an agent policy set.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Click the **Edit** icon associated with the agent policy set that contains the FastPath server you want to delete.

   Step Result: The ***Edit a Policy Set*** dialog opens.
3. Under ***Fastpath Servers*** click the **Modify** button adjacent to the **Servers** field.

   Step Result: The ***Edit FastPath Servers*** dialog opens.
4. Click the **Delete** icon associated with the FastPath server you want to delete.

   Step Result: A dialog opens asking you to acknowledge the deletion.
5. Acknowledge the deletion by clicking **OK**.

Result: The FastPath server is deleted.

Exporting Data for Agent Policy Sets

Click the toolbar **Export** button to export the list of Agent Policy Sets listed on the ***Agent Policy Sets*** page to a comma-separated value (`.csv`) file. Exporting data lets you work with data in other programs for reporting and analytical purposes.

Data for policy values are also exported. For additional information, refer to Exporting Data on page 47.

Assigning an Agent Policy Set to a Group

Assigning an Agent Policy Set to a group defines functional rules for the group.

Prerequisites:

Create an Agent Policy Set. Refer to Creating an Agent Policy Set (Groups Page) on page 387 for details.

Assign Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 415 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Assign**.

   Step Result: The **Select a Policy Set** list becomes active.

5. Select an agent policy set from the **Select a Policy Set** list.
6. Click the **Save** icon () to save your changes.

   Step Result: The **Select a Policy Set** list closes and your policy is assigned.

   Note: The **Cancel** icon () cancels your changes and any edits are not saved.

Result: The policy set is saved and associated with the group.

Unassigning an Agent Policy Set from a Group

When desired, you can unassign an Agent Policy Set from a group.

Prerequisites:

An Agent Policy Set is assigned. Refer to Assigning an Agent Policy Set to a Group on page 385 for details.

Unassign the Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 415 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.

3. Select a group from the directory tree.

Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Remove the desired policy sets.
   Use one of the following methods.

Method	Steps
To remove one Agent Policy Set:	Click the **Unassign** icon () associated with the Agent Policy Set you want to remove.
To remove multiple Agent Policy Sets:	1. Select the check boxes associated with the Agent Policy Sets you want to remove. 2. From the toolbar, click the **Unassign** button.

Note: An **Unassign Disabled** icon indicates you cannot remove an inherited Agent Policy Set. Instead, you must change the group policy inheritance setting or remove the inherited policy set from the parent group. Refer to *Policy Inheritance* in Editing Group Settings on page 409 for additional information.

Step Result: A dialog appears, prompting you to acknowledge the removal.

5. Click **OK**.

   Step Result: The selected policy set(s) are removed and the dialog closes.

Result: The Agent Policy Set(s) are no longer associated with the group.

Chapter 12

Using Patch Content

In this chapter:

The term *patch content* encompasses all updates across all endpoints registered to the Ivanti Patch and Remediation Server.

Within Ivanti Patch and Remediation, content consists of:

- The content description.
- Signatures and fingerprints required to determine whether the content is patched or not patched.
- Associated package or packages for performing the patch.

Packages contain all vendor-supplied updates and executable code used to correct or patch security issues.

The following graphic illustrates the relationship between content and packages. Typically, a single content item is shared by multiple endpoints on multiple operating system platforms. There may be a series of separate patches to remediate the same content in different environments. The separate patches are grouped in packages identified by their respective product or OS. As a result, a series of packages may be included for one content item.

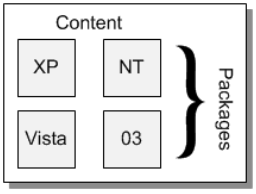


Figure 83: Patch Content and Package relationship

About Patch Content

The various pages pertaining to content display a listing of known vulnerabilities, software updates, and other patch content. Once reported and analyzed, the content is distributed to your Ivanti Endpoint Security server through the Global Subscription Service agent.

The agent installed on each endpoint checks for known content using the Discover Applicable Updates (DAU) task. The DAU runs an inventory scan and sends the results back to the Ivanti Endpoint Security server, which compares it with the list of known content. If the endpoint is found to be missing security items, a deployment can be set up to resolve the issues.

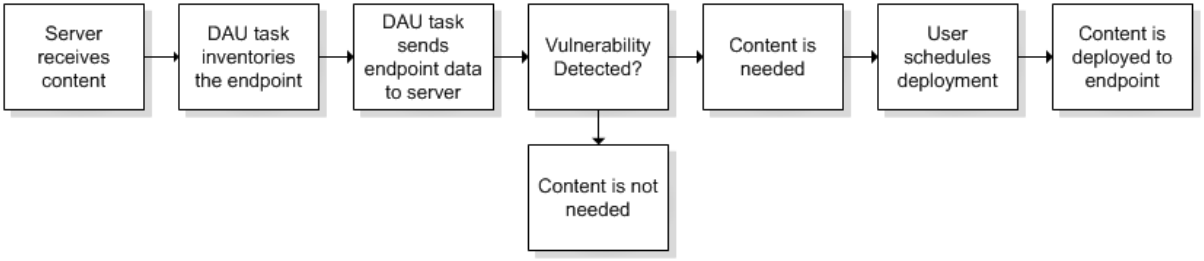


Figure 84: Discover Applicable Updates Task

Defining Content Structure

The structure of a content item allows the ability to create one patch applicable for many different operating systems and software versions. This allows for different packages and signatures capable of identifying the presence of patch files within an endpoint.

As depicted in the following diagram, for each content item you can have more than one signature. For each signature, you can have multiple fingerprints and pre-requisites. However, you can only have one package per signature.

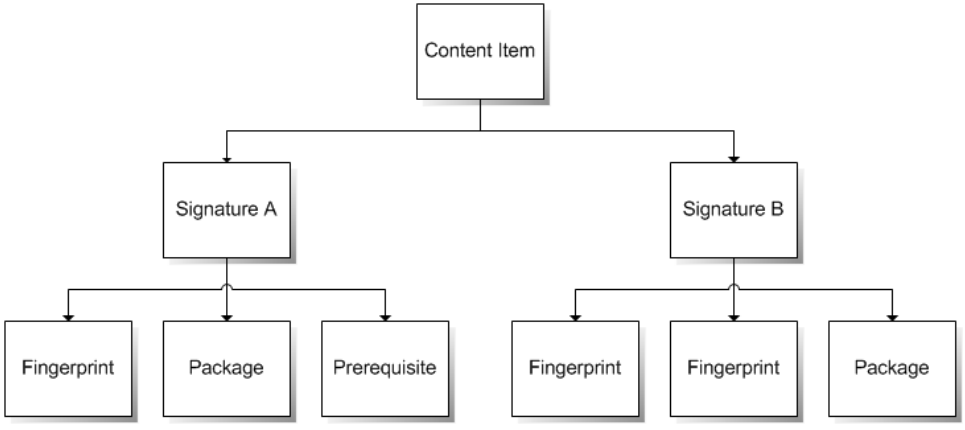


Figure 85: Patch Structure

Content Item

A content item is the container for the entire object. All properties set for the content item are viewed in content pages. Each security content item can have one or more signatures.

Signatures
Signatures recognize specific combinations of installed software in an operating system. Vulnerabilities usually contain multiple signatures to compensate for variances within applications. Frequently, a patch will require different executables, dynamic-link libraries, and switches in order to run or detect the patch within different operating systems.

Fingerprints
A fingerprint can represent a unique file, folder, registry key, or other data value somewhere within a system. Each signature can contain one or more fingerprints detecting if a patch is present in the system.

Pre-requisites
A pre-requisite is a signature belonging to another vulnerability with its own fingerprints.

Adding a pre-requisite to a signature requires the pre-requisite be met before analyzing the signature for the current patch. If that signature's pre-requisite is met, the agent will analyze the fingerprints of the current signature, otherwise they will be ignored and the patch will not be applied to the device.

Packages
The package contains the actual files used to update or install software on the system. Each package contains the script commands for installing the package files or running the executable that installs the patch.

Vulnerabilities

Vulnerabilities are fixes for critical security issues. They are categorized by content type, which indicates the level of need for an endpoint to have the vulnerability deployed and installed.

Vulnerabilities are classified into the following content types:

Critical	Ivanti or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent security updates fall in to this category. The patches for this category are automatically downloaded and stored on your Ivanti Patch and Remediation server.
Critical - 01	Ivanti or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. This patch is older than 30 days and has not been superseded.
Critical - 05	Ivanti or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. This patch has been superseded.

Critical - Intl	An international patch, where Ivanti or the product manufacturer has determined that this patch is critical and should be installed as soon as possible. Most of the recent international security updates fall in to this category. After 30 days international patches in this category will be moved to Critical - 01.

Software Content

Software content consists of content intended to keep software up to date.

You can review software content in the following categories:

Service packs	Collections of software fixes and enhancements that apply to installed software.
Software installers	Installers for third party software.
Updates	Non-critical updates to installed software.

In addition to the categories listed above, you can also view a list of all available software security content.

Other Content

Other content includes items that are not directly related to patching an endpoint or updating software. It is categorized by content type, which indicates the level of need for an endpoint to have the vulnerability deployed and installed.

Other content items are classified into the following content types:

Detection Only	These security content items contain signatures that are common to multiple vulnerabilities. They contain no associated patches and are only used in the detection process.
Informational	These security content items detect a condition that Ivanti or the product manufacturer has determined as informational. If the report has an associated package, you may want to install it at your discretion.
Policies	These security content items apply security policies to an endpoint.
Recommended	Ivanti or the product manufacturer has determined that these content items, while not critical or security related, are useful and should be applied to maintain the health of your endpoints.
Task	These security content items contain tasks which administrators may use to run various detection or deployment tasks across their network.

Virus Removal	This security content items contain packages which administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category.

About Custom Patch Lists

Custom Patch Lists are a Patch and Remediation feature you can use to create lists of patch content useful in your enterprise.

Ivanti Endpoint Security Patch and Remediation has access to a large repository of patch content. Due to the repository size, users can often have difficulty tracking the patch content they are working with.

You can create Custom Patch Lists from either the ***Patch Content*** page or the ***Groups*** page ***Vulnerabilities/Patch Content*** view.

Custom Patch List Usage Tips

- For content that is used frequently in your enterprise, create a Custom Patch List containing commonly used patch content, and maintain it as your enterprise network changes. As endpoints are updated with new hardware and software, you can update the list to include new patches, while removing old, superceded patches.
- For content that will only be deployed once, create a Custom Patch List containing only the patch content needed for that deployment. For example, you can populate a Custom Patch List with only content released on Patch Tuesday, and then use the content list to deploy it. Afterward, you can leave the Custom Patch List unedited, leaving a record or the patch content released and deployed for a month.
- Use Custom Patch Lists to cache patch content from the Global Subscription Service. Caching using a custom list is a good way of downloading a group of patches.
- Use Custom Patch Lists to test new patch content deployments. You deploy custom patch lists to a group of test endpoints before deploying them in a production enviroment.
- Use Custom Patch Lists for reporting purposes. Since these lists contain only patch content relevent in your enterprise, they are a great way to report deployment progress and status.

The Patch Content Page

Within Ivanti Endpoint Security, you can view all vulnerabilities and software available for deployment from the ***Patch Content*** page. This page contains a variety of filters that you can use to view content relevant in your enterprise.

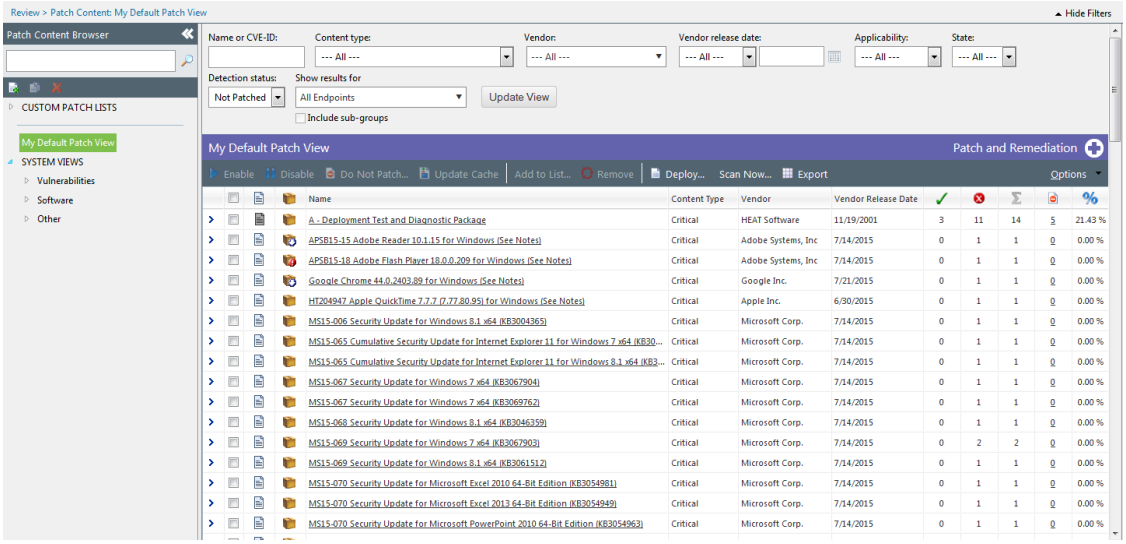


Figure 86: The Patch Content Page

You can open this page by selecting different items from the navigation menu. Depending on the menu cascade you select, the ***Patch Content*** page will open with different filtering options pre-selected. The following table lists all the navigation menu cascades you can select to open the ***Patch Content*** page.

Table 212: Content Page Navigation Menu Items

Menu	Menu Item	Sub-Menu Item
Review	**Vulnerabilities**	**All**
		Critical Vulnerabilities
		New Vulnerabilities
		Top Vulnerabilities
	Software	**All**
		Service Packs
		Software Installers
		Updates

Menu	Menu Item	Sub-Menu Item
	Other	**All**
		Detection Only
		Informational
		Packages
		Policies
		Recommended
		System Management
		Tasks
		Virus Removal

To Access the Content

Review content to see which content items are available and which items you may want to deploy to your managed endpoints.

1. From the **Navigation Menu**, select **Review** > **My Default Patch View**.
2. Choose filter settings to display the content you're looking for.

The Patch Content Browser

From each page that lists patch content, you can use the **Patch Content Browser**, a panel that lists Custom Patch Lists, your default patch view, the system view for each patch category. Use this browser to filter the patch content that is displayed, or use it to create a new custom patch list.

The **Patch Content Browser** is available from all content views selectable from:

- **Review** > **My Default View**.
- Each page selectable from **Review** > **Vulnerabilities**.
- Each page selectable from **Review** > **Software**.
- Each page selectable from **Review** > **Other**.
- The ***Vulnerabilities/Patch Content*** of the ***Groups*** page.

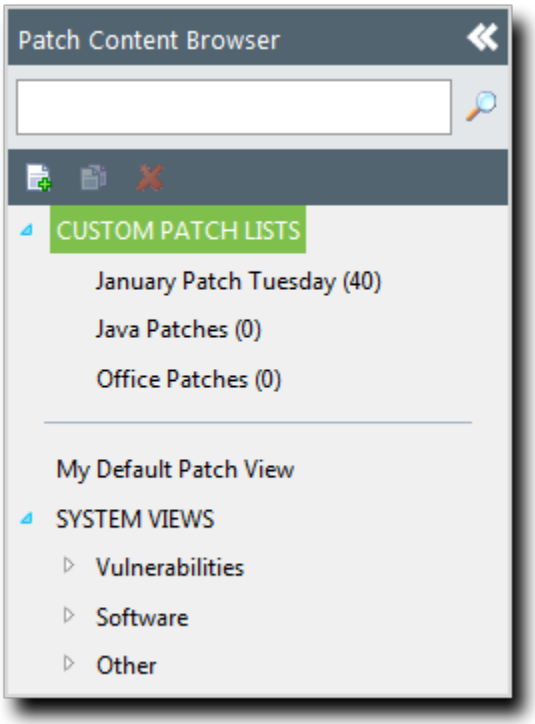


Figure 87: Patch Content Browser

You can interact with the **Patch Content Browser** in multiple ways:

- Display or hide the **Patch Content Browser** by clicking the browser **Chevron** (). However, note that the browser cannot be hidden when using the **Groups** page.
- Type criteria in the field to filter the **Patch Content Browser** for custom patch lists or system views.
- Right-click within **Custom Patch Lists** to create a new custom patch list, copy an existing list, rename an existing list, delete an existing list, or deploy the list content.
- Select a custom patch list from the browser to view the patch content within it. Patch content is displayed on the page list.
- Click the , , or icons to create, copy, or delete Custom Patch Lists. System views cannot be deleted.

The **Patch Content Browser** contains multiple nodes. Selecting each node type changes the content listed on the page.

Table 213: Patch Content Browser Nodes

Branch	Description
CUSTOM PATCH LISTS	Lists all Custom Patch Lists, which are lists of content that include only content items added by a user. For more information, see About Custom Patch Lists on page 463. • Selecting the root **CUSTOM PATCH LISTS** node provides controls in the main panel to create new a Custom Patch List or work with recent lists. • Selecting a list from the **CUSTOM PATCH LISTS** hierarchy displays its contents on screen. • Each list identifies how many content items are added to it using a parenthetical citation.
My Default Patch View	Lists the patch content according to the default filters, sorting, and column order selected by the logged-in user.
SYSTEM VIEWS	Lists the various default Patch and Remediation content views. The **System Views** are common filter combinations you can use to quickly sort patch content. For example, selecting the **Vulnerabilities** system view sets your page filters to **Content type: All Critical**, **Applicability: Applicable**, and **State: Enabled**. • Vulnerabilities are patches that fix security vulnerabilities. • Software installs software, service packs, or other updates. • Other includes patches that don't fit in the previous two categories, such as policy enforcement or virus removal.

The Create Custom Patch List Dialog

You can use this dialog to create *custom patch lists*, which are static lists of patch content items you have selected from the ***Patch Content*** page. You can use custom patch lists to research, recall, deploy, and report on patch content that is commonly used in your enterprise.

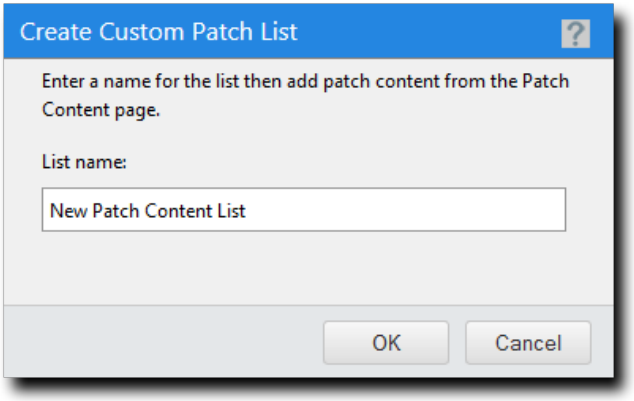


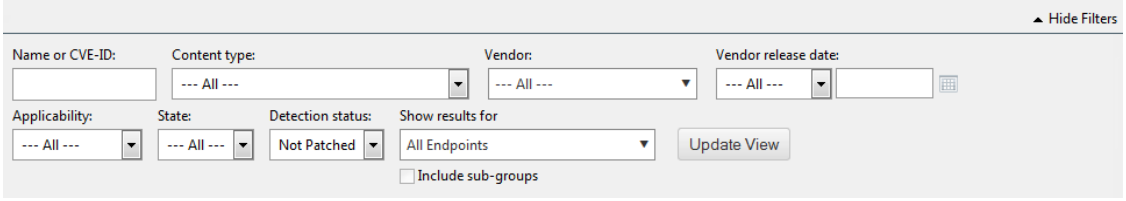
Figure 88: Create Custom Patch List Dialog

- Create a custom patch list by entering a **List name** and clicking **OK**.
- After you a create custom patch list, it is added to the **Patch Content Browser** on the ***Patch Content*** page. The custom patch list is added to the **Custom Patch Lists** hierarchy.
- After creating a custom patch list, you need to add patch content to it afterwards using the **Patch Content Browser**.
- After adding content to your custom patch list, you can deploy it quickly and easily using the **Patch Content Browser**.

Patch Content Filters

When using the ***Patch Content*** page, use the page filters to reduce the list to a manageable scope. This topic describes how each ***Patch Content*** page filter works.

Regardless of the navigation menu selection chosen to open the ***Patch Content*** page, the same filters are always available. You may need to toggle the **Show Filters / Hide Filters** button to display them. All filters can be used in combination with each other.



Filters

Name or CVE-ID	Use this field to filter the page by patch name or a patch's Common Vulnerability and Exposures ID.
Content type	Use this drop-down list to filter the page to a certain content type. See the **Content Types** list below for more info on what content is in each type.
Vendor	Use this drop-down list to filter the page to display content from only certain vendors. All vendors for content replicated from the Global Subscription Service or imported from Ivanti Content Wizard are listed. **Note:** When viewing Custom Patch Lists, only applicable vendors are available for selection.
Vendor release date	Use this drop-down list and field to filter the page for content released after (or before) a date that you define. To define a date, either use the calendar icon to select one, or type the date in a mm/dd/yyyy format.
Applicability	Use this drop-down list to filter the page for content that applies (or doesn't apply) to your enterprise endpoints (or groups).
State	Use this drop-down list to filter the page for content that is in an enabled or disabled state.
Detection status	Use this drop-down list to filter the page for content that has been installed (or hasn't been installed) on endpoints.
Show results for	Use this drop-down list to filter the page for content that applies only to the selected group. Select the **Include sub-groups** to include the group's child groups in the filtering process.

Content Types

The **Content type** filters contains a list of selectable content categories. The list below describes what content is includes in each category.

All	Displays all content available from the Global Subscription Service.
All Critical	Displays all content that Ivanti or the vendor recommends for immediate installation.
Critical (NEW)	Displays all English language content that Ivanti or the vendor recommends for immediate installation that is less than thirty days old. By default, Ivanti Endpoint Security automatically caches content in this category. After 30 days, critical patches are moved to **Critical > 30 Days**.

Critical > 30 Days	Displays all content that Ivanti or the vendor recommends for immediate installation that is more than thirty days old. Most security patches are included in this category.
Critical International (NEW)	Displays all non-English language content that Ivanti or the vendor recommends for immediate installation that is less than thirty days old. Most of the recent international security updates are included in this category. After 30 days, international patches are moved to **Critical > 30 Days**. This filter only returns results if you've used the ***Subscription Service Configuration*** dialog to select new content languages.
Critical and Not Superseded	Displays all content that Ivanti or the vendor recommends for immediate installation. All patches in this category has not been supplanted by newer patches.
Critical but Superseded	Displays all content that Ivanti or the vendor recommends for immediate installation. Content in this category has been supplanted by new content.
Software All	Displays available software. This category combines the **Software**, **Recommended**, and **Informational** types.
Software Installers	Displays available software installers.
Software Updates (Not Critical)	Displays updates to existing software. These patches are not critical to the applicable software's operation.
Not Applicable	Displays content that doesn't apply to your endpoints.
Not Critical	Displays a list of content applicable to your endpoints, but is not critical for security or operations (content listed under **All Critical**, **Critical > 30 Days**, and **Critical and Not Superseded**).
Detection Only	Displays content that contains signatures common in vulnerabilities. This content contains no patches and are only used in the detection process.
Informational	Displays content that detects a condition that Ivanti or the vendor has declared as informational. If the report has an associated package, you may want to install it as your discretion.
Policy	Displays content that impacts policy.
Recommended	Displays content that Ivanti or the vendor recommends installing. The content is not critical or security related, but is useful and should be applied end user convenience.
Tasks	Displays tasks that administrators may use to run various virus detections across their network. Anti-Virus tools and updates are included in this category.

Virus Removal	Displays a list of content that removes viruses and other malware.
Critical & Not Superseded/ Recommended	Displays all content classified as **All Critical** , **Critical and Not Superseded**, and **Recommended**.

The Patch Content Page Toolbar

Each page you can use to deploy content contains a toolbar of common functions.

The following table describes the toolbar functions used in each content page.

Table 214: Content Pages Toolbar Functions

Button	Function
Enable	Enables a selected disabled content item. For additional information, refer to Enabling Content Globally on page 479. **Note:** If no content items are disabled, **Enable** is unavailable.
Disable	Disables a selected enabled content item. For additional information, refer to Disabling Content Globally on page 479.
Do Not Patch...	Disables the selected patch for specific groups and endpoint that you select. For more information, see Disabling Content for Groups/ Endpoints on page 480.
Update Cache	Updates the package cache for the selected content item. For additional information, refer to Updating the Cache on page 485.
Add to List...	Adds content selected from the page list to a Custom Patch List. For additional information, refer to Adding Content to a Custom Patch List on page 485.
Remove	Removes content selected from a Custom Patch List. For additional information, refer to Removing Content from a Custom Patch List on page 487.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Using the Deployment Wizard on page 260.
Scan Now...	Prompts the Discover Applicable Updates task to launch immediately and scan all agent-managed endpoints within your network for vulnerabilities. For additional information, refer to Scanning Endpoints for Vulnerabilities on page 488.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Patch Content Page List

Use the page list to view information about each patch and the deployment information for it.

The following table describes the ***Patch Content*** page list.

Table 215: Column Definitions

Column	Icon	Definition
Status		The content item status, which indicates when the server downloaded the content item metadata. For additional information, refer to Content Status and Type on page 474.
Package Status		The cache status for the content item, which indicates if the server downloaded the content item packages. For additional information, refer to Content Icons and Descriptions on page 475.
Name	N/A	The content item name, which links to the ***Patch Status*** of the item. For additional information, refer to The Patch Status Page on page 489.
Content Type	N/A	Indicates the content item type. For more information, see one of the following topics: • Vulnerabilities on page 461 • Software Content on page 462 • Other Content on page 462
Vendor	N/A	The name of the vendor that created the software in the content item.
Vendor Release Date	N/A	The date and time that the vendor released the software in the content item.

Column	Icon	Definition
Number of endpoints which came up Patched	✓	The number of endpoints patched with the content item.
Number of endpoints which came up Not Patched	⊗	The number of endpoints not patched with the content item.
Total Applicable	Σ	The number of endpoints that the content item applies to.
Number of endpoints which came up Do Not Patch	⊖	The number of endpoints that administrators have created a patch exception for.
Percent Patched	%	The the percentage of applicable endpoints patched with the content item.

Additionally, you can expand each content item by clicking its arrow (**>**). The following table describes each field that displays when you expand a content item.

The following detail information appears on this page.

Table 216: Content Item Field Descriptions

Name	Description
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Associated packages	The number of packages associated with the content item.
Packages status	The cache status for the content item packages.
Ivanti Endpoint Security ID	The Ivanti Endpoint Security identifier for the content item.
Custom Patch Lists	A listing of all Custom Patch Lists that the content item is included in.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The Ivanti Endpoint Security user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor product ID	The identifier given to the security content item by the vendor.

Name	Description
Vendor release date/time (UTC)	The date and time the vendor released the software in the content item.
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Note: The page's **Content Type** filter **Software All** item combines the following **Content Type** filter items into one type:

- **Software**
- **Recommended**
- **Informational**

Content Status and Type
An icon in the **Status** column indicates the status of content items. The menu options and filter criteria that you select determines which content items are displayed. You can set the available filters to display content items of a certain status type.

Table 217: Status and Descriptions

Status	Description
New	Downloaded from the Global Subscription Service since the last session.
Current	Present content items residing on Ivanti Patch and Remediation.
Tasks	System task package.
Local	Locally created package.
Beta	Released to the Ivanti BETA community.

The following table includes descriptions of the security content status icons.

Table 218: Security Content Status Icons and Descriptions

New	Current	Beta	Status Description
			Active content.
			The content has been disabled.

Content Cache Status and Type

A content item may have any number of packages associated with it. A package contains the patch to address the security issue. Each package may be cached (downloaded) from the Global Subscription Service.

The downloading of packages can occur automatically if the security content item impact is rated as critical or if a deployment has been created for a particular package or content item. Selecting the **Package Status** icon displays a list of the individual packages associated with the content item.

Content Icons and Descriptions

An icon in the **Package Status** column indicates the cache status of content items. The menu options and filter criteria that you select determines which content items are displayed. You can set the available filters to display content items of a certain status type.

The content status icons and their status are classified as follows:

Table 219: Security Content Status Icons and Descriptions

New	Current	Tasks	Local	Description
			N/A	The package is not cached.
			N/A	The package has been scheduled to be cached or is in the process of being cached.
			N/A	An error occurred while trying to cache the package.
				The package is cached and ready for deployment.
				The package is currently deploying (animated icon).

New	Current	Tasks	Local	Description
				The package is disabled.

Content Name
The names of content items typically include the vendor (manufacturer of the content item) and specific application and version information.

Working With Content

There are several tasks designed to assist with management and deployment of content items. These are available from buttons located within the toolbar on the **Review** pages for the individual content types.

These tasks include:

- Creating Custom Patch Lists on page 476
- Copying Custom Patch Lists on page 477
- Deleting Custom Patch Lists on page 477
- Disabling Content on page 477
- Updating the Cache on page 485
- Disabling Content for Groups/Endpoints on page 480
- Enabling Patches for Groups/Endpoints on page 484
- Adding Content to a Custom Patch List on page 485
- Removing Content from a Custom Patch List on page 487
- Deploying from the Patch Content Page on page 487
- Scanning Endpoints for Vulnerabilities on page 488
- Exporting Content Data on page 488

Creating Custom Patch Lists

When you need to research, recall, deploy, or report on a set of patch content that you use regularly in your enterprise, you should create a *Custom Patch List*, which is static list of patch content items that you select from ***Patch Content*** page. The content in this list will not change based on applicability or changes in content type.

Create new custom patch lists using the ***Create Custom Patch List*** dialog, which can be opened using the navigation menu or the **Patch Content** browser.

1. From the **Navigation Menu**, select **Review** > **Custom Patch Lists** > **Create Custom Patch List**.

2. Type a new **List name** and click **OK**.

   Step Result: The ***Patch Content*** page opens, and your new Custom Patch List is added to the **Patch Content Browser** within the **Custom Patch Lists** hierarchy.

Copying Custom Patch Lists

You can copy existing Custom Patch Lists and use them as templates for other Custom Patch Lists.

Copy Custom Patch Lists from the ***Patch Content*** page.

1. From the **Navigation Menu**, select **Review** > **My Default Patch View**.
2. From the **Patch Content Browser**, expand **Custom Patch Lists** and select the list you want to copy.
3. Click .
4. [Optional] Type a new name for the copied list and press **ENTER**.

Result: A new Custom Patch List is added to **Patch Content Browser**. Edit the new list so that it fills a new enterprise role.

Deleting Custom Patch Lists

When you no longer need a **Custom Patch List**, delete it from the **Patch Content Browser**.

Delete **Custom Patch Lists** from the ***Patch Content*** page.

1. From the **Navigation Menu**, select **Review** > **My Default Patch View**.
2. From the **Patch Content Browser**, expand **Custom Patch Lists** and select the list you want to delete.
3. Click . Click **OK** to confirm.

Disabling Content

All content downloaded from the Global Subscription Service can be toggled between disabled and enabled states. You can disable content either globally or per endpoint.

Disabling Content Globally

Disable content globally when you don't want it to be installed on *any* endpoint in your network. Globally disabling content prevents it from being deployed mistakenly. Globally disabled content can be re-enabled at any time.

Disabling Content by Groups or Endpoints (also known as *Do Not Patch*)

Using the *Do Not Patch* feature, you can disable content for groups or endpoints that you choose. Use *Do Not Patch* when a particular patch is causing problems, or would cause known problems, for a group or endpoint. Content disabled by endpoint/group can also be re-enabled at any time.

You should know a few things about *Do Not Patch*:

- *Do Not Patch* is considered a special patch state.
  - The *Do Not Patch* state takes precedence over all other patch states, such as *patched*, *not patched*, and *not applicable*.
  - Content marked *Do Not Patch* is considered a special state different from *disabled* since it can still be deployed to most of your endpoints.

    Note: If you need find content marked *Do Not Patch* when filtering list pages or reports, clear all page filters and sort by the **Do Not Patch** column ( ).
  - Patches marked *Do Not Patch* exclude selected endpoints from its patch compliance score.
- If you mark content as *Do Not Patch* after it has already been installed on the endpoints you select:
  - The endpoints still enters a *Do Not Patch* state although the patch is installed.
  - You must uninstall the patch manually from those endpoints (because patches cannot be retroactively uninstalled). The *Do Not Patch* feature *does not* uninstall patches from endpoints.
- If you mark content as *Do Not Patch* for a group, that group's child hierarchy is also considered *Do Not Patch*.
- If you mark content included in a mandatory baseline as *Do Not Patch*, the endpoints or groups marked *Do Not Patch* are exempt from that patch.

***Do Not Patch* use example:**

Say your organization has mission-critical servers that require an older version of Java to operate. Although you should patch most of your endpoints with the latest version to secure them, these mission-critical servers need to remain on the older version to continue operations. In this case, mark the mission-critical servers as *Do Not Patch* to exempt them from a more recent version of Java.

Disabled/Enable Comments

When disabling/enabling content, you have the option of entering a reason for completing the action.

- A disable comment is useful for tracking why a content item is disabled. The default reasons include:
  - OS / System conflict
  - Application conflict
  - High incidence of installation failures
  - Not approved
- Typically, content is re-enabled when the reason for originally disabling it is resolved. Use re-enable comments to track why content has been reintroduced. The default enable reasons are:
  - Resolved OS / System conflict
  - Resolved application conflict
  - Resolved installation failures
  - Approved

Tip: Disable/enable comments also appear in related reports.

Disable/Enable Tips and Behaviors

- After a patch is disabled/re-enabled, you can edit the reason by expanding the patch's metadata from the ***Patch Content*** page list and clicking the Enable/Disable reason **Edit** link.
- If you disable a patch that's cached, it isn't updated if a new version of the patch is released.
- You can't retroactively remove a patch from a deployment that's scheduled or in-progress by disabling the patch. If you schedule a deployment but then globally disable a patch that's included, that patch is still deployed. If you need to stop the patch from being deployed, abort the deployment instead of disabling the patch.

Disabling Content Globally

Disabling a patch prevents it from being deployed.

1. From the **Navigation Menu**, select **Review** > **My Default Patch View**.
2. Filter the page to show content that's enabled.
   a) If necessary, click **Show Filters** to toggle the page filters.
   b) Select page filters. Make sure the **State** filter has **Enabled** selected.
   c) Click **Update View**.
3. Find and select the content you want to disable.
4. Click **Disable**.

   Note: If you disable a content item that's already been cached, the package will not be updated if a new version of the content item is released.

5. [Optional] Choose a reason for disabling the content.
   - To enter a new reason, type it in the field.
   - To choose a reason that's already been used, select it from the drop-down menu.
6. Click **Disable**.

   Note: You can't retroactively remove a patch from a deployment that's scheduled or in-progress by disabling the patch. If you schedule a deployment but then globally disable a patch that's included, that patch is still deployed. If you need to stop the patch from being deployed, abort the deployment instead of disabling the patch.

Result: The content is disabled. To confirm, filter the page to display disabled content and confirm it's listed.

Enabling Content Globally

Enabling a previously disabled content item allows you to deploy the content item to your endpoints.

1. From the **Navigation Menu**, select **Review** > **My Default Patch View**.
2. Filter the page to show content that's disabled.
   a) If necessary, click **Show Filters** to toggle the page filters.

b) Select page filters. Make sure the **State** filter has **Disabled** selected. Select the **Content type** filter **All** value to make sure all disabled content is displayed.
c) Click **Update View**.

3. Find and select the content you want to enable.
4. Click **Enable**.
5. [Optional] Choose a reason for disabling the content.
   - To enter a new reason, type it in the field.
   - To choose a reason that's already been used, select it from the drop-down menu.
6. Click **Enable**.

Result: The content is re-enabled.

Disabling Content for Groups/Endpoints

You can disable patches for specific groups and endpoints, placing them in a *do not patch* state for that patch.

1. Open a page that list patches ***Patch Content*** page.
   - Select **Review** > **My Default Patch View**, or any other **Review** menu item to open the ***Patch Content*** page.
   - Select **Manage** > **Endpoints**, click an endpoint link, and then select the **Vulnerabilities/Patch Content** tab.
   - Select **Manage** > **Groups** and select the **Vulnerabilities/Patch Content** view.
2. [Optional] Use the ***Patch Content*** page filters and click **Update View** to find patches that you want to disable for a group/endpoint.

   Tip: If the filters are not displayed, click **Show Filters**.
3. Select the patch you want to disable, and then click **Do Not Patch**.
4. Complete the ***Do Not Patch Groups and Endpoints*** wizard.

The Do Not Patch Groups and Endpoints Wizard

Use this wizard to mark the patch you've selected as "do not patch" for groups and endpoints that you choose. This wizard includes two to three pages, depending on the actions you choose while using it:

Select Groups and Endpoints to Mark as 'Do Not Patch' on page 481	Use this page to exclude specific groups and endpoints from receiving the patch.
Do Not Patch Reason on page 483	Use this page to record a reason why you're marking the patch as 'Do Not Patch'. You can see this record later to remind yourself why the patch is excluded.

OK to Patch Reason on page 484	If you're removing the patch exclusion for particular groups or endpoints later, you can also provide a reason on why you're marking it 'OK to Patch'.

Select Groups and Endpoints to Mark as 'Do Not Patch'
After opening the ***Do Not Patch Groups and Endpoints*** wizard, select groups, endpoints, or a combination of both. These endpoints (and groups) won't allow the patch that you selected to be applied to them when the wizard is completed.

From this page, you can either:

- Create a patch exception for groups, endpoints, or a combination of both by adding them to the **Do Not Patch** list.
- Remove existing patch exceptions for groups or endpoints (after resolving the reason that an exception was created).

When you're done modifying the **Do Not Patch** list, click **Add Reason** to proceed.

Adding Groups and Endpoints to the 'Do Not Patch' List

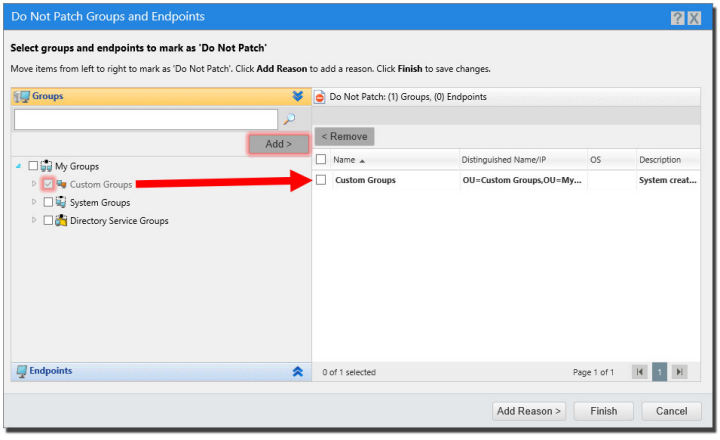


Figure 89: Add Group/Endpoint to Do Not Patch List

Add groups or endpoints to the **Do Not Patch** list when:

- You're creating a brand new patch exception.
- You're adding more groups/endpoints to the **Do Not Patch** list when exceptions for the patch already exist.

Toggle between groups and endpoints by clicking the **Groups** and **Endpoints** headers.

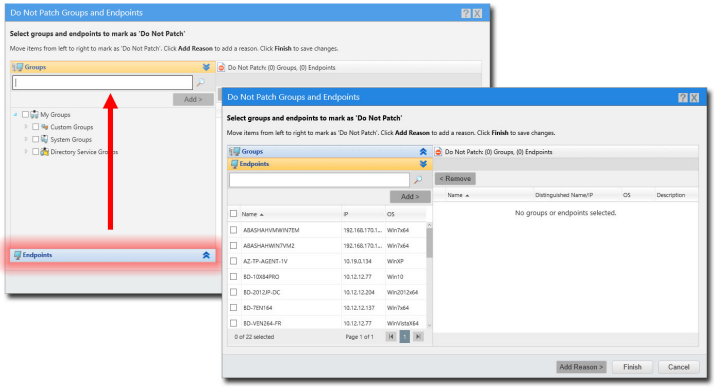


Figure 90: Toggle Group/Endpoint

Groups Panel

Use this panel to create a patch exception for a group.

- Expand the tree to find the groups you want to select.
- You can also type specific group names into the search field.

Endpoints Panel

Use this panel to search for specific endpoints that you want to select.

Removing Groups and Endpoints from the 'Do Not Patch' List

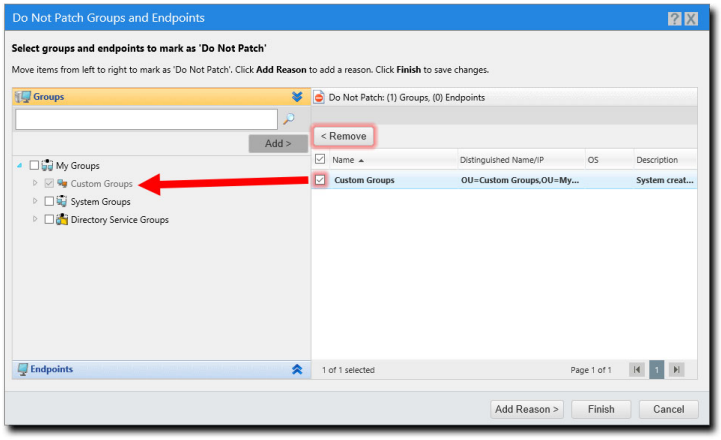


Figure 91: Remove Group/Endpoint

Remove groups or endpoints from the **Do Not Patch** list when you've resolved the reason that you created an exception in the first place.

Tip: You may never want to remove groups/endpoints from the **Do Not Patch** list.

Do Not Patch Reason

When you add groups/endpoints to the **Do Not Patch** list for a patch, you should select a **Do Not Patch** reason. These optional reasons are available for tracking and reporting purposes.

For example, while reviewing reports about networking patching, you can reference this reason for info on why an endpoint wasn't patched.

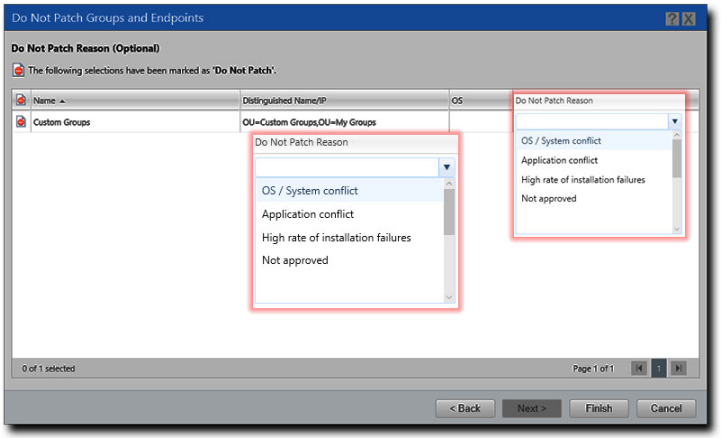


Figure 92: Do Not Patch Reasons

A **Do Not Patch Reason** drop-down is available for each group/endpoint on the **Do Not Patch** list.

- To select from a list of pre-created system reasons, select one from a group/endpoint drop-down.
- To create your own custom reason, type a reason instead.

Note: If you aren't adding groups/endpoints to the **Do Not Patch** list, this page won't appear.

OK to Patch Reason

When you remove groups and endpoints from the **Do Not Patch** list for a patch, you should select an **OK to Patch** reason. These optional reasons are available for tracking and reporting purposes.

For example, if your manager asks why a patch that was marked as **Do Not Patch** is later changed to **OK to Patch**, you can reference this reason to find out why the patch was approved.

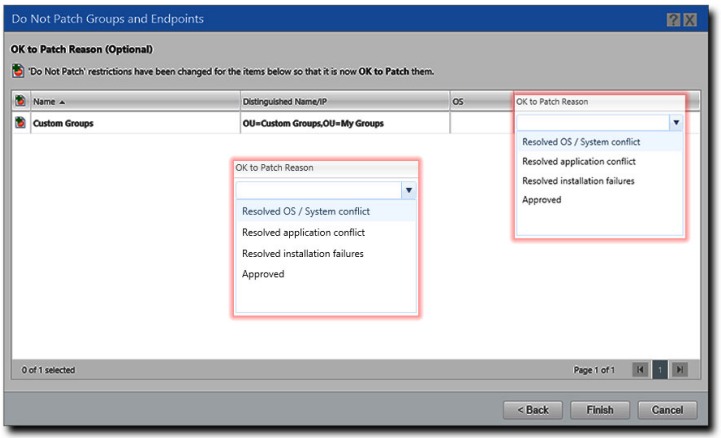


Figure 93: OK to Patch Reasons

A **OK to Patch Reason** drop-down is available for each group/endpoint removed from the **Do Not Patch** list.

- To select from a list of pre-created system reasons, select one from a group/endpoint drop-down.
- To create your own custom reason, type a reason instead.

Note: If you aren't removing groups/endpoints from the **Do Not Patch** list, this screen won't appear.

Enabling Patches for Groups/Endpoints

After you've resolved the reason that you've marked a group or endpoint as "Do Not Patch," you can go back and re-enable it.

1. Open a page that list patches ***Patch Content*** page.
   - Select **Review** > **My Default Patch View**, or any other **Review** menu item to open the ***Patch Content*** page.
   - Select **Manage** > **Endpoints**, click an endpoint link, and then select the **Vulnerabilities/Patch Content** tab.
   - Select **Manage** > **Groups** and select the **Vulnerabilities/Patch Content** view.
2. [Optional] Use the ***Patch Content*** page filters and click **Update View** to find patches that you want to enable for a group/endpoint.

   Tip: If the filters are not displayed, click **Show Filters**.
3. Select the patch you want to enable, and then click **Do Not Patch**.

4. Complete the ***Do Not Patch Groups and Endpoints*** wizard. From the ***Select Group and Endpoints to Mark as 'Do Not Patch'*** page, remove the groups/endpoints that you want to patch again from the **Do Not Patch** list.

Updating the Cache

Updating the cache initiates a process that gathers the packages associated with the selected vulnerability and copies those packages to your Ivanti Patch and Remediation server.

Within **Review** pages, the **Update Cache** feature is designed to assist with the management and deployment of content items.

Note: For optimum installation order, Ivanti recommends caching content prior to deployment. Failure to cache content prior to deployment may result in repeated endpoint reboots that interrupt workflow on those endpoints.

1. From the **Navigation Menu**, select **Review** > **My Default Patch View**.
2. If necessary, select filter criteria for to find content you're looking for and click **Update View**.
3. Select the check boxes associated with the content to cache.
4. Click **Update Cache**.

   Step Result: The ***Warning*** dialog box opens, informing you that the update request and this action may take an extended period of time.

   Note: The cache will not be updated for disabled content items that have had a new version released.

5. Click **OK**.

Result: The selected content begins caching.

Adding Content to a Custom Patch List

After you have created a Custom Patch List, you need to add patch content to it, which you then use for deployments and record keeping.

You can begin adding content to a Custom Patch List from the ***Patch Content*** page.

Tip: You can also create a new Custom Patch List after selecting content.

1. From the **Navigation Menu**, select **Review** > **My Default Patch View**.

2. Open the ***Patch Content*** page.
   - Select **Review** > **My default patch view**, or any other **Review** menu item that opens the ***Patch Content*** page.
   - Select **Manage** > **Groups** and select the **Vulnerabilities/Patch Content** view.

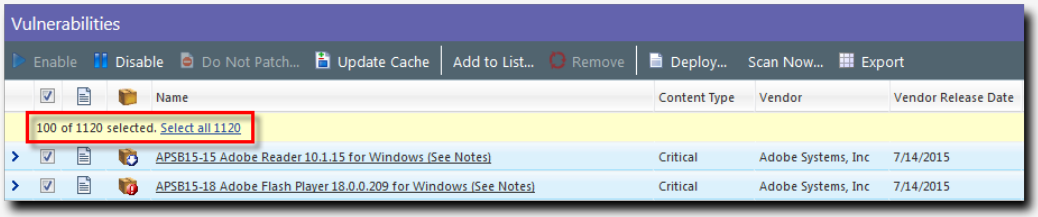
Tip: You can also initiate this task from the Navigation Menu by selecting **Review** > **Custom Patch Lists** > ***Target Patch List*** or **Manage** > **Custom Patch Lists** > ***Target Patch List***.

3. [Optional] Use the ***Patch Content*** page filters and click **Update View** to find specific content you want to add to the list.

Tip: If the filters are not displayed, click **Show Filters**.

4. Select the content items you want, and then click **Add to List**.

Note: If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.

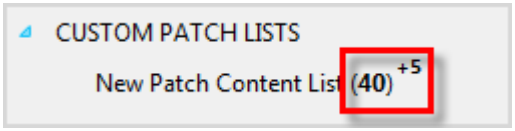


Step Result: The ***Add to List*** dialog opens.

5. Add the selected content items to a Custom Patch List.
   - To add the patch content to an existing Custom Patch List, select an existing **List name**.
   - To add the patch content to a new Custom Patch List, type a *new* **List name**.

6. Click **Add**.

Result:
- The ***Add to List*** dialog closes.
- If you typed a new **List name**, a new Custom Patch List is added to the **Patch Content Browser**.
- The content you selected is added to the Custom Patch List.



Removing Content from a Custom Patch List

If you have mistakenly added a patch content item to one of your Custom Patch Lists, remove it.

Remove patch content from a Custom Patch List using the ***Patch Content*** page toolbar.

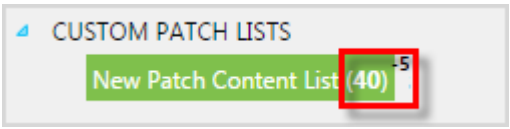
1. From the Navigation Menu, select the Custom Patch List you want to remove content from.

   Example: Select **Review** > **Custom Patch Lists** > **Custom Patch List Name**.

   Note: If you have more than five Custom Patch Lists, select **Review** > **All Lists** and use the **Patch Content Browser** to select a Custom Patch List.

2. Select the content items you want, and then click **Remove**.
3. If prompted, click **OK** to confirm the removal.

Result: The content you selected is removed from the Custom Patch List.



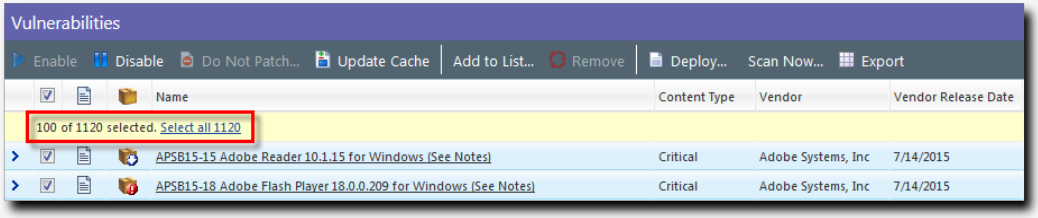
Deploying from the Patch Content Page

Within Ivanti Endpoint Security, content can be deployed from a number of pages, including any ***Content*** page. When deploying from these pages, the ***Deployment Wizard*** is preconfigured according to the content you select.

For additional information, refer to About Deployments on page 243.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. From the list, select the content you want to deploy.

   Note: If you select the **Select All** checkbox, all content visible on the page is selected. However, you can select all available content by clicking the **Select All** link.



3. Click **Deploy**.

Result: The ***Deployment Wizard*** opens, preconfigured to deploy the selected content.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Scanning Endpoints for Vulnerabilities

You can initiate a Discover Applicable Updates (DAU) task at any time. When you initiate this task, the agent scans its host endpoint for vulnerabilities and inventory. Scan results are then uploaded to Ivanti Endpoint Security, which you can view.

From the ***Content*** pages, you can schedule a DAU tasks for all managed endpoints in your network.

Note: With the AntiVirus module installed, you can launch two types of scans. The toolbar **Scan Now...** menu contains commands for the following scan types:

- A Discover Applicable Updates (DAU) task. This scan takes an endpoint hardware and vulnerability inventory. For additional information, refer to
- A virus and malware scan. This targets selected endpoints with an immediate (*on-demand*) virus scan. For additional information, refer to Using the Virus and Malware Scan Wizard.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Scan Now**.

   Step Result: The ***Scan Now*** dialog opens.
3. Select the **Yes, scan all endpoints**.
4. Click **Schedule**.

   Step Result: A notification displays, informing you that the scan has been scheduled. The notification contains a link to view the scheduled deployment.

   Note: Although the DAU task is scheduled for immediate execution, it does not execute until the next agent check in.
5. Click **Close**.

Result: The dialog closes.

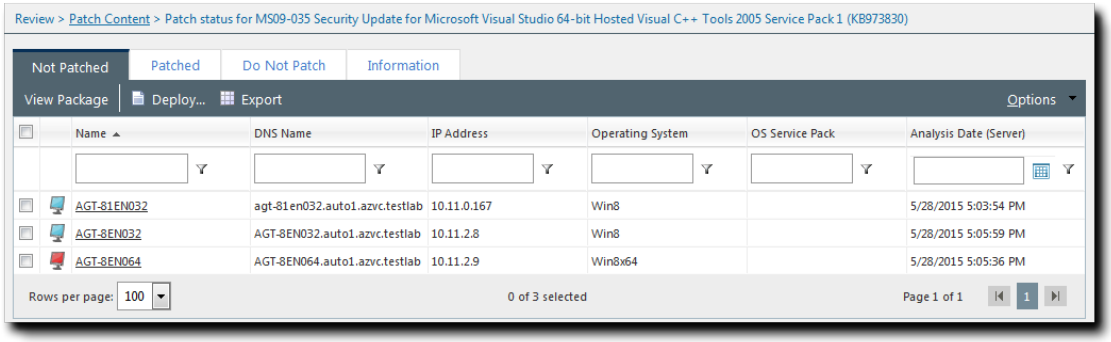
Exporting Content Data

From the various content pages, you can export all information listed on the page to a comma separated value (`.csv`) file. The exported information can be used for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 47.

The Patch Status Page

Each patch features a page that lists statistics and details about itself: the ***Patch Status*** page.



This page is divided into four tabs:

Not Patched	This tab lists each endpoint that the patch applies to. However, the patch is not installed on these endpoints yet. View this page to find out which endpoints you still need to patch for a vulnerability.
Patched	This tab lists each endpoint that the patch is installed on. You can view this page after a deployment to confirm that your endpoints are patched.
Do Not Patch	This tab lists each endpoint marked as *Do Not Patch* for a given patch (*Do Not Patch* means the patch is exempt from being installed on the endpoint). If you determine that an endpoint shouldn't have a certain patch installed, check this tab to see if the endpoint is already marked *Do Not Patch*.
Information	This tab lists metadata about the patch itself.

Viewing Content Patch Statuses

You can view details of a specific content item by selecting the desired content item and clicking the item name.

View a content item's patch status by clicking a content item's hyperlink from a content page list. The ***Patch Status*** page represents the results of the content item analysis and displays detailed data regarding the content item.

1. From the **Navigation Menu**, select **Review** > **Vulnerabilities** > **--- All ---** (or any of the other vulnerability options).
2. Select a content item from the list. You can only view the details of one content item at a time.

3. Click the content item's name.

Result: The ***Patch Status*** page for the selected content item opens.

The Not Patched Tab

This tab lists each endpoint that the patch applies to. However, the patch is not installed on these endpoints yet. View this page to find out which endpoints you still need to patch for a vulnerability.

The Not Patched Tab Toolbar

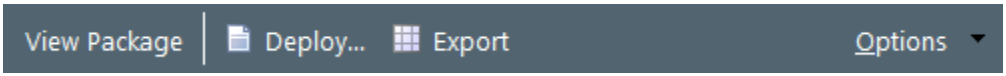


Table 220: Not Patched Tab Toolbar

Button	Description
View Package	Opens the ***Packages*** page and displays the package for the applicable content item.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Using the Deployment Wizard on page 260.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Not Patched Tab List

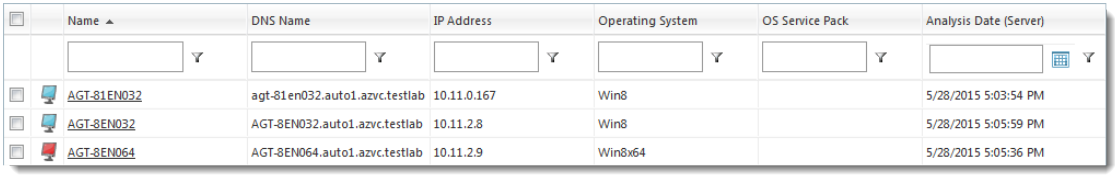


Table 221: Not Patched Tab List

Column	Description
Name	The name of the endpoint. Click the link to view its details.
DNS Name	The domain name system for the endpoint.

Column	Description
IP Address	The IP address of the endpoint.
Operating System	The operating system that the endpoint uses.
OS Service Pack	The service pack applied to the operating system (if one is installed).
Analysis Date	The last date and time that the endpoint was scanned for the patch.

The Patched Tab

This tab lists each endpoint that the patch is installed on. You can view this page after a deployment to confirm that your endpoints are patched.

The Patched Tab Toolbar

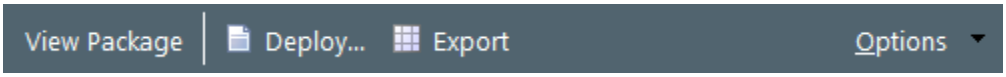


Table 222: Patched Tab Toolbar

Button	Description
View Package	Opens the ***Packages*** page and displays the package for the applicable content item.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Using the Deployment Wizard on page 260.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Patched Tab List

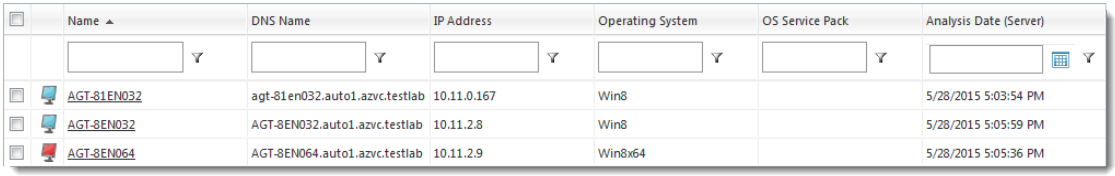


Table 223: Patched Tab List

Column	Description
Name	The name of the endpoint. Click the link to view its details.
DNS Name	The domain name system for the endpoint.
IP Address	The IP address of the endpoint.
Operating System	The operating system that the endpoint uses.
OS Service Pack	The service pack applied to the operating system (if one is installed).
Analysis Date	The last date and time that the endpoint was scanned for the patch.

The Do Not Patch Tab

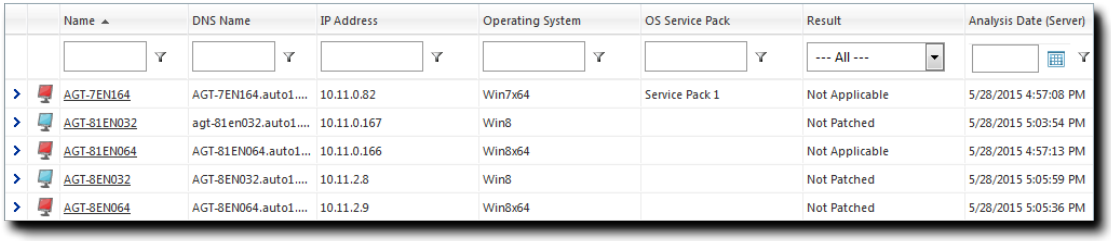
This tab lists each endpoint marked as *Do Not Patch* for a given patch (*Do Not Patch* means the patch is exempt from being installed on the endpoint). If you determine that an endpoint shouldn't have a certain patch installed, check this tab to see if the endpoint is already marked *Do Not Patch*.

The Do Not Patch Tab Toolbar

Table 224: Do Not Patch Toolbar

Button	Description
Do Not Patch...	Disables the selected patch for specific groups and endpoint that you select. For more information, see Disabling Content for Groups/Endpoints on page 480.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Do Not Patch Tab List



	Name	DNS Name	IP Address	Operating System	OS Service Pack	Result	Analysis Date (Server)
						--- All ---	
	AGT-7EN164	AGT-7EN164.auto1....	10.11.0.82	Win7x64	Service Pack 1	Not Applicable	5/28/2015 4:57:08 PM
	AGT-81EN032	agt-81en032.auto1....	10.11.0.167	Win8		Not Patched	5/28/2015 5:03:54 PM
	AGT-81EN064	AGT-81EN064.auto1...	10.11.0.166	Win8x64		Not Applicable	5/28/2015 4:57:13 PM
	AGT-8EN032	AGT-8EN032.auto1....	10.11.2.8	Win8		Not Patched	5/28/2015 5:05:59 PM
	AGT-8EN064	AGT-8EN064.auto1....	10.11.2.9	Win8x64		Not Patched	5/28/2015 5:05:36 PM

Table 225: Do Not Patch Tab List

Column	Description
Name	The name of the endpoint. Click the link to view its details.
DNS Name	The domain name system for the endpoint.
IP Address	The IP address of the endpoint.
Operating System	The operating system that the endpoint uses.
OS Service Pack	The service pack applied to the operating system (if one is installed).

Result	Indicates if the patch is installed on the endpoint.
	• In most cases, the result is either **Not Applicable** or **Not Patched** (since it's the ***Do Not Patch*** tab after all.)
	• In some rare cases, the result may be **Patched**. This result indicates either:
	  • The patch was installed *before* the patch was marked *Do Not Patch* for the endpoint.
	  • The patch was installed manually by an end user.

Analysis Date	The last date and time that the endpoint was scanned for the patch.

Each endpoint in the list can be expanded to show more detail about how it was assigned a patch exception. Expanding an endpoint shows whether it was assigned the patch exception directly or through group inheritance.

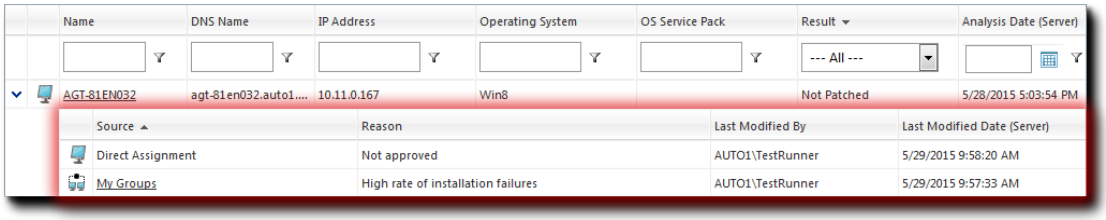


Table 226: Do Not Patch Tab List - Expanded Endpoint

Column	Description
Source	The source from which the endpoint inherited its *Do Not Patch* state. • Endpoints directly placed in a *Do Not Patch* state have a Source of **Direct Assignment**. • Endpoints that inherit their *Do Not Patch* state from a group list the source group. • Endpoints can have multiple *Do Not Patch* sources.
Reason	The last reason that Ivanti Endpoint Security user defined when granting a group or endpoint a patch exception.
Last Modified By	The user who last edited the group or endpoint *Do Not Patch* state
Last Modified Date (Server)	The server date and time that the group or endpoint *Do Not Patch* state was modified.

The Information Tab

The ***Information*** tab, unlike other ***Patch Content Details*** page tabs, features no list. Rather, it features reference information for the applicable content item.

The Information Tab

This tab lists metadata about the patch itself.

The Information Tab Buttons

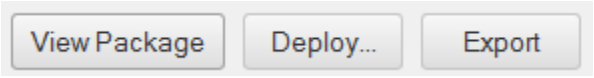


Table 227: Information Tab Buttons

Button	Description
View Package	Opens the ***Packages*** page and displays the package for the applicable content item.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Using the Deployment Wizard on page 260.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47.
	Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Information Tab List

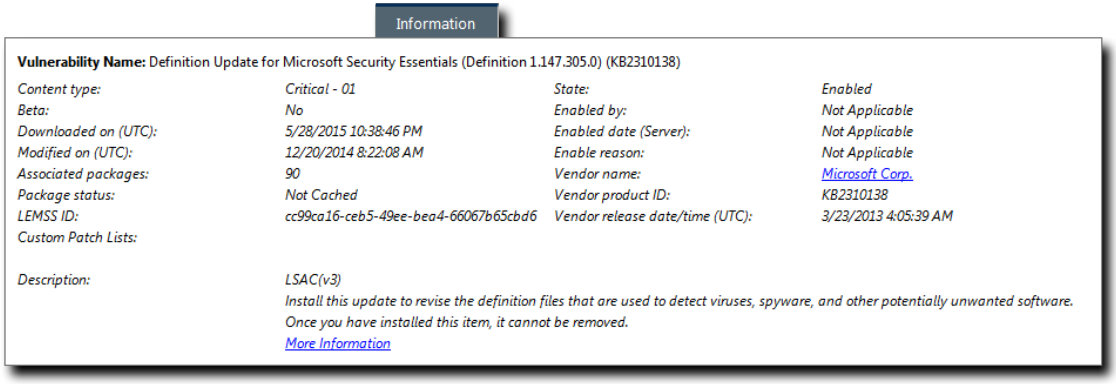


Table 228: List Text Descriptions

Name	Description
Vulnerability Name	The name of the content item.
Content Type	The content item type.
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Modified on (UTC)	The date and time the content item was last modified.
Associated packages	The number of packages associated with the content item.
Packages status	The cache status for the content item packages.
Ivanti Endpoint Security ID	The Ivanti Endpoint Security identifier for the content item.
Custom Patch Lists	A listing of all Custom Patch Lists that the content item is included in.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The Ivanti Endpoint Security user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor name	The name of the content item vendor.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/ time (UTC)	The date and time the vendor released the software in the content item.

Name	Description
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Information
This section displays information about the applicable content item.

Table 229: Content Item Field Descriptions

Name	Description
Vulnerability Name	The name of the content item.
Content Type	The content item type.
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Modified on (UTC)	The date and time the content item was last modified.
Associated packages	The number of packages associated with the content item.
Packages status	The cache status for the content item packages.
Ivanti Endpoint Security ID	The Ivanti Endpoint Security identifier for the content item.
Custom Patch Lists	A listing of all Custom Patch Lists that the content item is included in.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The Ivanti Endpoint Security user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.

Name	Description
Vendor name	The name of the content item vendor.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/ time (UTC)	The date and time the vendor released the software in the content item.
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Working with Content Items

From the ***Patch Status*** page, you can perform tasks related to a specific content item.

From the different page tabs, you can perform the following tasks:

- View Packages on page 498
- Deploying Content on page 499
- Exporting Content Item Data on page 499

View Packages

While viewing the ***Patch Status*** page for a content item, you can immediately view that content item's page.

Perform this tasks from any ***Patch Status*** page tab.

1. Select the desired tab:
   - ***Not Patched***
   - ***Patched***
   - ***Error***
   - ***Detecting***
   - ***Information***

2. Click **View Package**.

Result: The ***Packages*** page opens, displaying the package for the applicable content item.

Deploying Content

Deploying content items to endpoints is a key function of the Ivanti Patch and Remediation module.

Deployments are initiated by clicking **Deploy...** and completing the ***Deployment Wizard***. The ***Deployment Wizard*** provides step-by-step instructions for defining and distributing security content items to the protected endpoints in the network. For additional information, refer to Working With Deployments and Tasks on page 253.

Exporting Content Item Data

When viewing the ***Patch Status*** page, you can export the all data displayed for the selected tab to a comma separated value (`.csv`) file.

For additional information, refer to Exporting Data on page 47.

Chapter 13

Managing Packages

In this chapter:

Packages contain the actual files used to update or install software on the system. Each package contains the script commands for installing the package files or running the executable that installs the patch.

Packages can run tasks, scripts, install software applications, send files to a specified location, and change the configuration of an application or service.

About Packages

Packages contain all vendor-supplied updates and executable code used to correct or patch security issues. The ***Packages*** page displays a listing of known vulnerabilities, software updates, and other patches.

The Packages Page

You can expand a package's listing on the ***Package*** page to view its details.

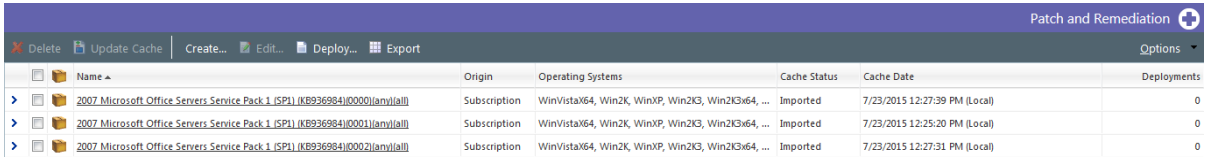


Figure 94: Packages Page

Viewing Packages

The Packages page lists packages by package name. You can expand the page to view package details.

1. Select **Review** > **Other** > **Packages** from the navigation menu.

2. If needed, select filter criteria from the available fields and click **Update View**.

Result: The system displays the existing package list in the ***Packages*** page.

The Packages Page Toolbar

The toolbar on the ***Packages*** page contains buttons that initiate the tasks that you can perform on packages.

The following table describes each toolbar button.

Table 230: Packages Page Buttons and Descriptions

Button	Description
Delete	Deletes the package. For more information, refer to Deleting a Package on page 506.
Update Cache	Sends a request to the Global Subscription Service to get the latest version of the package. For more information, refer to Updating the Package Cache on page 507.
Create...	Opens the ***Package Editor Wizard***, allowing you to create custom packages. For more information, refer to Using the Package Editor on page 515.
Edit	Opens the ***Package Editor Wizard***, allowing you to edit custom packages. For more information, refer to Editing a Package on page 507.
Deploy...	Opens the ***Deployment Wizard***, allowing you to deploy content to managed endpoints. For more information, refer to Working With Deployments and Tasks on page 253.
Export	Opens a ***File Download*** dialog, allowing you to view package details or save them in a comma-separated value (.csv) format. For more information, refer to Exporting Data on page 47.
Options	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Packages Page List

The ***Package*** page list contains identification, origin, operating system, and associated deployment information.

The following table describes the column definitions on the ***Packages*** page.

Table 231: Package Column Definitions

Column	Icon	Definition
Package Status		Indicates the content item package status. For additional information, refer to Content Icons and Descriptions on page 475.
Name	N/A	Name includes vendor, application, and version information.
Origin	N/A	The origin of the task or which company created the package.
Operating Systems	N/A	The platforms that are supported by the package.
Cache Status	N/A	Indicates if the package is cached (`Imported`), in progress (`Pending`), not cached or in progress (column entry is blank).
Cache Date	N/A	The date on which the package cache was updated most recently.
Deployments	N/A	The number of times the package has been deployed.

Additionally, you can expand each package by clicking the **rotating chevron** (**>**). The following table describes each field that displays when you expand a package.

Table 232: Package Field Descriptions

Field	Description
Package Name	Title of the package.
Origin	Point of origin of the package. An origin of Subscription refers to packages downloaded from the Global Subscription Service.
Status	The current status of the package, stating if the package is enabled and ready to be requested from the Global Subscription Service.
Cache Status	The current cache status of the package. A package is considered cached when it has been downloaded from the Global Subscription Service and actually resides on the local server.
Cache Request Status	Indicates if the package has been requested from the Global Subscription Service.

Field	Description
Deployment Availability	Indicates if the package is available for deployment.
OS Platforms	The operating systems and platforms that the package supports and may be deployed to.
Created By Username	The user who created the package. Packages created by Ivanti may have a value of Patchlink Corp. in this field.
Created On	The date and time the package was created.
Last Modified By Username	The user who last modified the package. Packages created by Ivanti may have a value of Patchlink Corp. in this field.
Last Modified On	The date and time of the last change to the package.
Last Created Deployment Date	The date and time a deployment was last created using this package.
More Information	If available, presents a link to detailed package information. This might be an article or other resource from a third-party.
License Information	If available, presents a link to detailed license information.
Description	Narrative description of the distribution package. Also includes links to any relevant Ivanti knowledge base articles.
Version	The package version.
Total Directories in Package	The number of directories contained in the package.
Total Files in Package	The number of files contained in the package.
Compressed Size of Package	The file size of the compressed package (in KB).
Number of Prescripts	The total number of prescripts contained in the package.
Number of Postscripts	The number of postscripts contained in the package.
Number of Command-Line Scripts	The number of command-line scripts contained in the package.
Number of Dependencies	The number of dependencies associated with the distribution package.
Total Deployments Not Started	The number of deployments that have not started.
Total Deployments In Progress	The number of deployments in progress.

Field	Description
Total Deployments Not Deployed	The number of deployments that were not deployed (because the package is not applicable or an endpoint was marked *Do Not Patch*).
Total Deployments Failed	The number of failed deployments.
Total Deployments Success	The number of successful deployments.

Content Package Icons and Descriptions

Package icons indicate whether a package is cached, deploying, or disabled.

The package status icons and their status are classified as follows:

Table 233: Security Content Status Icons and Descriptions

New	Current	Tasks	Local	Description
			N/A	The package is not cached.
			N/A	The package has been scheduled to be cached or is in the process of being cached.
			N/A	An error occurred while trying to cache the package.
				The package is cached and ready for deployment.
				The package is currently deploying (animated icon).
				The package is disabled.

Working with Packages

There are several tasks that you can perform using Ivanti Patch and Remediation to assist you in the management and deployment of packages. These are available from commands located in the toolbar on the ***Packages*** page.

These tasks include:

Deploying Selected Packages

Within Ivanti Endpoint Security, you can deploy packages from the ***Packages*** page.

For additional information, refer to About Deployments on page 243.

1. Select **Review** > **Vulnerabilities** > **Packages**.
2. From the list, select the packages you want to deploy.

   Tip: Unless you are deploying custom content, Ivanti recommends using the vulnerability content type for deployments. Vulnerabilities can contain multiple packages for multiple platforms, thus simplifying the remediation process.

3. Click **Deploy**.

Result: The ***Deployment Wizard*** opens, preconfigured to deploy the selected content.

After Completing This Task:
Review Using the Deployment Wizard on page 260 and complete subsequent tasks.

Deleting a Package

Deleting a package removes it from the list of available packages. All records of the package are removed from the database. However, system-task packages cannot be removed.

Note: Package metadata for Ivanti-provided packages that were deleted will be re-downloaded from the Global Subscription Service. However, the package will not be cached unless it is associated with a critical content item or included in a deployment.

1. Select **Review** > **Other** > **Packages**.
2. In the ***Packages*** list, select one or multiple packages.

3. In the toolbar, click **Delete**.

   Step Result: The ***Warning*** dialog box opens, which displays the expected processing time for the action.

4. Click **OK** to confirm the request to delete the package(s).

   Step Result: The package(s) is deleted from the packages list.

Updating the Package Cache

Updating the system cache initiates the process to cache (or re-cache) the selected packages.

Note: When you update the package cache, the package itself is not cached. The scripts that are used when the package is deployed are cached.

1. Select **Review** > **Other** > **Packages**.
2. In the ***Packages*** list, select one or multiple packages.
3. In the toolbar, click **Update Cache**.

   Step Result: The ***Warning*** dialog box opens, informing you of the expected processing time for the action.

   Note: The cache will not be updated for disabled content items that have had a new version released.

4. Click **OK**.

   Step Result: The Package scripts are cached.

Creating a Package

Creating a package is a multi-step process that you can accomplish using the ***Package Editor*** wizard.

Complete the following steps to create a package.

1. Select **Review** > **Other** > **Packages**.
2. Click **Create**.

   Step Result: The ***Welcome to the Package Editor*** page opens.

3. Refer to Using the Package Editor on page 515 for details on changing packages through the ***Package Editor Wizard***.

Editing a Package

Changing a package is restricted to custom packages created by you or another Ivanti Patch and Remediation administrator.

Note: Packages with an origin of Ivanti or System cannot be modified.

1. Select **Review** > **Other** > **Packages**.
2. In the ***Packages*** list, select a package.
3. In the toolbar, click **Edit**.

   Step Result: The package is displayed in the **Edit Packages** dialog box.
4. Make the desired edits and click **OK**.

The Package Details Page

This tabbed page lists the information and deployment history for a selected package. Select a tab to view deployments or information. You can also use this page to perform tasks related to the package.

The **Package Details** page contains the following tabs:

- The Deployments Tab (Package Details Page) on page 509
- The Information Tab (Package Details Page) on page 512

Viewing the Package Details Page

View this page to view information about a specific package or to performs tasks related to it.

View the ***Package Details*** page by selecting a package from the ***Packages*** page.

1. Select **Review** > **Other** > **Packages**.

   Step Result: The ***Packages*** page opens.
2. Click the ***Name*** link associated with the package you want to view.

   You may have to page through the list to find the package you want to view.

Result: The ***Package Details*** page opens.

The Deployments Tab (Package Details Page)

The ***Deployments*** tab lists the deployment history for the selected package. It also contains a toolbar you can use to perform tasks related to the package.

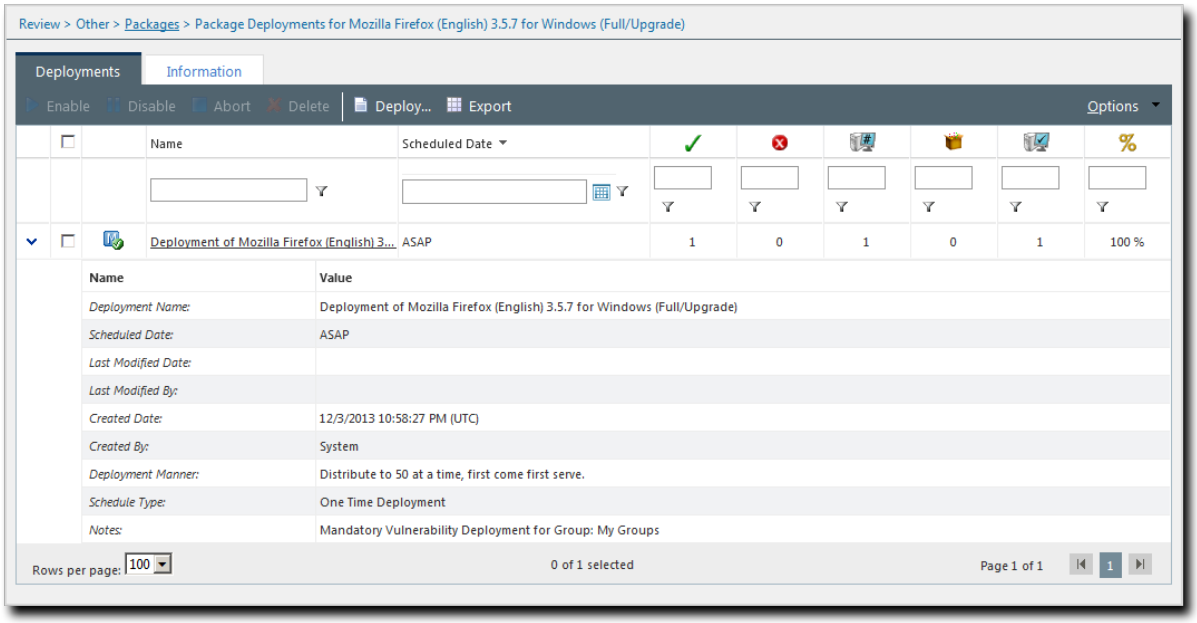


Figure 95: Deployments Tab

The Deployments Tab Toolbar (Package Details Page)

The ***Package Details*** page ***Deployments*** tab contains a toolbar you can use to performs tasks related to the selected deployment.

The ***Deployments*** tab contains a toolbar that allows you to perform actions on packages.

Table 234: Deployments Tab Toolbar

Menu Item	Function
Enable (Patch and Remediation only)	Enables the selected disabled deployment or task. For additional information, refer to Enabling Deployments on page 254.
Disable (Patch and Remediation only)	Disables the selected enabled deployment or task. For additional information, refer to Disabling Deployments on page 254.

Menu Item	Function
Abort (Patch and Remediation only)	Cancels the deployment or task for any endpoints which have not already received the deployment package. For additional information, refer to Aborting Deployments and Tasks on page 254.
Delete (Patch and Remediation only)	Removes the deployment or task from your Ivanti Endpoint Security. For additional information, refer to Deleting Deployments on page 259.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Using the Deployment Wizard on page 260.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Deployments Tab List (Package Details Page)
The ***Package Details*** page ***Deployments*** tab list contains information and statistics about package deployments.

The following table describes each column in the list.

Table 235: Deployments Tab List

Column	Icon	Description
Name	N/A	The name of the package.
Scheduled Date	N/A	The date on which the package was scheduled to deploy.
Number of Endpoints/Groups which were Successful	✓	Total number of endpoints or groups that finished the deployment successfully.
Number of Endpoints/Groups which Failed	⊗	Total number of endpoints or groups that finished the deployment unsuccessfully.

Column	Icon	Description
Number of Endpoints/Groups assigned to the Deployment		Total number of endpoints or groups that are assigned the deployment.
Number of Endpoints/Groups which are In Progress		Total number of endpoints or groups that are in the process of executing the deployment.
Number of Endpoints/Groups which have Complete the Deployment		Total number of endpoints or groups that finished the deployment.
Percentage Complete		Percentage of the endpoints or groups that finished the deployment. = [Total Finished Endpoints / Total Assigned Endpoints]

Each deployment listed be expanded to display additional details about the package. The following table describes each field listed when you expand a deployment.

Table 236: Expanded Package Deployment

Name	Value
Deployment Name	The name of the deployment.
Scheduled Date	The date and time the deployment was scheduled.
Last Modified Date	The date and time the deployment was last modified.
Last Modified By	The user that last modified the deployment.
Created Date	The date and time the deployment was created.
Created By	The user that created the deployment.
Deployment Manner	The manner in which the package was deployed.
Schedule Type	The schedule type selected during deployment configuration.
Notes	The notes entered during deployment configuration.

The Information Tab (Package Details Page)

You can access information similar to that found on the ***Package Details*** page by clicking the package name and selecting the ***Information*** tab.

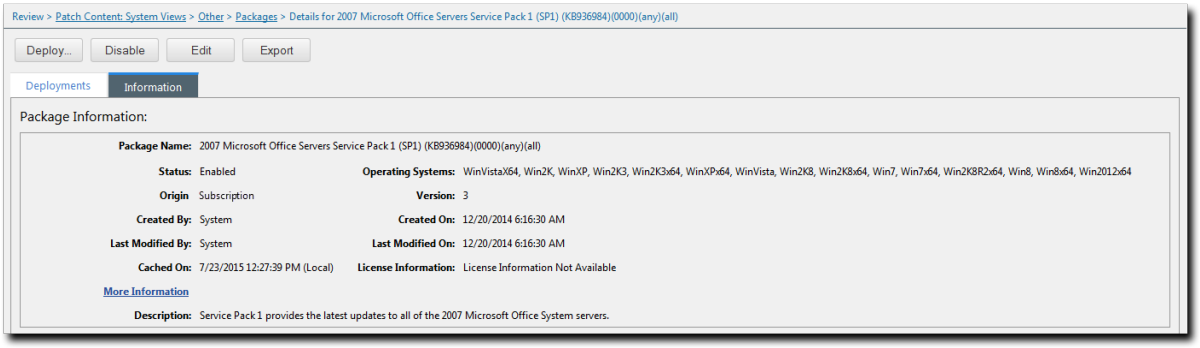


Figure 96: Information Tab

The Information Tab

This tab lists metadata about the patch itself.

The Information Tab Buttons

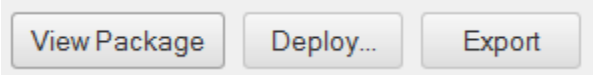


Table 237: Information Tab Buttons

Button	Description
View Package	Opens the ***Packages*** page and displays the package for the applicable content item.
Deploy...	Opens the ***Deployment Wizard***. For additional information, refer to Using the Deployment Wizard on page 260.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 47. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 39.

The Information Tab List

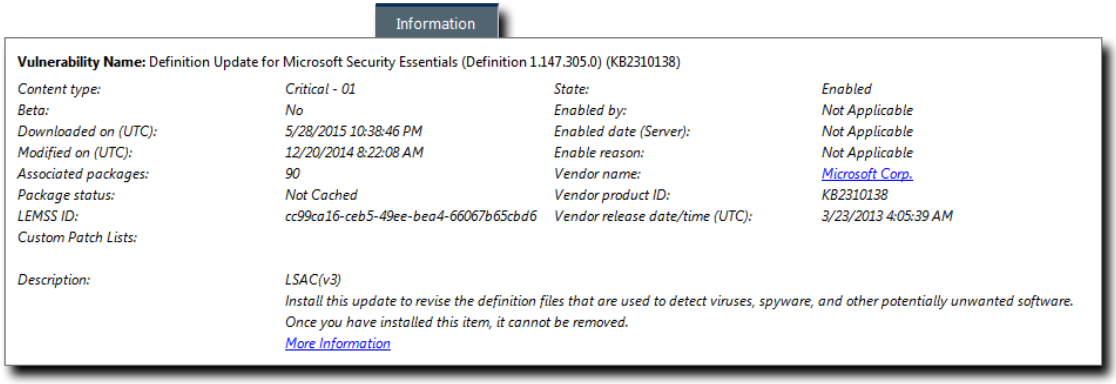


Table 238: List Text Descriptions

Name	Description
Vulnerability Name	The name of the content item.
Content Type	The content item type.
Beta	Indicates if the content item is in beta.
Downloaded on (UTC)	The date and time on which the content was downloaded.
Modified on (UTC)	The date and time the content item was last modified.
Associated packages	The number of packages associated with the content item.
Packages status	The cache status for the content item packages.
Ivanti Endpoint Security ID	The Ivanti Endpoint Security identifier for the content item.
Custom Patch Lists	A listing of all Custom Patch Lists that the content item is included in.
State	The enabled/disabled/completed status of the content item.
Enabled/Disabled by	The Ivanti Endpoint Security user who last disabled or enabled the content.
Enabled/Disabled date (Server)	The date and time the content was disabled or enabled.
Enable/Disable reason	The reason the user provided for disabling or enabling the content. You can click the **Edit** link to change the reason.
Vendor name	The name of the content item vendor.
Vendor product ID	The identifier given to the security content item by the vendor.
Vendor release date/ time (UTC)	The date and time the vendor released the software in the content item.

Name	Description
Common Vulnerability Exploit (CVE) [1]	The CVE number for the content.
Vulnerability Code Description [1]	A description of the vulnerability associated with the content item.
Reference Text [1]	The reference text(s) associated with the content item vulnerability.
Description [1]	The narrative description of the distribution package. This section may include important notes about the content item and a link to more information.
[1]This meta data appears conditionally based on whether it was added for the content item. Additionally, there may be multiple instances of each meta data section.	

Package Information

The ***Package Details*** page ***Information*** tab lists package information, deployment information, and package contents for the selected package.

The following table describes each field listed on the ***Information*** tab.

Table 239: Package Information Definitions

Status	Description
Package Information	
Package Name	Title of the package
Status	The current status of the package, stating if the package is enabled and ready to be requested from the Global Subscription Service.
Origin	The origin of the task or which company created the package.
Created By	The user who created the package.
Last Modified By	The user who last modified the package.
Cached On	The date and time the distribution package was last cached.
More Information	If available, presents a link to detailed package information. This might be an article or other resource from a third-party.
Description	Narrative description of the distribution package. Also includes links to any relevant Ivanti knowledge base articles.
Operating Systems	The operating systems and platforms that the package supports and may be deployed to.
Version	The package version.

Status	Description
Created On	The date and time the package was created.
Last Modified On	The date and time of the last change to the package.
License Information	If available, presents a link to detailed license information.
Deployment Information	
Total Deployments	The total number of deployments.
Total Scheduled	The number of scheduled deployments.
Total In Progress	The number of running deployments.
Total Success	The number of successful deployments.
Package Contents	
Files	The number of files contained in the package.
Disk Space	The file size of the compressed package (in KB).
Scripts	The total number of scripts (includes Prescripts, Postscripts, and Command-line scripts) contained in the package.
Directories	The number of directories contained in the package.
Dependencies	The number of dependencies associated with the distribution package.

Using the Package Editor

Creating distribution packages is performed using the ***Package Editor*** wizard.

Note: The ***Package Editor*** is supported in the Internet Explorer Web browser only. To use the ***Package Editor*** with the Internet Explorer Web browser, you must install an ActiveX control.

Caution: If the Application Control module has been installed and its Easy Lockdown feature applied to an endpoint, a browser on that endpoint will not be able to install a new ActiveX control. Before using Package Editor in this situation, the administrator must create a Trusted Publisher policy that assigns the Ivanti Security certificate to that endpoint. For additional information, refer to *Easy Lockdown in Practice* and *Creating a Trusted Publisher Policy* within the Application Control User Guide (https://help.ivanti.com) .

1. Select **Review** > **Other** > **Packages**.
2. In the ***Packages*** list, click **Create**.

   Step Result: The ***Welcome to the Package Editor*** screen opens.

3. Click **Next**.
4. Type Package Information in each field.
   The following table describes the information you type in each field.

Field	Description
Name	A name or title for the package. Ivanti recommends using short and descriptive names. Duplicate package names are permitted, and package names can be edited after initial creation.
Description	A description of package details. Ivanti recommends adding information as the package is modified, providing necessary information as needed.
Information URL	Link(s) to additional information about the content and usage of the package. The information URL is displayed when viewing package information.

Note: Deployment options for manual installations of a patch can be included in the **Description** field. For more information about using deployment options, refer to Including Deployment Options in a Package on page 517.

5. Click **Next**.
   Step Result: The ***Select Operating System*** page opens displays.
6. In the ***Operating Systems*** page, select the target operating systems from the list. These are the platforms running endpoints that are the target for the package deployment.

Note: Since directory structures, executable file types, and available scripting languages vary greatly within operating systems, a package designed for one operating system may fail when applied to another operating system.

7. Click **Next**.
   Step Result: The ***Add Files*** page opens.
8. Add files to the package.
   For additional details regarding adding files to a package, refer to Adding Files and Directories to a Package on page 520.
9. Click **Next**.
   Step Result: The ***Create Scripts*** page displays.
10. If needed, add a script to run on the target endpoint during the deployment process.
    For additional details regarding package scripts, refer to Creating Scripts for a Package on page 523.

11. Click **Next**.

Step Result: The ***Enter a License*** page opens.

12. In the ***License Agreement*** dialog, select the **License Agreement** check box and enter the appropriate URL in the destination address of the **License URL** field.

The ***License Agreement*** dialog allows you to enter in an optional ***License URL***, which can link to licensing information for the contents of the package. This option is primarily for packages containing items such as operating system service packs, endpoint drivers, and so on. The License URL displays when viewing package information and allows the user to link to the license information.

13. Click **Next**.

Step Result: The ***Summary*** page displays.

14. Click **Upload**.

15. In the ***Summary*** page, review the summary of the package to be deployed.

Selecting the **Make this package available for rollout** check box enables the package to display in the list of available packages. You may clear this option if you are creating a package that will contain additional files or details added at a later date or do not want to deploy the package at this time.

16. The ***Upload Status*** page verifies that the data is unpacking and uploading. Once all files are uploaded, click **Next**.

Step Result: The ***Upload Summary*** page displays.

17. Click **Finish**.

Result: The page refreshes and the ***Package*** page opens with the custom package. When you refresh the ***Packages*** page, you can view the package by the name you gave it, and view the operating systems that you chose to deploy to during the patch building process.

Including Deployment Options in a Package

Package flags control the behavior of a distribution package when it is deployed.

The following flags indicate a manual installation of the patch is required. To use this option, type `(manual install)` in the **Description** field.

A number of additional deployment options are available by including them in with the flags delimiter. To add these, enter `(PLFlags: <Your Flags>)` to the **Description** field.

Package Flag Descriptions

Package flags allow you to attach behavior to package deployments.

The following table defines flag behavior and their descriptions:

Table 240: Package Flag Descriptions

Description (flag behavior)	Display Flag	Select Flag
Perform an uninstall; can be used with -mu or -q.	-yd	-y
Force other applications to close at shutdown.	-fd	-f
Do not back up files for uninstall.	-nd	-n
Do not restart the computer when the installation is done.	-zd	-z
Use quiet mode, no user interaction is required.	-qd	-q
Use unattended setup mode.	-dmu	-mu
Install in multi-user mode[1]	N/A	-su
Restart service after installation[1]	N/A	-restart
Do not restart service after installation[1]	N/A	-norestart
Reconfigure after installation[1]	N/A	-reconfig
Do not reconfigure after installation[1]	N/A	-noreconfig
Download packages to the default package cache directory for the Linux distro, but don't install them[2] Packages are downloaded to the following locations: • Redhat and CentOS: `/var/cache/yum` • SUSE: `/var/cache/zypp/packages` • Ubuntu: `/var/cache/apt`	N/A	-CACHEPACKAGES

Description (flag behavior)	Display Flag	Select Flag
Install packages cached in the `tmp` folder[2]	N/A	-INSTALLFROMCACHE
Tip: If you are patching Linux and Unix endpoints that receive content directly from vendor repositories, deployments may exceed your scheduled window because the patch content must first be downloaded, a process that may be excessively long. To reduce the likelihood of deployments that exceed maintenance schedules: **1.** Cache the content to the endpoints by completing a deployment using the -CACHEPACKAGES flag. This deployment downloads the content, but doesn't install it. **2.** Install the cached content by completing a second deployment using the -INSTALLFROMCACHE flag. The deployment skips the download of content, and installs the content already cached.		
Ignores discrepancies between libraries available in different architectures[2]	N/A	-YUM_PROTECTED_MULTILIB
Skips packages with broken dependencies when updating the endpoint[2]	N/A	-YUM_SKIP_BROKEN
Performs a trial run of the deployment with no package changes made.[3]	N/A	-TRIAL_RUN
This package is chainable and will run Qchain.exe (Windows) or (UNIX/Linux).	-dc	-c
Suppress the final chained reboot.	-dc	-sc
Repair permissions.	-dr	-r
Deploy only.	-PLD1	-PLDO
No Pop-up	-PLN1	-PLNP
Debug	-PLDG	-PLDEBUG
Suppress Repair	-dsr	-sr
Force the script to reboot when the installation is done.	-1d	-1
Reboot is required.	N/A	-2
Reboot may occur.	N/A	-3
Reboot is required, and may occur.	N/A	-4

1. This flag applies to Linux and Unix operating systems only.
2. This flag applies to only Red Hat Enterprise Linux 5.5-7.x, Oracle Enterprise Linux 5.5-7.x, and CentOS Linux 5.5-7.x.
3. This flag applies to only Oracle Solaris 10 Update 9.

Adding Files and Directories to a Package

There are several options for adding files, folders, and macros to a package.

Files and directories can be added to the package by right-clicking the ***Package Content*** window, and selecting one of the following options:

Adding a Directory to a Package

Once a macro, directory, or folder has been created, a new directory can be added to it. A file system window is opened where you can locate and select an existing directory to add to the package.

1. Right-click the macro, directory, or folder associated with the target computer.
2. Select **Add Directory**.

   Step Result: The ***Browse for Folder*** window opens.
3. Select the directory to add to the macro, directory, or folder.
4. Click **Open**.

   Step Result: The directory is added to the macro, directory, or folder.

Creating a Drive for a Package

Use the **New Drive** option to deploy a package to a drive other than the `C:\` or `%TEMP%` drives.

1. Right-click inside the ***Target Computer*** window.
2. Select **Create Drive...** from the pop-up menu.

   Step Result: The ***Create Drive*** window opens.
3. In the **Drive** or **Volume Name** field, type the letter you require for the drive name, followed by a colon in `X:` format.
4. Click **OK**.

   Step Result: The drive is added to the ***Target Computer*** window.

Adding a New Macro to a Package

Macros access existing system directories. A macro can be either an environment variable, as defined by the operating system, or a macro that only the agent can expand.

The following pre-defined macros are available under the **New Macro** menu:

- %TEMP% - The operating system temp directory location. Expands to `C:\Windows\Temp`, `C:\Temp`, `C:\WinNT\Temp`, or `/tmp` depending on operating system and configuration.
- %WINDIR% - The operating system windows directory location. %WINDIR% typically expands to `C:\Windows`.
- %BOOTDIR% - The operating system boot directory location. Typically expands to `C:\`.
- %ROOTDIR% - The operating system root directory location. Typically expands to `C:\`.
- %PROGRAM FILES% - The operating system program files location. Typically expands to `C:\Program Files`.
- %COMMON FILES% - The operating system common files location. Typically expands to `C:\`.

Note:

Not all macros are available on all operating systems. Choose only the macros that are compatible with the operating systems and configurations you are using.

1. Right-click inside the ***Target Computer*** window.
2. Select **Create Macro**.

   Step Result: A list opens.
3. Select the macro required for the package.

   Step Result: The selected macro displays in the ***Target Computer*** window.

Creating a Folder for a Package

The ***Create Folder*** window allows for creating a folder within the Package Content directory.

1. Right-click inside the ***Target Computer*** window.
2. Select **Create Folder**.

   Step Result: The ***Create Folder*** window opens.
3. In the **Folder Name** field, type the name of the new folder.
4. Click **OK**.

   Step Result: The folder is added to the ***Target Computer*** window.

Adding a File to a Package

Once a folder, directory, or macro has been created, a file can be added. A file system window is opened where you can locate and select an existing file to add to the Package.

1. Right-click the directory, folder, or macro associated with the ***Target Computer***.
2. Select **Add File**.

   Step Result: The ***Open*** window opens.
3. Select the file to add to the directory, folder, or macro.
4. Click **Open**.

   Step Result: The file is added to the directory, folder, or macro.

Deleting a File from a Package

You can remove a directory or file from a package. This option is available only for files added to the ***Target Computer*** window.

1. Right-click the directory, folder, or macro associated with the ***Target Computer*** that you want to delete.
2. Select **Delete**.

   Step Result: The file is deleted for the package.

Renaming a File within a Package

The Rename option allows for renaming of a previously created drive or macro within the package.

1. In the ***Target Computer*** directory tree, select the directory where the file is to be renamed

   Step Result: The file is highlighted and the cursor becomes active.
2. Type the new name of the file.
3. Click **OK**.

   Step Result: The folder name is changed and displays in the ***Target Computer*** window.

Folder Properties for a Package

The ***Properties*** window allows you to set properties for the selected item. Only available when you right click on a folder that has previously been added to the ***Target Computer*** window.

1. In the ***Target Computer*** window, select the directory where the file is located.
2. Right-click the selected file.

3. Select **Properties**.

   Step Result: The ***Properties*** window opens.

4. In the **Attribute** field, select or deselect the **Overwritable** check box.

   Example:

   Note: Removing the check-mark from the **Overwritable** attribute will prevent subsequent patches that contain the same file from overwriting the file.

5. Click **Apply**.

   Step Result: The folder properties are changed.

Creating Scripts for a Package

You can add functionality to packages using scripts.

There are three types of scripts. These scripts can be written in Microsoft Visual Basic Script or Microsoft Jscript. Documentation regarding these languages can be found at MSDN Library: Scripting (http://msdn2.microsoft.com/en-us/library/ms950396).

The following scripts are listed by the order in which they execute within the package:

1. Pre-Script - Used to test for a machine condition or shutdown a service. For example you can stop the package rollout in the pre-script by using the `SetReturnCode` in the `PLCCAgent` script object.
2. Command Line Script - Used to launch executable files. The format is the same as a standard `.CMD` or `.BAT` file.
3. Post-Script - Used for any clean-up operations such as the deletion of files, starting services, or running an installed file.

There can be a maximum of one of each script type in a software package. When all three scripts are present, they will be executed in the order listed above.

Note: Unless the **Execution Directory** option is selected and a valid directory is defined, all scripts run in the `ROOT` directory.

1. Select the type of script to execute from the **Type of Script** drop-down list.
2. Select the scripting type from the **Script Language** drop-down list.
3. Click **Edit**.

   Step Result: The ***Script Editor*** window opens.

4. Type or copy the script to be added in the **Script** field.
5. Click **Run**.

   Step Result: The script is checked and the ***Errors*** box displays **Success** when the script is validated.

6. Click **OK**.

   Step Result: The ***Script Editor*** window closes and returns to the ***Package Editor*** wizard.

7. If needed, select **Script Execution Directory** if a different directory location is required.

   Step Result: The **Script Execution Directory** field becomes active.

8. Type the back-up directory path, or click **Browse**.

   Step Result: The location displays in the **Script Execution Directory** field.

Chapter 14

Patch and Remediation Reporting

In this chapter:

Ivanti Endpoint Security can generate a variety of reports pertaining to Patch and Remediation functions.

Use these reports for internal reporting, management briefing, and assistance when using Ivanti Endpoint Security.

About Patch and Remediation Reports

Reports are records that document activity and information pertaining to your network environment. When the Patch and Remediation module is installed, Ivanti Endpoint Security includes reports that include data related to Patch and Remediation.

Ivanti Endpoint Security offers multiple predefined report templates that list and/or depict data collected during network management. Data for Patch and Remediation-related reports include information about content and deployments. Reports are created by selecting a report type and defining its parameters.

Additionally, report formats vary. Some reports are in a HTML (`.html`) file format, while others are in a PDF (`.pdf`) format.

The Patch and Remediation Report Pages

From these pages, you can generate all available Patch and Remediation reports. Use this page to generate reports related the module's various functions. Before generating the report, select the report type and define the report parameters.

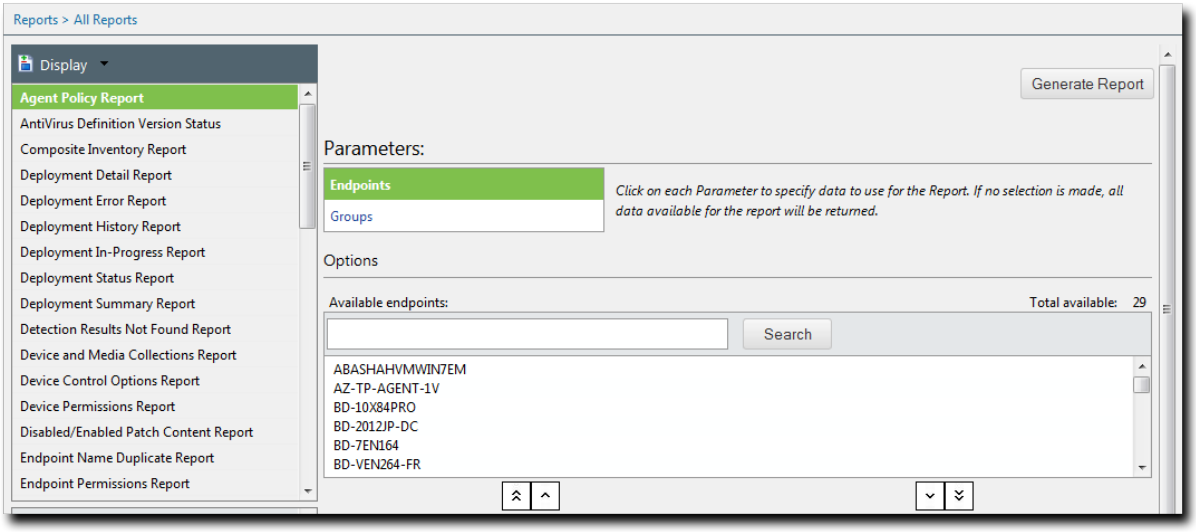


Figure 97: All Reports Page

Note: From the **Reports** menu, you can select multiple ***All Reports*** page variants. Based on which **Reports** menu item you select, the resulting page that opens groups its **Display** menu differently.

The following table lists the items available in the **Reports** navigation menu when Patch and Remediation is installed.

Table 241: Reports Menu Commands

Command	Description
Deployments	Reports are grouped with the **Deployments** group expanded. Deployment reports display information related to content deployment.
Inventory	Reports are grouped with the **Inventory** group expanded. Inventory reports display information related to network assets and endpoint hardware and software.
Policy and Compliance	Reports are grouped with the **Policy and Compliance** group expanded. These reports display information about agent policy sets, Mandatory Baselines, and Mandatory Baseline endpoint compliance.

Command	Description
Risks	Reports are grouped with the **Risks** group expanded. This report displays information about possible vulnerabilities in your network.
Vulnerabilities/Patch Content	Reports are grouped with the **Vulnerabilities/Patch Content** group expanded. These reports display information about network vulnerabilities.

Viewing the Patch and Remediation Report Pages

Navigate to these pages to generate either HTML or PDF reports related to Patch and Remediation.

Tip: You can select any of the Report sub-menu items to filter the page for report categories.

Generate the desired report.

Generating a Report

Ivanti Endpoint Security provides multiple predefined reports for Patch and Remediation. Generate reports to brief management or to view network behavior and statistics.

Generate reports from any Patch and Remediation report page.

1. From the **Navigation Menu**, select **Reports** > **All Reports**.
2. From the **Display** list, select the report you want to generate.
3. Define parameters using the available fields, drop-downs, lists, and so on. Each report has distinct required and optional parameters.

   Note: Refer to the individual report descriptions for details regarding which parameters are required and which parameters are optional.
4. [Optional] Select the optional report parameters.
5. Click **Generate Report**.

   Step Result: The report generates.

   Important: The Enhanced Security Configuration feature for Internet Explorer suppresses pop-up windows from appearing and must be disabled to display report data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress report display functionality and should be disabled.

Result: The report is generated in a new window.

Configuration Policy Compliance - Benchmark Perspective

This report shows the number of endpoints passing the security configuration assessment at predetermined levels, based on the parameters that you select.

Optional Parameters: `Benchmarks`, `Endpoints`, `Groups`, `Profile`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes the columns included in the report.

Table 242: Configuration Policy Compliance - Benchmark Perspective Column Definitions

Column	Definition
Benchmark	The name of the security configuration benchmark applied to the endpoint.
Profile	The name of the security configuration profile applied to the endpoint.
Assessment Engine	The version of the check tool that processed the benchmark when it was uploaded.
Group	The name of the endpoint group that was assessed.
95% Passing	The number of endpoints that passed the benchmark at a level of 95% or higher.
94.9%-90% Passing	The number of endpoints that passed the benchmark at levels from 90% to 94.9%.
< 90% Passing	The number of endpoints that passed the benchmark at levels of less than 90%.
Total	The total number of endpoints assessed.

Configuration Policy Compliance - Group Perspective

This report shows the number of endpoint groups passing the security configuration assessment at predetermined levels, based on the parameters that you select.

Optional Parameters: `Benchmarks`, `Endpoints`, `Profile`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes the columns included in the report.

Table 243: Configuration Policy Compliance - Group Perspective Column Definitions

Column	Definition
Benchmark	The name of the security configuration benchmark applied to the endpoint.
Profile	The name of the security configuration profile applied to the endpoint.

Column	Definition
Assessment Engine	The version of the check tool that processed the benchmark when it was uploaded.
Group	The name of the endpoint group that was assessed.
95% Passing	The number of endpoints that passed the benchmark at a level of 95% or higher.
94.9%-90% Passing	The number of endpoints that passed the benchmark at levels from 90% to 94.9%.
< 90% Passing	The number of endpoints that passed the benchmark at levels of less than 90%.
Total	The total number of endpoints assessed.

Configuration Policy Details Report

This report shows the number and percentage of endpoints that are compliant or non-compliant.

Optional Parameters: `Endpoints`, `Groups`, `Benchmarks`, `Result`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes the columns included in the report.

Table 244: Configuration Policy Details Report Column Definition

Column	Definition
Benchmark	The name of the security configuration benchmark applied to the endpoint.
Profile Name	The name of the security configuration profile applied to the endpoint.
Rule Group	The name of the category to which a rule belongs.
Rule	The name of the security configuration rule.
Total Passed	The number of endpoints that comply with the security configuration rule.
Total Failed	The number of endpoints that do not comply with the security configuration rule.
Score %	The percentage of endpoints that comply with the security configuration rule.
Result	The pass or fail result.

Configuration Policy Rule Result Report

This report shows pass or fail results for individual security configuration profile rules.

Optional Parameters: `Groups`, `Benchmarks`, `Profile`, `Result`

Note: If no parameter selection is made, the report generates using available data.

The following table describes the columns included in the report.

Table 245: Configuration Policy Rule Result Report

Column	Definition
Benchmark	The name of the security configuration benchmark applied to the endpoint.
Profile Name	The name of the security configuration profile applied to the endpoint.
Rule Title	The title of the category to which a rule belongs.
Device Name	The name of the endpoint.
Result	The pass or fail result.

Configuration Policy Summary Report

This report shows the number and percentage of endpoints that have passed or failed configuration policy tests, based on the parameters that you select.

Optional Parameters: `Endpoints`, `Groups`, `Benchmarks`, `Result`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes the columns included in the report.

Table 246: Configuration Policy Summary Report

Column	Definition
Benchmark	The name of the security configuration benchmark applied to the endpoint.
Profile Name	The name of the security configuration profile applied to the endpoint.
Benchmark Group	The name of the benchmark group applied to the endpoint.
Rule Group	The name of the category to which a rule belongs.
Rule	The name of the security configuration rule.
Total Passed	The number of endpoints that comply with the security configuration rule.
Total Failed	The number of endpoints that do not comply with the security configuration rule.

Column	Definition
Score %	The percentage of endpoints that comply with the security configuration rule.
Result	The pass or fail result.

Deployment Detail Report

This report provides information about a selected list of deployments. In the report, each deployment name is listed in the **Deployment Name** column. The report provides information as to the status of the particular deployment activity.

Optional Parameters: `Exclude Do Not Patch Reason`, `Include Do Not Patch Reason`, `Deployments`, `Packages`, `Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 247: Deployment Detail Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Endpoint Name	The name of the endpoint.
Deployment Result	The deployment status.
Deployment Start Date	The date the deployment was sent.
Date Installed	The date the package was installed on the endpoint.
Vulnerability Status	The content item patch status.
Do Not Patch - Reason	The reason the endpoint is marked as *Do Not Patch*. This column appears only if you selected **Include Do Not Patch Reason** when generating the report.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) task.

Note: If a selected content item does not have an associated deployment, it will not appear in the report.

Deployment Error Report

This report provides information about deployments that have returned an error.

Optional Parameters: `Deployments`, `Packages`, `Endpoints`, `Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 248: Deployment Error Report Column Definitions

Column	Definition
Deployment Status	The deployment status.
Status Code	The reference code for support identification. When contacting support, use this code to help identify the deployment issue.
Error Message	The actual error text returned by the deployment.
Install Date	The date the agent was installed on the endpoint.
Package Name	The name of the package.
Deployment Name	The name of the deployment.
Device Name	The name of the endpoint.

Deployment History Report

This report allows selection of multiple patch deployments. It also displays a single pie chart for each deployment and shows deployment status counts for the deployment.

Required Parameters: Selection of one or multiple `deployment(s)`.

The following table describes each report field.

Table 249: Deployment History Report Field Definitions

Field	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Deployment Status	The deployment status.
Deployment Date	The date the deployment was sent.
Created Date	The date and time the deployment was scheduled.
Created By	The user who created the deployment.
Graph Key	

Field	Definition
Added to the Group After the Deployment Started	The number (or percentage) of deployments that did not complete because the endpoint was added to the group after the deployment started.
Already Patched	The number (or percentage) of endpoints that are already patched.
Caching Package	The number (or percentage) of deployment packages that are being cached.
Deployment Aborted by Client User	The number (or percentage) of deployments that were aborted by endpoint users.
Deployment Aborted by User	The number (or percentage) of deployments that were aborted by Ivanti Endpoint Security users.
Disabled	The number (or percentage) of deployments that were disabled.
Do Not Patch - Not Deployed	The number (or percentage) of endpoints that were marked as *Do Not Patch* for the content being deployed.
Failure	The number (or percentage) of deployments that failed.
In-Progress	The number (or percentage) of deployments that are in progress.
Not Applicable	The number (or percentage) of endpoints where the deployment does not apply.
Not Started	The number (or percentage) of deployments that have not started.
Not Started - Recurring	The number (or percentage) of recurring deployments that have not started deploying.
Removed from Deployment and Group	The number (or percentage) of deployments removed from deployments and groups.
Removed from Deployment by User	The number (or percentage) of deployments removed by users.
Success	The number (or percentage) of successful deployments.
Total	The total number of endpoints assessed.

Note: If there are no occurrences of a particular status during a deployment, that status does not appear in the ***Deployment History Report*** graph key.

Deployment In-Progress Report

This report provides information about deployments that have started but have not yet completed. Reports can be generated for each deployment, package, or endpoint. It also provides the status of the deployment.

Optional Parameters: `Deployments`, `Packages`, `Endpoints`, `Groups`

Note: Selecting no parameters will generate the report using all available data.

The following table describes each report column.

Table 250: Deployment In-Progress Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Total Not Deployed	The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, marked *Do Not Patch*, added to the group after the deployment started, or the deployment was aborted by the user).
Total Already Patched	The number of endpoints that are already patched.
Not Applicable	The number of endpoints where the deployment does not apply.
Do Not Patch	The total number of endpoints that are marked as *Do Not Patch*.
Total Deployed	The total number of endpoints that were assigned the deployment.
Total Success	The total number of endpoints successfully patched.
Total In-Progress	The total number of endpoints currently receiving the deployment.
Not Started	The number of endpoints yet to receive the deployments.
Caching Package	Indicates whether the deployment package is being cached. 1 = Caching, 0 = Complete
Total Failed	The total number of deployments that failed.
Total Disabled	The total number of endpoints that are disabled and cannot receive the deployment.
Percent Successful	The percentage of endpoints that successfully received the deployment.
Percent Failure	The percentage of endpoints on which the deployment has failed.

Deployment Status Report

This report provides the current status of a specified package deployment. It also includes a pie chart that shows deployment status counts for the deployment, as well as deployment results.

Required Parameters: Selection of one `deployment`.

Optional Parameters: `Deployment Results`.

The following table describes the report fields and columns.

Table 251: Deployment Status Report Field and Column Definitions

Field / Column	Definition
General Information	
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Deployment Status	The deployment status.
Deployment Date	The date the deployment was sent.
Created Date	The date and time the deployment was scheduled.
Created By	The user who created the deployment.
Graph Key	
Added to the Group After the Deployment Started	The number (or percentage) of deployments that did not complete because the endpoint was added to the group after the deployment started.
Already Patched	The number (or percentage) of endpoints that are already patched.
Caching Package	The number (or percentage) of deployment packages that are being cached.
Deployment Aborted by Client User	The number (or percentage) of deployments that were aborted by endpoint users.
Deployment Aborted by User	The number (or percentage) of deployments that were aborted by Ivanti Endpoint Security users.
Disabled	The number (or percentage) of deployments that were disabled.
Do Not Patch	The number (or percentage) of endpoints that are marked as *Do Not Patch*.
Failure	The number (or percentage) of deployments that failed.
In-Progress	The number (or percentage) of deployments that are in progress.

Field / Column	Definition
Not Applicable	The number (or percentage) of endpoints where the deployment does not apply.
Not Started	The number (or percentage) of deployments that have not started.
Not Started - Recurring	The number (or percentage) of recurring deployments that have not started deploying.
Removed from Deployment and Group	The number (or percentage) of deployments removed from deployments and groups.
Removed from Deployment by User	The number (or percentage) of deployments removed by users.
Success	The number (or percentage) of successful deployments.
Total	The total number of endpoints assessed.
Table Columns	
Server Name	The IP address of the Ivanti Endpoint Security server where the deployment originated.
Agent Name	The name endpoint that hosts the agent.
IP Address	The IP address of the endpoint.
Install Date	The date and time the deployment commenced.
Status Detail	Displays the status details applicable to the endpoint.
Failure Reason	Displays applicable failure reasons.

Note: If there are no occurrences of a particular status during a deployment, that status does not appear in the ***Deployment Status Report*** graph key.

Deployment Summary Report

This report provides information about a selected list of deployments. It also provides a summary of the particular deployment activity.

Optional Parameters: `Deployments`, `Packages`, `Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 252: Deployment Summary Report Column Definitions

Column	Definition
Deployment Name	The name of the deployment.
Package Name	The name of the package.
Total Not Deployed	The total number of endpoints and groups that were excluded from the deployment (because the package was already applied, not applicable, marked *Do Not Patch*, added to the group after the deployment started, or the deployment was aborted by the user).
Total Already Patched	The number of endpoints that are already patched.
Not Applicable	The number of endpoints where the deployment does not apply.
Do Not Patch	The total number of endpoints that are marked as *Do Not Patch*.
Total Deployed	The total number of endpoints that were assigned the deployment.
Total Success	The total number of endpoints successfully patched.
Total In-Progress	The total number of endpoints currently receiving the deployment.
Not Started	The number of endpoints yet to receive the deployments.
Caching Package	Indicates whether the deployment package is being cached. 1 = Caching, 0 = Complete
Total Failed	The total number of deployments that failed.
Total Disabled	The total number of endpoints that are disabled and cannot receive the deployment.
Percent Successful	The percentage of endpoints that successfully received the deployment.
Percent Failure	The percentage of endpoints on which the deployment has failed.

Note: If a selected content item has no associated deployment, it does not appear in the report.

Detection Results Not Found Report

This report returns a list of endpoints that have not completed a Discover Applicable Updates task with the server. The report lists each agent name, the installation date of the agent, and information required to identify and locate the endpoint.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 253: Detection Results Not Found Report Column Definitions

Column	Description
Agent Name	The name endpoint that hosts the agent.
OS Abbr Name	The abbreviated operating system name.
Agent Version	The version of the agent.
Last Contact Date	The last date the Ivanti Endpoint Security had contact with the agent.
Installation Date	The date and time the agent was installed on the endpoint.
IP Address	The IP address of the endpoint.
DNS Name	The name used by the Domain Name System (DNS) to identify the endpoint.
OS Info	A description of the operating system.
Last DAU Date	The date of the last Discover Applicable Updates (DAU) task.
Last DAU Status	The status of the last Discover Applicable Updates (DAU) task.

Disabled/Enabled Patch Content Report

This report returns a list of content that has been disabled by an Administrator, with the disable reason text (if applicable) and date. This report can also be configured to show re-enabled content.

Optional Parameters: `Disabled vulnerabilities/patch content`, `Re-enabled vulnerabilities/patch content`

Note: If no parameter selection is made, the report generates using all available data.

Table 254: Disabled / Enabled Patch Content Report

Column	Description
Name	The name of the selected content group.
Content Type	The type of content in the content item.
Vendor	The name of the vendor that created the software in the content item.
Vendor Release Date	The date and time that the vendor released the content item.
State	The state of the content item (disabled or enabled).
Disabled/Enabled By	The user that disabled or enabled the content item.

Column	Description
Disabled/Enabled Date	The date and time that the content item was disabled or re-enabled.
Reason	The reason that the content item was enabled or disabled.

Endpoint Name Duplicate Report

This report returns a list of duplicate endpoints registered with Ivanti Endpoint Security. Duplicate endpoints are usually the result of applying the agent uniqueness feature that permits an agent installed on ghost images to register multiple times with Ivanti Endpoint Security.

Optional Parameters: `Date Range`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 255: Device Duplicate Report Column Definitions

Column	Definition
Device Name	The name of the endpoint.
Status	The current status of the endpoint.
Install Date	The date the agent was installed on the endpoint.

Hardware Inventory Detail Report

This report provides information about hardware associated with an endpoint and endpoint status.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 256: Hardware Inventory Detail Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	The name of the hardware device.
Device Name	The name of the endpoint.
Device OS Info	A description of the operating system.

Hardware Inventory Summary Report

This report provides a summary of reported hardware and the endpoints associated with them.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 257: Hardware Inventory Summary Report Column Definitions

Column	Definition
Hardware Device Class	The type of hardware.
Hardware Device Name	The name of the hardware device.
Instances	The number of times this device occurs. (Within the parameters of the report.)

Mandatory Baseline Detail Report

This report provides information about the Mandatory Baseline status associated with an endpoint.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 258: Mandatory Baseline Detail Report Column Definitions

Column	Definition
Endpoint Name	The name of the endpoint.
Assigned By Group	The distinguished name of the group that assigned the Mandatory Baseline.
Package Name	The name of the package.
Mandatory Baseline Enabled	Indicates whether the *Assigned By Group* has Mandatory Baselines enabled.
Package Enabled	Indicates whether the package is enabled. If the package is disabled, it cannot be deployed to an endpoint.
Mandatory Status	Identifies whether the endpoint is applicable, patched, not patched, marked as *Do Not Patch*, or needs patching by the Mandatory Baseline.
Deployment Status	The deployment status.

Column	Definition
Package Release Date	The date the package was released.
Date Deployed	The date the package was deployed.
Date Installed	The date the package was installed on the endpoint.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) task.
Assigned	Indicates whether the Mandatory Baseline is assigned to the endpoint. 1 = Assigned, 0 = Not Assigned

Mandatory Baseline Summary Report

This report returns a summary list of patch content and deployment information for all Mandatory Baseline packages and content associated with the selected list of endpoints.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each table column.

Table 259: Mandatory Baseline Summary Report Column Definitions

Column	Definition
Mandatory Baseline Item Name	Name of the Mandatory Baseline content item.
Total Endpoints	The total number of endpoints selected for the report.
Total Patched	The total number of endpoints patched by the deployment.
Total Not Applicable	The total number of endpoints for which the deployment does not apply.
Total Do Not Patch	The total number of endpoints that are marked as *Do Not Patch*.
Total In-Progress	The total number of endpoints currently receiving the deployment.
Total Disabled	The total number of endpoints that are disabled and cannot receive the deployment.
Total Error Condition	The total number of endpoints on which the deployment has failed.
Percent Patched	The percentage of applicable endpoints that are patched.

Operating System Inventory Detail Report

This report provides information about the operating system associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 260: Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Device Name	The name of the endpoint.

Operating System Inventory Summary Report

This report provides a summary about the operating system associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates all available data.

The following table describes each report column.

Table 261: Operating System Inventory Detail Report Column Definitions

Column	Definition
Operating System	The operating system name and description.
Instances	The number of times this operating system occurs. (Within the parameters of the report.)

Package Compliance Detail Report

This report provides information about patch and deployment status for a specific package or endpoint. The report lists each package associated with the selected endpoint(s) or group(s). In the report, each package is listed in the **Package Name** column. The report also provides details for the vulnerability status for each package, and the associated endpoint, status, and deployment details.

Optional Parameters: `Exclude Do Not Patch Reason`, `Include Do Not Patch Reason`, `Packages`, `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 262: Package Compliance Detail Report Column Definitions

Column	Definition
Package Name	The name of the package.
Package Release Date	The date the package was released.
Endpoint Name	The name of the endpoint.
Vulnerability Status	The content item patch status.
Do Not Patch - Reason	The reason the endpoint is marked as *Do Not Patch*. This column appears only if you selected **Include Do Not Patch Reason** when generating the report.
Last DAU Run	The date of the last Discover Applicable Updates (DAU) task.
Last DAU Status	The status of the last Discover Applicable Updates (DAU) task.
Date Last Verified	The date of the last Discover Applicable Updates (DAU) task.
Deployment Name	The name of the deployment.
Deployment Start Date	The date the deployment was sent.
Deployment Status	The deployment status.
Date Installed	The date the package was installed on the endpoint.
Date Scheduled	The date the package was scheduled for deployment to the endpoint.

Note: If a selected package has no associated deployment, it does not appear in the report.

Package Compliance Summary Report

This report returns a summary list of patch and deployment information by package name for all applicable endpoints.

Optional Parameters: `Packages`, `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 263: Package Compliance Summary Report Columns

Column	Definition
Package Name	The name of the package.

Column	Definition
Endpoints Selected	The total number of endpoints included within the scope of the report.
Applicable Endpoints	The total number of applicable endpoints.
Endpoints Patched	The number of endpoints that are already patched.
Not Patched/Not Scheduled	The number of endpoints not patched, and have no deployment scheduled.
Not Patched/Scheduled	The number of endpoints not patched, but are scheduled for a deployment.
Deployments Completed	The number of deployments that have completed successfully.
Deployments Failed	The number of failed deployments.
Deployments In-Progress	The number of endpoints currently receiving the deployment.

Note:

- If a package has no associated deployment, it does not appear in the report.
- Endpoints marked as *Do Not Patch* are not included in the report data.

Patch Agent Configuration Report

This report provides a simple-to-read view of patch agent configurations. There are no options for this report. However, when generating this report, you must select an agent group.

Required Parameter: Selection of one `agent group`.

The following table describes each report field.

Table 264: Patch Agent Configuration Report Field Definitions

Field	Definition
Policy (Group) Information	
Name	The name of the selected agent group.
Description	A description of the selected group.
General Information	
Polling Interval (minutes)	Indicates the interval (in minutes) between agent and Ivanti Endpoint Security communication.
User Defined	Indicates whether the group policy is user defined or predefined.
Last Modified	The date and time the group policy was last modified.
Deployment Notification Options	

Field	Definition
Patch Deployment: User May Cancel	Indicates if deployment recipients can cancel deployments.
Patch Deployment: Users May Snooze	Indicates if deployment recipients can snooze deployments.
Patch Deployment: Deploy Within	Indicates the maximum time frame a deployment recipient can snooze deployments.
Reboot Notification Options	
Patch Reboot: User May Cancel	Indicates if deployment recipient can cancel reboots.
Patch Reboot: User May Snooze	Indicates if deployment recipients can snooze reboots.
Patch Reboot: Reboot Within	Indicates the maximum time frame a deployment recipient can snooze reboots.
Notification Window Options	
Patch Deployment: Always On Top	Indicates if the deployment notifications window opens on top of all other windows until the recipient acknowledges the notification (`yes` or `no`).
Patch Reboot: Always On Top	Indicates if the reboot notifications window opens on top of all other windows until the recipient acknowledges the notification (`yes` or `no`).

Patch Agent Inventory Report

This report provides the details of the agents with the patch module installed associated with the specified agent groups. This includes a pie chart that shows the patch status count for the agent groups and details (IP address, name, operating system, and status) for each agent.

Required parameters: Selection of one or multiple `agent groups`.

Optional parameters (default setting): `Sort By` (IP address, machine name, operating system [OS]), `Included OSs`, `Included IP adresses`.

The following table describes each report field and column.

Table 265: Patch Agent Inventory Report Field and Column Definitions

Field / Column	Definition
General Information	
Server Name	The Ivanti Endpoint Security server name.
Agent Groups	The agent groups included in the report.
Agent Status Summary	

Field / Column	Definition
Total Known Endpoints	The total number of endpoints with the patch module installed.
Agents Checking In	The number of agents communicating with Ivanti Endpoint Security.
Working	The number (or percentage) of patch modules that are working on a deployment.
Idle	The number (or percentage) of patch modules that are idle.
Sleeping	The number (or percentage) of patch modules that are sleeping due to hours of operation settings.
Agents Not Checking In	The number of patch modules that are not communicating with Ivanti Endpoint Security.
Offline	The number (or percentage) of patch modules that are offline.
Disabled	The number (or percentage) of patch modules that are disabled.
Agent Status Summary Graph	
Disabled	The number (or percentage) of patch modules that are disabled.
Idle	The number (or percentage) of patch modules that are idle.
Offline	The number (or percentage) of patch modules that are offline.
Sleeping	The number (or percentage) of patch modules that are sleeping due to hours of operation settings.
Working	The number (or percentage) of patch modules that are working on a deployment.
Total	The total number of patch modules assessed.
Agent Inventory Table	
Agent IP	The IP address of the endpoint the agent is installed on.
Agent Name	The name endpoint that hosts the agent.
Operating System	The operating system name and description.
Ivanti Patch and Remediation Status	The current status.

Patchable Status Report

This report returns the current status of the selected endpoints (or endpoints in the selected groups). In the report, each endpoint is listed in the **Endpoint Name** column. The report then provides information about the particular endpoint.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 266: Patchable Status Report Column Definitions

Column	Definition
Device Name	The name of the endpoint.
DNS Name	The name used by the Domain Name System (DNS) to identify the endpoint.
IP Address	The IP address of the endpoint.
OS Name	The operating system name.
OS Build No.	The operating system's build number.
OS Service Pack	The latest service pack applied to the operating system (if applicable).
Agent Version	The version of the agent.
Last Contact Date	The last date Ivanti Endpoint Security had contact with the agent.
Patchable Status	The reboot/chained status of the agent.
Group List	A listing of the groups, by distinguished name, to which the endpoint belongs.

Potential Data Leakage Report

This report returns a list of Windows-based endpoints that have removable storage.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each table column.

Column	Definition
AgentName	The name of the endpoint hosting the agent.
HardwareClass	The type of external storage device associated with the agent.
HardwareName	The name of the applicable external storage device.

Column	Definition
Quantity	The number of external storage devices associated with the agent.
IPAddress	The IP address of the agent.
DetectionDate	The date and time the endpoint and its external storage device(s) were detected.

Services Inventory Detail Report

This report provides information about the service associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 267: Services Inventory Detail Report Column Definitions

Column	Definition
Service Name	The name of the service.
Device Name	The name of the endpoint.
Service Startup State	The state the service should enter upon endpoint boot.
Service Current State	The current state of the endpoint.

Services Inventory Summary Report

This report provides summary information about the services associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 268: Services Inventory Summary Report Column Definitions

Column	Definition
Service Name	The name of the service.
Instances	The number of times this service occurs. (Within the parameters of the report.)

Software Inventory Detail Report

This report provides information about the software associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 269: Software Inventory Detail Report Column Definitions

Column	Definition
Software Program	The name of the software installed on the endpoint.
Device Name	The name of the endpoint.

Software Inventory Summary Report

This report provides information about the software associated with an endpoint and the endpoint status.

Optional Parameters: `Endpoints`, `Groups`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 270: Software Inventory Summary Report Column Definition

Column	Definition
Software Program	The name of the software installed on the endpoint.
Instances	The number of times this software occurs. (Within the parameters of the report.)

Vulnerability Analysis Report

This report summarizes the remediation status for the selected content items. The report lists each vulnerability affecting the selected endpoint or group. The report can also be generated for a single or multiple content items. In the report, each content item is listed in the **Vulnerability Name** column. The report also provides patch status details for each content item and if a deployment is required.

Optional Parameters: `Endpoints`, `Groups`, `Vulnerabilities`, `Custom Patch Lists`

Note: If no parameter selection is made, the report generates using all available data.

The following table describes each report column.

Table 271: Vulnerability Analysis Report Column Definitions

Column	Definition
Name	The name of the content item.
Content Type	The type of content in the content item.
Vendor	The name of the vendor that created the software in the content item.
Vendor Release Date	The date that the vendor released the patch.
Endpoints Selected	The total number of endpoints included within the scope of the report.
Endpoints Applicable	The total number of endpoints that the patch applies to.
Endpoints Patched	The number of endpoints that are already patched.
Endpoints Not Patched	The number of endpoints not patched.
Percent Patched	The percentage of applicable endpoints that are patched.

Note: If an endpoint (or group) is marked *Do Not Patch* for a content item, the **Endpoints Applicable**, **Endpoints Patched**, **Endpoints Not Patched**, and **Percent Patched** columns do not include that endpoint in their data.

Chapter 15

Using the Patch Module for Endpoints

In this chapter:

The Patch Module is the software that executes Ivanti Patch and Remediation functions on an endpoint.

When added to the Ivanti Endpoint Security Agent, the Patch Module scans the endpoint for vulnerabilities and uploads the scan results to Ivanti Endpoint Security. The results returned to Ivanti Endpoint Security server can be viewed at any time, even if the workstation is disconnected from your network. The scan results are used by Patch and Remediation to determine a vulnerability's applicability for each endpoint. If a vulnerability is applicable, the Ivanti Endpoint Security Web console displays the endpoint as `Not Patched`.

After adding the Patch Module, there is generally no additional user interaction required at the endpoint.

About Patch Module for Windows

The Patch Module for Windows communicates Patch and Remediation-related information about the host endpoint to the Ivanti Endpoint Security. The Patch Module is responsible for uploading endpoint data and downloading content.

The Patch Module for Windows 7 and later is managed through the **Patch Module Management Console**. With this user interface, you can launch Discover Applicable Update tasks, scan the endpoint

for system changes, view server information, configure proxy servers, and so on. You can install Patch Module for Window 7 and later on the following endpoint operating systems:

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Viewing the Patch Module

Viewing the Patch Module provides access to module functionality and connectivity data.

Open the Patch Module from the endpoint hosting it.

1. Open ***Windows Control Panel***.

   Step Result: ***Windows Control Panel*** opens.

2. Open the Ivanti Endpoint Security Agent.
3. Select the **Ivanti Patch and Remediation** panel.
4. Click **Ivanti Patch Module**.

   Step Result: The ***Patch Module Management Console*** opens to the ***Home*** page.

The Patch Module Management Console

You can use this console to configure behavior for the Windows version of the Patch Module. You can also use it to view communication data between the module and server.

This console includes the following information and settings:

The Management Console Toolbar

Within the ***Patch Module Management Console***, a toolbar is displayed. Use this toolbar to navigate within the Patch Module or perform module actions.

The following table describes each ***Patch Module Management Console*** toolbar button.

Table 272: Management Console Toolbar Buttons

Button Title	Button	Description
Backward		Returns you to the previously used ***Management Console*** information or settings.
Forward		Advances you to the information or settings you viewed prior to clicking **Backward**.
Scan		Launches an endpoint scan for system changes, which are uploaded to the server. Click the arrow to expand a menu.
Scan > **Scan**	N/A	Launches an endpoint scan for system changes, which are uploaded to the server
Scan > **Check for Deployments**	N/A	Launches check-in with the server for endpoint deployments. If a deployment is scheduled, you can complete it using ***Notification Manager*** controls.
Scan > **Deployment Service**	N/A	Opens the a dialog you can use to restart the Ivanti Patch Module service.
Tools		Opens ***Tools and Settings***. For additional information, refer to Tools and Settings on page 555.
?		Opens Help for ***Patch Module Management Console***. Click the arrow to expand a menu.
? > **Help**	N/A	Opens Help for the ***Patch Module Management Console***.
? > **Exit the Control Panel**	N/A	Closes the ***Patch Module Management Console***.
? > **About the Control Panel**	N/A	Opens the ***About*** dialog. This dialog lists the Patch Module trademark information.

The Home Page

The ***Patch Module Management Console*** opens to the ***Home*** page. This page lists module information and function.

The ***Home*** page includes:

- Compliance Banner
- Active Scan Statistics
- Status

The ***Home Page*** features a **Compliance Banner**, which lists the status of the deployment service. This banner displays whether the endpoint is compliant with corporate policies.

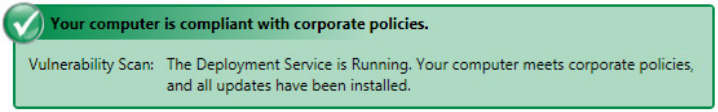


Figure 98: Compliance Banner Example

The following table describes each possible status.

Table 273: Compliance Banner Statuses

Color	Status
Green	**Your computer is compliant with corporate policies** The deployment service is running. Your computer meets corporate policies, and all updates are installed on your computer.
Orange	**The module is determining if your computer is still compliant with corporate policies** The deployment service is performing a vulnerability detection.
Red	**The module is unable to determine your computer's compliance with corporate policies** The deployment service is stopped and the module is offline.
Orange	**Your computer is not compliant with corporate policies** The deployment service is running and your computer requires a reboot to finish installing updates.
Blue	**Your computer has not been able to contact the management server** The deployment service is running and the module is in an unknown state.

Active Scan Statistics display only after clicking the **Scan** button. You can use the active scan statistics controls to start a scan if one is not already active. This section also displays the scan type, start time, duration, and status.

Table 274: Active Scan Statistic Fields

Field	Description
Scan Type	The type of scan that was performed.
Start Time	The time the scan was started.
Duration	The amount of time the scan lasted in minutes and seconds.
Signatures Evaluated	The phase of scan in progress.

Note: The scan start time and duration values are only populated if you started the scan. If the scan was running prior to you clicking the **Scan** button, the exact start time and duration are unknown.

Status fields indicate when the last endpoint scan took place.

Table 275: Status Fields

Field	Description
Last scan	The date and time of the last scan.
Update schedule	The communication interval between the module and server.
Definition date	The date and time of the definition file.
Patch module version	The version of the Patch Module installed and the date of installation.

Tools and Settings

Tools and Settings includes links to module configuration settings and utilities.

Tools and **Settings** can be expanded or collapsed by their arrow icons. The following links appear in ***Tools and Settings***.

Table 276: Tools and Setting Links

Link	Description
Settings	
Proxy Settings	Opens ***Proxy Settings***, allowing you to view of modify the module proxy configuration. For additional information, refer to Proxy Settings on page 556.
Logging	Opens ***Log Files***, allowing you to view or clear the module log files. For additional information, refer to Log Files on page 558.

Link	Description
Notification Manager	Opens ***Notification Manager***, allowing you to define the ***Notification Manager*** behavior. For additional information, refer to Notification Manager on page 559.
Tools	
Ivanti Endpoint Security Server	Opens ***Server Settings***, which lists information about your server. For additional information, refer to Server Settings on page 560.

Proxy Settings

Proxy Settings displays information about the proxy server used to download content and reroute communications between your server and the agent. You can also use the settings to define the proxy server manually.

Proxy Settings is divided into two sections:

- Server Provided Proxy Settings on page 556
- Client Defined Proxy Settings on page 557

Note: When installed, the Patch Module controls all communication with a proxy server rather than the Ivanti Endpoint Security Agent.

Server Provided Proxy Settings

This ***Proxy Settings*** section lists the FastPath server that the endpoint is currently using to route communication with the server, if applicable. FastPath servers are caching proxies applied to the endpoint by agent policy set.

You can expand or collapse this section by clicking the rotating chevron (**>**).

When the **Server Provided Proxy Settings** section is expanded, a table displays. This table lists information about each FastPath server assigned to the endpoint. For additional information about FastPath servers and how to assigned them to Patch and Remediation endpoints, refer to About FastPath on page 453.

Table 277: Server Provided Proxy Settings

Column	Description
Server	Lists the name of the FastPath server.
Port	Lists the FastPath server port used to route server and endpoint communications.
Authenticated	Lists whether the FastPath server requires authentication (`Yes` or `No`).

Server Provided Proxy Settings also includes the **Use a Proxy Server** check box. If your administrator has not assigned any FastPath servers to the endpoint, you can select this check box to manually define a proxy. For additional information, refer to Configuring Client Proxy Settings on page 557.

Client Defined Proxy Settings
This ***Proxy Settings*** section lists client provided proxy settings. You can define these settings after selecting the **Use a Proxy Server** check box in **Server Provided Proxy Settings**.

You can expand or collapse this section by clicking its associated arrow icon.

The following table describes each field you can define within **Client Defined Proxy Settings**.

Table 278: Client Defined Proxy Settings Field

Field	Description
Proxy Server Address	The name or IP address of the proxy server you want to use to route communication between the server and the endpoint.
Proxy Server Port	The port number the proxy server uses to route communication.

The **Client Defined Proxy Settings** section contains a sub-section, the **Proxy Authentication** section. When defining client proxy settings, define these settings if the proxy requires authentication.

To define these settings, select the **Enter your proxy authentication credentials** check box and type values into the fields described in the following table, which become available after selecting the check box.

Table 279: Proxy Authentication Field Descriptions

Field	Description
Username	A username that authenticates with the proxy.
Password	The username password.
Password Retyped	The password retyped.

Configuring Client Proxy Settings
If your Ivanti Endpoint Security administrator has not assigned your endpoint a FastPath server, you can configure the Patch Module to use a proxy server of your choice.

Tip: Ivanti recommends assigning proxy servers by Agent Policy Set instead. For additional information, refer to About FastPath on page 453.

Define proxy settings from the ***Proxy Settings*** options in the ***Patch Module Management Console***.

1. From the toolbar, click **Tools**.

   Step Result: ***Tools and Settings*** open.

2. Click **Proxy Settings**.

   Step Result: ***Proxy Settings*** open.

3. Ensure **Server Provided Proxy Settings** is expanded.

4. Ensure the **Use a proxy server** check box is selected.

   Note: If this check box is unavailable, you cannot define a proxy server because your administrator has already defined proxy servers using FastPath.

5. Ensure **Client Provided Proxy Settings** is expanded.
6. Define the following fields by typing the applicable information in them.
   The following table describes each field.

Field	Description
Proxy Server Address	The name or address of the proxy server you want to use.
Proxy Server Port	The port number the proxy uses to route server and module communication.

7. If the defined proxy require authentication, ensure **Proxy Authentication**, select the **Enter your proxy authentication credentials, and type the applicable information in the following fields:**

Field	Description
Username	A username that authenticates with the proxy.
Password	The password associated with the username.
Retype Password	The password retyped.

8. Click **Save**.

Log Files
The ***Log Files*** options contains buttons to open or clear the Patch Module log files.
The following table describes each ***Logging Files*** column.

Table 280: Logging Files Column

Column	Description
Name	The name of the log files.
Date Modified	The date and time the log files were last modified.
Size	The size of the log files in kilobytes.

Column	Description
Action	Buttons used to interact with logs. • Click **View** to open a log. For more information, see Opening Log Files on page 559. • Click **Truncate** to partially delete the log contents.

Tip: By default, logs are available at `<Program Files>\HEAT Software\HEATAgent\live\patch`

Opening Log Files
You can open Patch Module logging files to review Patch Module events.

Open log files from the ***Log Files*** page.

1. From the toolbar, click **Tools**.

   Step Result: ***Tools and Settings*** open.

2. Click **Logging**.

   Step Result: ***Log Files*** opens.

3. Click the **View** for the log you want to view.

Result: The log opens in the **Log Viewer**.

Tip:

- Click **Refresh** to update the log.
- Use the **Log Viewer** controls to reformat, magnify, or search for text.

Notification Manager
Use the ***Notification Manager*** options to define how Patch Module notifications display on the endpoint.

The following table describes each ***Notification Manager*** setting.

Table 281: Notification Manager Settings

Setting	Description
Notification Manager Version	Displays the version of the Patch Module Management Console installed on the endpoint.
Always Show Icon in System Tray	When selected, forces the Notification Manager icon to displays in the Windows system tray.

Server Settings

Server Settings contain information about the server that the Patch Module is registered with.

The following table describes each ***Server Settings*** field.

Table 282: Server Setting Field Descriptions

Field	Description
Ivanti Endpoint Security Server	The name of the server the Patch Module is registered with. Click the name open the Ivanti Endpoint Security Web console.
Ivanti Endpoint Security Server Version	The version of the server that the Patch Module is registered with.
Agent Center Version	The ***Patch Module Management Console*** version.

About Notification Manager

When the ***Deployment Wizard*** is configured to notify endpoint users of a deployment or a follow-up reboot, users are notified by ***Notification Manager***, a dialog that lets users proceed with actions related to the deployment.

Notification Manager displays when you have selected the following options while configuring the ***Deployment Wizard***:

- **Notify users of this deployment**
- **Notify users of the reboot**

You can also give users the ability to cancel or snooze deployment actions by selecting the following options:

- **Allow user to cancel**
- **Allow user to snooze**

For additional information, refer to Using the Deployment Wizard on page 260.

Completing a Deployment from an Endpoint

Although most deployments require no interaction, you may occasionally schedule one that does require user interaction. After you schedule a deployment configured to notify users, they will have to acknowledge it using ***Notification Manager***.

Based on how you configure the deployment, the user may also have the option of snoozing or canceling the deployment. Complete the deployment after ***Notification Manager*** opens.

1. Review the deployment text.

   This text displays information about the content being deployed.

2. [Optional] If you do not want to install the content immediately, snooze the deployment. Select an item from the **Remind me in** list.

   Note: You can only snooze if your administrator enabled this option.

3. When you are ready, install the content by click **Install**.

   Note: If multiple users are logged on the endpoint, each user must approve the restart before it can begin.

   Tip: You can click **Cancel** to abort the deployment if your administrator enabled this option.

Result: Installation of the deployment content begins.

Note: If you (or any other logged on user) do not begin the install by the time deadline, the install begins automatically.

Completing a Restart from an Endpoint

Some deployments require a restart to finish installation of new content. In most instances, you should notify endpoint users of these reboots so that so that they can save their work before the restart occurs.

Based on how you configure the deployment, the user may also have the option of snoozing or canceling the restart. Complete the restart after ***Notification Manager*** opens.

1. Review the restart text.

   This text displays information about why an endpoint restart is required.

2. [Optional] If you do not want to restart the endpoint immediately, snooze the restart. Select an item from the **Remind me in** list.

   Note: You can only snooze if your administrator enabled this option.

3. Save your work.
4. When you are ready, click **Restart Now**.

   Note: If multiple users are logged on the endpoint, each user must approve the restart before it can begin.

   Tip: You can click **Cancel** to abort the restart if your administrator enabled this option. An endpoint with a canceled restart is left in a chained state and must be rebooted to complete installation of content.

Result: The endpoint restart begins.

Note: If you (and any other logged on user) do not begin the restart by the time deadline, the restart begins automatically.

Chapter 16

Configuring Linux, UNIX, and Mac Endpoints

In this chapter:

You can use Ivanti Endpoint Security to deploy patch content to commonly used Linux, UNIX, and Mac endpoints.

This chapter includes information on how to:

- Get started setting up a local repository to support Linux and UNIX endpoints, if necessary.
- Configure your endpoints to support patching Linux and Unix endpoints.
- Use commands for the Patch Agent on Linux, Unix, and Mac endpoints.

Configuring Your Enterprise for Linux and Unix Patching

There are two ways to configure Linux and Unix endpoints for patching: configuring your server, or configuring your individual endpoints. Depending on the platforms you are supporting in your enterprise, your may need configure your server, configure your indivual endpoints, or both.

- If you support any platforms listed in Server Configuration to Support Linux and Unix Platforms, complete Configuring Your Server for Linux/Unix Patching on page 565. This workflow takes you through each procedure needed to:
  - Register your server with your Linux or Unix vendor.
  - Configure your server to function as a local repository.
- If you support any platforms listed in Endpoint Configuration to Support Linux and Unix Platforms, complete Configuring Your Linux/Unix Endpoints for Patching on page 566 to register the endpoints with their vendors and point them toward the main vendor repository. You must complete this procedure for each individual endpoint running on these platforms.

  Attention: If you are supporting any of the platforms listed in Endpoint Configuration to Support Linux and Unix Platforms, you should consider creating a dedicated local repository to host patch content (if you don't have one already). Newer Linux and Unix platforms cannot use the Ivanti Endpoint Security Server as a local repository due to vendor endpoint registration requirements. Creating a dedicated repository can substantially shorten deployment times and reduce bandwidth consumption. If want to use a local repository, follow the vendor documentation referenced in Using Ivanti Endpoint Security with Local Repositories on page 568 instead of completing *Configuring Your Linux/Unix Endpoints for Patching*.

- If you support platforms listed in both sections listed below, complete both Configuring Your Server for Linux/Unix Patching on page 565 *and* Configuring Your Linux/Unix Endpoints for Patching on page 566.
- If you support Ubuntu 14.04 LTS or 16.04 LTS, neither server nor endpoint configuration is required. Simply install the Patch Agent for Linux, UNIX, and Mac. For more information, see Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .

Server Configuration to Support Linux and Unix Platforms

If you support any of the following operating systems, you must configure your Ivanti Endpoint Security Server to function as a local repository.

- CentOS 5.5-6.x
- Novell SUSE Linux 10.x-11.x
- Oracle Enterprise Linux 5.5-6.x
- Oracle Solaris 10 Update 9
- SUSE Linux Enterprise 10 SP2-12

Endpoint Configuration to Support Linux and Unix Platforms

If you support any of the following operating systems, you must register each individual Linux or Unix endpoint with its vendor, and then point it toward a repository available either over the Internet or locally.

- Cent OS Linux 7.x

Note: CentOS Linux 5.5-7.x is a bit of an exception here. You *do not* have to register it with CentOS before it will work with Ivanti Endpoint Security. Skip Configuring Your Linux/Unix Endpoints for Patching on page 566 for CentOS Linux 5.5-7.x endpoints.

- IBM AIX 6.1- 7.1
- Oracle Enterprise Linux 7.x
- Oracle Solaris 11.x
- Red Hat Enterprise Linux 5.5-7.x

Endpoint Configuration to Support Mac Platforms

Configuring Mac endpoints for Patch and Remediation is easy to do. All you need to do is install the agent. After that, the agent takes care of the rest. For more information on agent install, see Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .

Configuring Your Server for Linux/Unix Patching

If you are patching older versions of Linux and Unix, you must subscribe to vendor content and then configure you Ivanti Endpoint Security Server to function as a local repository. Afterwards, install agents and deploy content to your endpoints.

Perform this procedure on your Ivanti Endpoint Security Server if you are supporting older Linux/Unix platforms.

1. Subscribe to the Linux or Unix vendor subscription network for each platform you're supporting in your enterprise.
   - My Oracle Support for Solaris
   - Oracle Unbreakable Linux Network
   - Novell Customer Center
   - HP IT Resource Center

   Note: You don't need a subscription for CentOS. It's free.

2. Notify Ivanti that you have a Linux or Unix subscription, and that you want to use Ivanti Endpoint Security to deploy patch content these platforms. We will update your licensing so that you can access patch content for your platforms.
3. From the Ivanti Endpoint Security Console, replicate with the Global Subscription Service.

   This action downloads new license information and the Content Credentials Manager, a utility you'll use in the next step.

4. From the Ivanti Endpoint Security Server, use Content Credentials Manager to subscribe to a vendor subscription network. Enter credentials for each subscription you have.

   Use this command-line utility to enter your vendor subscription credentials in the Ivanti Endpoint Security Server. Once you enter your credentials, Ivanti Endpoint Security uses them to connect to your vendor subscription network and download patch content. Instructions for using Content Credentials Manager on each supported platform are included. Note that the instructions for CentOS are a little different; since that OS doesn't require a subscription, it uses a different utility to simply enter the address information for a content mirror.

   - Solaris 10
   - Oracle Linux 5 and 6
   - Novell SUSE Linux 11
   - HP-UX 11.11, 11.21. and 11.31

5. From the Ivanti Endpoint Security Console, replicate again.

   Now that you have registered with your Linux/Unix vendors, complete a replication to download new patch content definitions.

6. Install the Patch Agent on your Linux and Unix endpoints.

   Instructions for installing the Patch Agent are available in the Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .

7. Deploy content to your endpoints.

   This process is similar to deploying Windows patch content using the ***Deployment Wizard***. The one discernible difference is setting content flags, a method used to set deployment behavior for a patch. Rather than using the regular options, you'll need to edit a text box to set deployment behavior.

Configuring Your Linux/Unix Endpoints for Patching

If you are working with newer Linux or Unix platforms, you must register your individual endpoints with the vendor before you can begin patching them. This registration is required because Linux/Unix vendors require entitlements on individual endpoints before they are eligible for content from the vendor's repository.

Attention: If you are supporting any of the platforms listed in Endpoint Configuration to Support Linux and Unix Platforms, you should consider creating a dedicated local repository to host patch content (if you don't have one already). Newer Linux and Unix platforms cannot use the Ivanti Endpoint Security Server as a local repository due to vendor endpoint registration requirements. Creating a dedicated repository can substantially shorten deployment times and reduce bandwidth consumption. If want to use a local repository, follow the vendor documentation referenced in Using Ivanti Endpoint Security with Local Repositories on page 568 instead of completing *Configuring Your Linux/Unix Endpoints for Patching*.

Perform this procedure on *all* newer versions of Linux/Unix endpoints you are supporting.

Note: CentOS Linux 5.5-7.x is a bit of an exception here. You *do not* have to register it with CentOS before it will work with Ivanti Endpoint Security. Skip this procedure for CentOS Linux 5.5-7.x endpoints.

1. Subscribe to the Linux or Unix vendor subscription network for each platform you're supporting in your enterprise.
   - Red Hat Enterprise Linux 5.5-7.x
   - Solaris 11.x
   - Oracle Enterprise Linux 7.x
   - Novell Customer Center
   - IBM AIX 6.1-7.1
2. Notify Ivanti that you have a Linux or subscription, and that you want to use Ivanti Endpoint Security to deploy patch content these platforms. We can update your licensing so that you can access this content.
3. From the Ivanti Endpoint Security Console, replicate with the Global Subscription Service.

   This action downloads your newly available patch content licensing.
4. Register your endpoints with your vendors and install entitlements on the endpoint.

   This process varies for each Linux/Unix platforms. The following links provide step-by-step instructions on how to complete this process for each supported platform.
   - Red Hat 5.5-7.x Endpoint Configuration (GUI) on page 575
   - Oracle Enterprise Linux 7 Configuration on page 577
   - Oracle Solaris 11 Endpoint Configuration on page 577
   - SUSE Linux 12 Endpoint Configuration on page 578
   - Configuring AIX 7.1 and 6.1 Endpoints to Download Content on page 579
5. From the Ivanti Endpoint Security Console, replicate again.

   Now that you have registered with your Linux or Unix vendor, complete a replication to download new patch content definitions.
6. Install the Patch Agent on your Linux and Unix endpoints.

   Instructions for installing the Patch Agent are available in the Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .
7. Deploy content to your endpoints.

   This process is similar to deploying Windows patch content using the ***Deployment Wizard***. The one discernible difference is setting content flags, a method used to set deployment behavior for

a patch. Rather than using the regular options, you'll need to edit a text box to set deployment behavior.

Note: If you have completed this workflow, you are likely using the default vendor repositories available on the Internet. When deploying patch content from a default repository to Red Hat Enterprise Linux 5.5-7.x, Oracle Enterprise Linux 5.5-7.x, SUSE Linux Enterprise 10 SP2-12, or CentOS Linux 5.5-7.x, deployments can exceed scheduled maintenance due to endpoints caching content from a remote location. To reduce likelihood of deployment that exceed maintenance schedules, Ivanti recommends splitting your deployment into two, smaller deployments using two new flags. These flags are only available for Red Hat Enterprise Linux 5.5-7.x, Oracle Enterprise Linux 5.5-7.x, SUSE Linux Enterprise 10 SP2-12, and CentOS Linux 5.5-7.x:

1. Complete the first deployment using the -CACHEPACKAGES flag. This flag instructs endpoints to cache the patch content you've selected, but not install it.
2. Complete the second deployment using the -INSTALLFROMCACHE flag. This flag instructs endpoints to install the patch content cached during the previous deployment.

Using Ivanti Endpoint Security with Local Repositories

If you are a Ivanti Endpoint Security administrator managing newer Linux platforms, creating a local repository and then pointing your endpoints toward them can substantially reduce deployment times.

When working with older releases of Linux and Unix, your Ivanti Endpoint Security Server functions as a local repository, which speeds deployment time by caching packages to your server.

If you only work with older release of Linux and Unix, don't read on any further; this doesn't apply to you. Refer to Configuring Your Server for Linux/Unix Patching on page 565.

However, if you are working with newer releases of Linux and Unix, you can substantially reduce deployment times by setting up a dedicated local repository, which is an on-premise mirror of the vendor repository. Because newer Linux and Unix platforms require each individual endpoint to register with the vendor, you cannot use your Ivanti Endpoint Security Server as a local repository. By setting up a dedicated local repository, you can maintain the deployment speeds while still conforming to Linux/Unix endpoint registration requirements.

If you want to set up a local repository, complete the following workflow. If you elect to use a local repository, skip completion of Configuring Your Enterprise for Linux and Unix Patching on page 564; The vendor documentation includes this information.

To use local repositories in conjunction with Ivanti Endpoint Security:

1. Set up a local repository for your vendor's patch content. Ivanti recommends following the vendor-provided documentation. This documentation includes information on how to set up local repositories and point your endpoints toward them.

Red Hat Satellite 6.0 Documentation	You can set up a local repository for RHEL 7.x using Red Hat Satellite 6.0. Red Hat refers to local repositories as *satellite servers*. This documentation includes info on: • How to set up a satellite server • How to configure your endpoints (which Red Hat refers to as *hosts*) to point toward the satellite server .
How to create a local Unbreakable Linux Network mirror	You can set up a local repository for Oracle Linux 7.x. Oracle Linux refers to local repositories as *Unbreakable Linux Network Mirrors*. This documentation includes info on: • How to setup an Unbreakable Linux Network Mirror. • How to configure endpoints (which oracle refers to as *clients*) to point toward the mirror.
How to Create a Local Package Repository for Solaris 11	You can setup a local repository for Oracle Solaris 11.x. If you use this documentation, skip over the content for Oracle Linux 6. It isn't relevant.
YaST: Setting up a local SUSE Linux update Server	You can set up a local repository for SUSE Linux Enterprise 12.x. SUSE refers to local repositories as *local SUSE Linux update servers*. This documentation includes info on: • How to setup a local SUSE Linux update server. • How to configure endpoints (which SUSE refers to as *clients*) to point toward the server.

2. Configure your endpoints to point toward your local repository. Refer to the vendor documentation above.
3. Install the Patch Agent on your Linux and Unix endpoints.

   Instructions for installing the Patch Agent are available in the Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .
4. Deploy content your endpoint.

   This process is similar to deploying Windows patch content using the ***Deployment Wizard***. The one discernible difference is setting content flags, a method used to set deployment behavior for a patch. Rather than using the regular options, you'll need to edit a text box to set deployment behavior.

Server Configuration Procedures

When setting up Ivanti Endpoint Security to be a local repository for a Linux or Unix platform, complete each of the following procedure for platforms you support.

Solaris Server Configuration

Enable enhanced content to allow Ivanti Endpoint Security server to download content directly from third parties rather than from the Global Subscription Service. This functionality leads to faster turnaround time when installing content.

If you are running the Oracle Solaris 10 or earlier operating system, you must configure your credentials with My Oracle in order to receive content.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Update Now**.

   Step Result: Replication between your Ivanti Endpoint Security (Ivanti Endpoint Security) server and the Global Subscription Service (GSS) begins.
3. When replication is complete, open a command prompt.
4. Navigate to the `Replication Services` directory. You can locate this directory here: `<Installation Directory>\HEAT Software\EMSS\Replication Services`.

5. From a command prompt, enter the following command and usage, replacing the variables listed below with the appropriate values:

```
CredentialsManager.exe /source:solaris /username:SolarisUserName /password:SolarisPassword
```

Note: If you use a proxy to separate your Ivanti Endpoint Security Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.

Result: You can now remediate your Oracle Solaris endpoints through using the Ivanti Endpoint Security server.

After Completing This Task:

Complete Updating Ivanti Endpoint Security System Files and Content on page 137. You cannot remediate your Oracle Solaris endpoints until your Ivanti Endpoint Security server replicates with the GSS.

You must also allow outbound access through ports 80 and 443 to the following URLs:

- https://getupdates2.sun.com
- http://getupdates.oracle.com
- http://a248.e.akamai.net

Oracle Linux Server Configuration

Enable enhanced content to allow Ivanti Endpoint Security server to download content directly from third parties rather than from Global Subscription Service. This leads to faster turnaround time when installing content

If you are running the Oracle Enterprise Linux operating system, you must configure your credentials on the Oracle Unbreakable Linux Network in order to receive enhanced content.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Update Now**.

   Step Result: Replication between your Ivanti Endpoint Security server and the Global Subscription Service begins.

3. When replication is complete, open a command prompt.
4. Navigate to the `Replication Services` directory. You can locate this directory here: `<Installation Directory>\HEAT Software\EMSS\Replication Services`.

5. From a command prompt, enter the following line, replacing the variables listed below with the appropriate values:

   `CredentialsManager.exe /source:oracle /u:username /p:password /csi:xxxxxxxx / hostname: computername /release: x /arch:architecture`

   Note:

   - You must perform this step for each Oracle Enterprise Linux subscription that you want Ivanti Endpoint Security server to remediate.
   - If you use a proxy to separate your Ivanti Endpoint Security Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.
   - For a complete list of commands, type `/source: oracle /HELP`.

   Step Result: A successful registration message displays.

After Completing This Task:
Complete Updating Ivanti Endpoint Security System Files and Content on page 137. You cannot remediate your Linux endpoints until your Ivanti Endpoint Security server replicates with the GSS.

SUSE Linux Server Configuration

Before you can deploy patch content to your SUSE endpoints, you must configure Ivanti Endpoint Security so that it can log in to SUSE repositories.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Update Now**.

   Step Result: Replication between your Ivanti Endpoint Security (Ivanti Endpoint Security) server and the Global Subscription Service begins.

3. When replication is complete, open a command prompt.
4. Navigate to the `Replication Services` directory. You can locate this directory here: `<Installation Directory>\HEAT Software\EMSS\Replication Services`.
5. From a command prompt, enter the following command. Replace the variables with your SUSE subscription credentials.

   `CredentialsManager.exe /source:suse /a:mirror /u:<username> /p:<password>`

   Note:

   - If you use a proxy to separate your Ivanti Endpoint Security Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.
   - For a complete list of commands, enter: `/source:suse /HELP` at the command prompt.

   Step Result: A successful registration message displays.

6. Optionally, you can list the operating system types registered with the Ivanti Endpoint Security server and validate the status of the channels providing enhanced content. Enter the following commands at the command prompt.
   - To list the operating system types registered with the server, enter: `CredentialsManager.exe /source:suse /list`.
   - To validate the status of the channels providing the enhanced content, enter: `CredentialsManager.exe /source:suse /validate`.

Result: You can now remediate your Novell SUSE Linux endpoints using Ivanti Endpoint Security server.

After Completing This Task:
Complete Updating Ivanti Endpoint Security System Files and Content on page 137. You cannot remediate your Linux endpoints until your Ivanti Endpoint Security server replicates with the GSS.

HP-UX Server Configuration

The Ivanti Endpoint Security server must be configured to download content directly from third-party vendors rather than the Global Subscription Service. This functionality leads to faster turnaround time when installing content.

If you are running the HP-UX operating system, you must configure your credentials with the HP IT Resource Center in order to receive content.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Click **Update Now**.

   Step Result: Replication between your Ivanti Endpoint Security server and the Global Subscription Service begins.

3. When replication is complete, open a command prompt.
4. Navigate to the `Replication Services` directory. You can locate this directory here: %Installation Directory%\HEAT Software\EMSS\Replication Services.
5. From a command prompt, enter the following lines, replacing the variables listed below with the appropriate values:

```
CredentialsManager /source:hpux /u:HP IT Resource Center UserName /p:HP IT Resource Center Password
```

Note: If you use a proxy to separate your Ivanti Endpoint Security Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.

Table 283: Credentials Manager configuration

Variable	Description
HP IT Resource Center Username	Your user name on HP IT Resource Center.

Variable	Description
HP IT Resource Center Password	Your password on HP IT Resource Center.

Step Result: A warning appears indicating that registering your server with the Credentials Management tool may result in a loss of patch deployment history and increased replication times.

6. Enter `Y` to acknowledge the warning and confirm the registration.

Note: You must perform the previous step and this step for each Red Hat subscription that you want Ivanti Endpoint Security to remediate.

Result: You can now remediate your HP-UX endpoints using Ivanti Endpoint Security.

After Completing This Task:
Complete Updating Ivanti Endpoint Security System Files and Content on page 137. You cannot remediate your Linux endpoints until your Ivanti Endpoint Security server replicates with the GSS.

Additionally, you must also allow outbound access through ports 80 and 443 to the following URLs:

- http://itrc.hp.com
- http://ftp.itrc.hp.com

CentOS Server Configuration

In environments containing CentOS endpoints, Ivanti recommends defining a Mirror site that your Ivanti Endpoint Security server can use to download CentOS Patch and Remediation content. Using a mirror site increases content download speeds and reduces download traffic from the CentOS community locations.

Define a content mirror using your Web browser and the Ivanti Endpoint Security server ***Computer*** dialog.

Note: Mirror site definition requires use of the Specify Site Mirror Tool. The Ivanti Endpoint Security Server downloads this tool during its first replication with the Global Subscription Service.

1. From any computer, obtain the address of the content mirror closest to your enterprise geographical location.
   a) Open your web browser and navigate to http://www.centos.org/download/mirrors/.
   b) From the list of mirrors, identify the mirror closest to your geograpical location. Write down or copy the mirror **HTTP Location**. Close the web browser when you're done.
2. From the Ivanti Endpoint Security server, open a command prompt.
3. From the command prompt, change directories to your Ivanti Endpoint Security Server Replication Services folder.
   Enter `cd %Installation Directory%\HEAT Software\EMSS\Replication Services`

4. Enter `SpecifyMirrorSite.exe /name:"name" /uri:"mirrorlist"`.

Note:

- This command only validates that the URI resolves. It does not validate CentOS data.
- Your Ivanti Endpoint Security must allow outbound access though ports 80 and 443 to the chosen mirror.
- If you use a proxy to separate your Ivanti Endpoint Security Server from the Internet, the proxy settings defined the Subcription Updates page are used during replication of Linux and UNIX content.

5. [Optional] Validate the CentOS mirror locations.

   Enter `SpecifyMirrorSite.exe/validate`.

Endpoint Configuration Procedures

When setting up newer Linux or Unix endpoints for patching, complete one of the following procedures on each Linux/Unix endpoint you support.

- Red Hat 5.5-7.x Endpoint Configuration (GUI) on page 575
- Red Hat 5.5-7 Endpoint Configuration (Terminal) on page 576
- Oracle Enterprise Linux 7 Configuration on page 577
- Oracle Solaris 11 Endpoint Configuration on page 577
- SUSE Linux 12 Endpoint Configuration on page 578
- Configuring AIX 7.1 and 6.1 Endpoints to Download Content on page 579

Note: Mac users, all you have to do is run the agent installer (you don't need to do any vendor registration). See Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) for info on installing the agent.

Red Hat 5.5-7.x Endpoint Configuration (GUI)

Before you can deploy patch content to your Red Hat Enterprise Linux 7 (RHEL) endpoints using Ivanti Endpoint Security, you must register the endpoint with Red Hat and subscribe to a repository. RHEL includes a wizard that makes this process fast and painless.

Complete this task from your RHEL 7 endpoints.

Note: This procedure contains basic instructions for attaching to the Red Hat repository. For more detailed information about attaching to different repositories, consult the RHEL Systems Registration Guide.

1. From the dashboard, search for `Red Hat Subscription Manager`. When it displays, click **Red Hat Subscription Manager**.
2. Enter your root password.
3. Click **Register**.

4. Define a server to register against.
   - To register with the RHEL repository, leave the default server name.
   - To register with a RHEL satellite server within your enterprise, type your satellite server name in the **I will register with** field.
5. If you will use a proxy to connect with the defined repository, click **Configure Proxy** and fill in the required information.

   If you aren't using a proxy, skip to the next step.
6. Click **Next**.
7. From ***System Registration***, enter your Red Hat account information.
8. If necessary, change your **System Name**, but in most cases just use the default.
9. Click **Register**.
10. When prompted, review your **Subscription**. If the info looks good, click **Attach** to connect to the repository.

Result: Your endpoint is subscribed to the entitlement you chose. Provided that the endpoint has a Patch Agent installed, you can begin deploying content to it.

Red Hat 5.5-7 Endpoint Configuration (Terminal)

Before you can deploy patch content to your Red Hat Enterprise Linux (RHEL) endpoints using Ivanti Endpoint Security, you must register the endpoint with Red Hat and subscribe to a repository. Power users can finish this process quickly using Terminal.

Complete this task from your RHEL endpoints.

Note: This procedure contains basic instructions for attaching to the Red Hat repository. For more detailed information about attaching to different repositories, consult the RHEL Systems Registration Guide.

1. Open ***Terminal***.
2. Elevate your privledges.
   a) Enter `sudo -s`
   b) Enter the root password.
3. Register the endpoint with RPM using your Red Hat Network credentials.
   a) Enter `subscription-manager register --username=`*`yourusername`* `--pasword=`*`yourpassword`*

      Step Result: If regitration completes successfully, ***Terminal*** displays your new RPM registration ID.

4. Subscribe to one or more entitlement.
   a) Enter `subscription-manager list --available | less`
      This command list the entitlements attached to your Red Hat Network account. Write down or copy the **Pool ID** for each entitlement you want to use for the endpoint.
      When you're done copying **Pool ID**s, close out the list by typing `q`.
   b) Enter `subscription-manager attach --pool=YourPoolId`

   Tip: You can subscribe to all entitlements for your Red Hat Network account by entering `subscription-manager attach --auto`

Result: Your endpoint is subscribed to the entitlement you chose. Provided that the endpoint has a Patch Agent installed, you can begin deploying content to it.

Oracle Enterprise Linux 7 Configuration

Before you can deploy patch content your Oracle Linux 7 endpoints, you have to register your endpoints with Oracle Unbreakable Network and attach to a repository.

You can complete this process either before or after you install the Patch Agent.

1. Open the dashboard and search for `ULN Registration`. When it displays, click **ULN Registration**.
2. Enter your root password.
3. Click **Forward**.
4. From the **Enter your account information** page, enter your Unbreakable Linux Network account information.
5. If your Oracle Linux 7 endpoint uses a proxy to access the Internet, click **Advanced Network Configration** to enter proxy information. Close the dialog when you're done.
6. Click **Forward**.
7. [Optional] Enter a **System Name** and choose whether to send Oracle your system profile data.
8. Click **Forward**.
9. Click **Finish** to complete registration.

Result: Your endpoint is subscribed to the Oracle Unbreakable Network. Provided that the endpoint has a Patch Agent installed, you can begin deploying content to it.

Oracle Solaris 11 Endpoint Configuration

Before you can deploy patch content to you Oracle Solaris 11 endpoints, you have to register your endpoints Solaris and attach a repository.

Complete this process from you Solaris 11 endpoints.

Note: This procedure will get your endpoints up and running, but it you need full documentation, you can find it at the Oracle Technology Network.

1. Download a certificate and key from Oracle so that the endpoint can access the Oracle Solaris 11 repository you're licensed for.
   a) Open a Web browser and navigate to http://pkg-register.oracle.com.
   b) Click **Request Certificates**.
   c) Sign in using your Oracle Account credentials.
   d) Select a repository and click **Submit**.
   e) If necessary, type a comment in **ADDITIONAL CERTIFICATE DATA**.
   f) Review Oracle's License Agreement and, if you agree to their terms, click **Accept**.
   g) Click **Download Key** and **Download Certificate**.

   Step Result: The certificate and key are downloaded. **Leave the Web browser open.** It contains instruction for installing your downloads.

2. Install the repository certificate you just downloaded on your endpoint.
   a) Open ***Terminal***.
   b) Follow the instructions listed in your Web browser.

Result: Your endpoint is subscribed to your licensed Solaris repository. Provided that the endpoint has a Patch Agent installed, you can begin deploying content to it.

SUSE Linux 12 Endpoint Configuration

Before you can deploy patch content to your SUSE Linux 12 endpoints using Ivanti Endpoint Security, you must register the endpoint with the SUSE Customer Center. SUSE 12 includes a wizard that makes this process fast and painless.

Complete this task from your SUSE 12 endpoints.

1. From the dashboard, search for YaST, open it, and then enter the root password.
2. Open **Online Update**.
3. When prompted, run the configuration workflow.
4. Enter the email address for your SUSE Customer Center account and your registration code.
5. If you have a local registration server, click **Local Registration Server** and enter its URL.
6. Click **Next** to begin registration.

Result: Your endpoint is subscribed. Provided that the endpoint has a Patch Agent installed, you can begin deploying content to it.

Important: While using Patch and Remediation to patch your SUSE 12 endpoints, you may need to disable the Snapper snapshot manager. If you leave it enabled, it takes two snapshots every time you make a deployment to your endpoints. These snapshots may lead to disk space issues. See Knowledge Base Article 1734 for information on disabling Snapper.

Configuring AIX 7.1 and 6.1 Endpoints to Download Content

To patch your AIX 6.1 and later endpoints using Ivanti Endpoint Security, your AIX endpoints must have Service Update Management Assistant (SUMA) enabled. SUMA is enabled by default, but you may need to configure some of its variables to work in your environment before you can begin patching the endpoint using Ivanti Endpoint Security.

1. Log on to your AIX endpoint.
2. Elevate your privileges.

   From the command line, enter `su` and your password.
3. Preview a maintenance download to check if SUMA is working correctly.

   Enter `suma -x -w -a Action=Preview`.

   The download preview may take a minute.

   Step Result: If the preview download succeeds, you'll see output similar to:

   ```
               ...
               Download SUCCEEDED: /usr/sys/inst.images/installp/ppr/
   wio.fcp.6.1.6.18bff
               Summary:
                       586 downloaded
                       0 failed
                       0 skipped
   ```

   If you see this in the command line, you're done! Don't worry about completing the next step.
4. If the preview download fails, SUMA is not configured correctly to work in your environment. You'll need to edit SUMA before you can use Ivanti Endpoint Security to patch AIX.

   a) From the command line, enter `smit suma`
   b) Select `Configure SUMA` and press **ENTER**.
   c) Press **ENTER** to select **Base Configuration**.
   d) Edit the list of options that appear for operations in your enterprise. When you're done, close SUMA.
   e) Once again, preview a maintence download to check if SUMA is working correctly.

      Enter `suma -x -w -a Action=Preview`.

Result: If SUMA is working correctly, you're all set to begin patching your AIX endpoints using Ivanti Endpoint Security. However, if you're still having trouble getting SUMA to work, contact your enterprise IT Helpdesk. You may have restrictive firewall settings in place that are interfering with SUMA.

Patch Agent Command Line Usage

The Patch Agent for Linux, UNIX, and Mac is a command line based application that does not have a user interface.

From the `usr/local/patchagent/` directory within terminal, you can enter a variety of commands to control the agent.

Table 284: Patch Agent Commands

Command	Description
`./patchservice info`	Indicates general information about the agent.
`./patchservice status`	Indicates the status of the agent process.
`./patchservice daustatus`	Indicates the status of the Discover Applicable Updates task.
`./patchservice detect`	Starts the detection task.
`./patchservice stop`	Stops the agent process.
`./patchservice restart`	Stops and starts the agent process.
`./patchservice patchdirectory`	Sets the directory where patches will be temporarily downloaded.
`./patchservice setmacro`	Specifies the macro definitions that should be used by the agent.
`./patchservice archivelogs`	Archives the agent logs so that they can be sent to Ivanti.
`./patchservice proxysetup`	Configures your proxy server.
`./patchservice clearAgentLog`	Clears the agent error log file.
`./patchservice clearErrLog`	Clears the agent error log file.
`./patchservice clearDetectLog`	Clears the agent detection log file.
`./patchservice trimlogs`	Reduces the size of the error, agent, and detect log files. Oldest entries are deleted and the file is truncated at 100,000 lines.
`./patchservice setagentnice`	Sets the agent's prioritization value.
`./patchservice help`	Displays the patch server script usage information.

Appendix
A

Glossary

In this appendix:

- Glossary

This glossary defines terms related to Ivanti Endpoint Security. Some terms apply to information technology in general, while others are specific to Ivanti Endpoint Security.

Glossary

This glossary contains list of terms related to Ivanti Endpoint Security, as well as their definitions.

A

AAA Architecture	In client/server networking, an architecture that combines three necessary elements of security, to make them available on one server and able to work with each other in a coordinated manner.
access control list (ACL)	A database file that stores information regarding entities that may request access to a network, as well as the rights and privileges to be granted upon request.
accessible endpoints	A feature that associates an individual endpoint with a particular role. This feature allows you to limit a user's permissions to specific endpoints. For example, you can limit a user with administrative rights to administration of a single endpoint.
accessible endpoint groups	A feature that associates an individual group with a particular role. This feature allows you to limit a user's permissions to specific groups. For example, you can limit a user with administrative rights to administration of a single group.
access rights	System privileges that determine whether or not a user can access an individual feature or page. There is an access right for each system page and function. Access rights for a user are determined by selecting rights for a user role, and then assigning that user role to the applicable user.

accounting	In network security architectures, records what users do once they are granted access to a network, or in the case of denied access, it can report how many failed attempts, and even details of the attempts.
Active Directory	Microsoft's trademarked system that centralizes the management of networked resources by making each item on a network, including most applications, objects in a relational database and then enabling the administrator to manage those objects through one management center.
active directory synchronization	The process by which the Application Control module synchronizes with a network active directory. This process crawls targeted active directories for users, user groups, endpoints, endpoint containers, and other data stored in the active directory.
Active Server Page	An HTML page that contains embedded server side scripting that is processed on a Microsoft Web Server before the page is sent to the user.
ActiveX	A technology, built on Microsoft's Component Object Model (COM), that enables software components, regardless of the language used to create them, to interact with one another in a networked environment.
Active Template Library	A Microsoft program library for use when creating ASP code and other ActiveX program components to run in a browser window.
Address Resolution Protocol	An OSI layer-3 protocol used to find an endpoint's MAC address using its IP address.
agent	A software routine that resides in background memory on a computer or other device and waits to perform an action when a specified event occurs.
Agent Management Job	Jobs that let you install agents upon endpoints within your network remotely. The first function of this job is to discover the targeted endpoints as in a *Discovery Scan Job*. The second function of this job is to install agents upon endpoints discovered during the first function. These jobs access the targeted endpoints by providing credentials specified during job configuration.
Agent Policies	The agent rules for communicating with the server. These rules include: communication interval, deployment notification options, discovery agent mode, hours of operation, logging level, and reboot notification options. Agent policies are assigned to groups, but any group that has not been explicitly assigned an agent policy will use the default system policy, as defined within the Ivanti Endpoint Security server.

agent policy conflict resolution	A series of protocols that determine which setting takes priority when a group or endpoint is assigned two or more agent policy sets with policies that conflict.
Agent Policy Sets	The combined selected agent policies as defined by the user. After their definition, these sets are then assigned to groups.
Application Browser	A navigation feature in Application Library which provides both predefined and user-defined views of the library's contents.
Application Control	A Ivanti Endpoint Security module that helps prevent the execution of malicious code and unwanted, unproductive software on a network. This module uses a security approach called *application whitelisting*, which allows only authorized applications to run on endpoints such as laptops, desktops, servers, and other IT resources.
application control log	A log that records Ivanti Application Control events for a given set of endpoints. These events include applications being allowed to run or being blocked by specific Ivanti Application Control policies. The application control log is an important tool for introducing, implementing, and maintaining application control in the enterprise.
application group	A user-defined grouping of applications in Application Library. Typically, an application group is a set of applications used by a group or organizational unit within the enterprise.
Application Library	A central area for managing all applications and executable files under application control. The Application Library is populated when an application scan is performed during Easy Auditor or Easy Lockdown. The administrator can then organize the executable files into applications and application groups.
application updater	Software used to update installed applications, which may involve adding, modifying, or replacing files on an endpoint.
application whitelisting	The security approach used by Ivanti Application Control to prevent the execution of malicious code and unwanted software by only allowing authorized applications to run. Such applications are either on an endpoint whitelist or permitted by a trust mechanism.
asset	An endpoint, along with all the hardware and software that is installed on that endpoint. Each endpoint, individual hardware device, and individual software application is considered an asset.
authentication	The process of identifying a user, typically through the use of credentials such as a user name and password, as the originator of a message or as the end point of a channel. High level authentication can use such other tokens as the originating IP address, or an encryption key, providing evidence of the authenticity of the request.

Authenticode	A technology based on information technology security industry standards that provides a method for developers to digitally sign their code. When code is signed, the company signing the code takes responsibility for the code and guarantees that the code is safe and free from viruses.
authorization vs. authentication	Whereas authentication is the process of verifying that a user is who they say they are, like having two forms of ID from different places, or dating paint and frame wood to verify authenticity of a painting, authorization is verifying the level of access available to that user, such as aisle and row seating stamped on a concert ticket, or possessing a back-stage pass.
authorization	The process of determining what level of access to grant a user to a system or software application function based upon their log in credentials.
Automatic Caching System (ACS)	A system that automatically writes packages marked critical to a memory queue, allowing administrators to have the critical and security-related patches available for rapid deployment.

B

baseline	In information technology, it is the base set of files that comprises a system, or the backup state available for reversions in the case of viral infection or other loss of data, such as when a system is restored from a backup.
behavior	A specific desired outcome for any patch or package deployment, configurable by the use of deployment flags and options.
blacklist	A centralized list of executable files (stored in the form of hash values) that are forbidden to run on endpoints under application control.
blocked application message	A message displayed when an end user tries to run a non-authorized application. This message can be customized by the Ivanti Application Control administrator.
browser	Software that allows the user to find, view, hear, and interact with material on a corporate Intranet or the World Wide Web.

C

chained deployment	The deployment of multiple packages in sequence, flagged to prevent reboot until the last of the chain has been deployed. Chained deployments are a Patch and Remediation module function

child hierarchy	The entire group hierarchy belows a specific group within the group hierarchy. Child groups have only one parent. Nesting child groups within parent groups creates an inheritance, which lets you apply one agent policy set to a parent and its children.
client	In computer networks, a client is any user, computer, node, server, or system that is requesting files from or access to some other system, regardless of whether it also acts as a server.
code signing	The process of digitally signing programs for verification purposes.
Common Vulnerabilities and Exposures (CVE)	A list of standardized names for vulnerabilities and other information exposures. CVE aims to standardize the names for all publicly known vulnerabilities and exposures.
communication interval	Determines how much time the Ivanti Endpoint Security agent will sleep between communication with the Ivanti Endpoint Security server. When the agent communicates with the server, it is checking for agent policy updates and deployments. This interval is critical since if the interval is too long, the agents will not get their tasks in a reasonable amount of time. If the interval is too short, the server may constantly be busy and other agents may not be able to get their tasks. Interval rates typically vary between 15 and 60 minutes depending on the number of nodes, network architecture and bandwidth.
components	The components that form Ivanti Endpoint Security. components come in two types: platform components and module components. Platform components form a basis for module components to operate. Module components are the individual security solutions used to prevent network security breaches.
Component Object Model (COM)	Microsoft's programming architecture in the Windows family of operating systems that enables software components to communicate between processes and fit easily into object-oriented program design. The family of COM technology includes COM+, Distributed COM (DCOM) and ActiveX.
compliance	An expression of whether the node being evaluated meets the Mandatory Baseline of content to make it safe for admission to the network in a quarantine arrangement. Usually expressed by the boolean true or false, a station can either be compliant or non-compliant. If non-compliant, it is set up for remediation and under quarantine until fully patched. This expression applies to environments with the Patch and Remediation module installed.

concurrent deployment limit	Defines the maximum number of Ivanti Endpoint Security agents that can receive active deployments at the same time. The purpose of the limit is to control the number of deployments to agents across the entire network and to reduce the chance of overloading your Ivanti Endpoint Security server. If an agent takes longer than 60 minutes to finish its deployment, it is no longer counted against this limit. This is the only value that cannot be overridden by a group's agent policy set, as it limits deployments for all agents. This option is available in environments with the Patch and Remediation installed.
content	Any type of content that the Ivanti Endpoint Security server can deploy to agents. Types of content include vulnerabilities, software, patches, hotfixes, and so on. Security content items contain pre-requisites, fingerprints, and signatures (all of which determine whether content is applicable to an endpoint) in addition to the package that contains the software to be installed. Content is available in environments with the Patch and Remediation module installed.
context	Pertaining to Microsoft Active Directory, context refers to the exact container position in the directory tree, thus allowing for the location of resources in a tree, by use of relative rather than fully qualified identifiers.
Control Panel applet	An application designed to be run within Microsoft Windows Control Panel. Ivanti's Control Panel applet allows easy interaction with the Ivanti Endpoint Security agent.
Coordinated Universal Time (UTC)	An international standard that allows for synchronization of events across many geographic zones. On a Ivanti Endpoint Security server, UTC might be chosen instead of local time if a scheduled event is desired to run at the same time at all sites, dependent also upon deployment constraints.
credentials	An object or objects presented along with a request for admission to a network or server that is used to validate the authorization of the presenter. Usually a credential is a combined user name and password, but can also consist of IP address, MAC address or an encryption key to verify that the request comes form an authorization location.
cross-platform	Portable or applicable to more than one operating system.

D

decryption	The process of converting ciphered text back to plain text after it travels across a public access medium. A previously determined key is used once the text arrives at its destination to convert the ciphered message back to clear text.
decryption key	A string of seemingly random bits of data used with cryptographic algorithms to create or verify digital signatures and unscramble cipher text back to its original clear text. Keys can be public or private and keeping at least one key private provides high security. Keys at least 128 bits long are considered more secure by modern standards, as many shorter ones have been cracked by modern computing technology.
deadline	When deploying patches or packages, it is the date and time by which a package or patch absolutely must deploy, and until which, a user may snooze a deployment if inconvenient. This term applies to environments with the Patch and Remediation module installed.
Definition file	A collection of signatures used by AntiVirus to identify and capture viruses and other malware.
Denied Applications policy	A managed policy that adds an application to a centralized blacklist. This explicitly stops the application from running for specified endpoints and users.
deployment flag	When preparing a package or patch deployment, the administrator has many options and flags that can be set to fine tune how and when the deployment occurs and what events accompany and follow the deployment. This function is available in environments with the Patch and Remediation module installed.
deployment	The planned delivery of content to any or all nodes determined to be non-compliant. Deployments are available in environments with the Patch and Remediation module installed.
device class	A group of physical devices or device drivers that have similar characteristics and that can be managed in a similar manner.
device collection	A group of target devices that can be managed in a similar manner.
dirty *C* state	Indicates that the Ivanti Endpoint Security agent received a chained deployment and the reboot is currently suppressed. While in the *C* state, the agent will only accept other chained deployments or a reboot deployment. Only a reboot deployment or manual reboot will clear this state. This term applies to environments with the Patch and Remediation module installed.

dirty *R* state	Indicates that the Ivanti Endpoint Security agent received a deployment that required a reboot and the reboot was suppressed. While in the *R* state, the agent will only accept a reboot deployment. Only a reboot deployment or manual reboot will clear this state. This term applies to environments with the Patch and Remediation module installed.
dirty state	The term used to describe an agent that displays a `C` or `R` on the ***Endpoints*** page of the Ivanti Endpoint Security server. Agents that are in a clean state display no such lettering. This term applies to environments with the Patch and Remediation module installed.
Discover Applicable Updates (DAU)	A predefined system task that launches the Ivanti Endpoint Security agent on a client endpoint. The DAU runs following subscription replication, five minutes after the application of a patch, after a reboot and when an agent checks in after the **ScanNow** button has been clicked in the Ivanti Endpoint Security server interface.
discovery methods	The methods used to designate targets (endpoints and devices) during discovery scan jobs. Endpoints and devices can be discovered using a single IP address, an IP address range, a single computer name, network neighborhood, or active directory.
discovery options	A series of queries and scans that collect information about targets defined for detection during discovery scan jobs. These options (which include Verify with PING, ICMP Discovery, Port Scan Discovery, SNMP Discovery, Windows Version Discovery, Resolve DNS Names, Resolve MAC Addresses, and Resolve NetBIOS Names) identify whether an endpoint is present, and, if one is, what its address and operating system information are.
Discovery Scan Job	A network-based scan run from the Ivanti Endpoint Security server that discovers assets in your network (endpoints, routers, switches, printers, and so on) by using user-specified IP addresses or asset names and/or domains. These jobs also discover additional information about assets (operating system, address information, and so on) through port scans, information queries, and address mask requests.
Distributed Component Object Model (DCOM)	An extension of the Component Object Model (COM) that extends COM's capabilities across network boundaries, allowing objects to communicate across a network. COM, unlike DCOM, is designed for interprocess communication on the same node or computer.

domain	On a local or wide area network, a domain is a set of network resources and services available to a group of users. Domains act as containers that can be identified by a name and address, which can then provide authorized users access to any elements they contain. Domains can also share resources with each other as trust is extended by administrators to those other domains.
Domain Name System (DNS)	The system used to name computers and especially servers for easier location. A domain name is a meaningful and human-readable name associated with an IP address. Domain names most often take on the format of domainname.com and the most common ones are associated with WWW locations.
Dynamic Host Configuration Protocol (DHCP)	A protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network by establishing a range of IP addresses to be assigned automatically and indexed. Without DHCP, managers would have to manually assign and keep track of each host IP address on the network.
dynamic-link library file (DLL file)	A file that has linked and compiled one or more functions used by a separate process, which can be loaded into the memory space of that process when the program is started or running.

E

Easy Auditor	A managed policy that scans an endpoint and authorizes the applications it finds by creating a whitelist of those applications. It does not block other applications from subsequently installing and/or running, but it does not add these later applications to the whitelist.
Easy Lockdown	A managed policy that scans an endpoint and authorizes the applications it finds by creating a whitelist of those applications. It blocks other applications from subsequently installing or running, thereby enforcing application control.
encryption	The process of converting clear, readable text to ciphered text before it travels on network media, so that it can only be read or understood by a recipient with the proper decryption key. Some of the most secure encryption methods include RSA, AES, IKE, MDS, SSL, and SHA-1.

encryption key	A string of ciphered bits used with cryptographic algorithms to create or verify digital signatures and scramble clear text to protect it from being intercepted and read while traveling across public networking media. Keys can be public or private, and keeping at least one key private provides high security. Keys at least 128-bits long are considered more secure by modern standards, as many shorter ones have been compromised by modern computing technology.
Endpoint	In a client/server network architecture, an endpoint is any node that is a destination of two-way communication, whether requesting or responding. Additionally, in regard to the Ivanti Endpoint Security, the term endpoint is synonymous with any computer in your network that can have an agent installed.
executable file	The type of file recognized and managed by Ivanti Application Control to implement endpoint security. Specifically, it is any file that conforms to the Portable Executable (PE) format. These include `.exe`, `.dll`, `.sys`, `.ocx`, `.cpl`, `.drv`, and `.scr` files.

F

False positive	An antivirus scan result where a file is wrongly suspected to be infected by a virus or other malware. This term applies to environments with the AntiVirus module installed.
file shadowing	A feature that tracks the data read, written to, or written from a device. Depending on the configuration, either copies of the files are created or only filenames are recorded.
File Transfer Protocol (FTP)	A protocol that uses simple, clear text. Thus, it is a non-secure protocol used to exchange files between computers on a network or the internet.
fingerprint	A group of unique identifiers used to determine the presence of a patch, and/or vulnerability, and/or content item. Fingerprints can include unique files, file attributes, directories, registry keys or data values. This term applies to environments with the Patch and Remediation module installed.
firewall	A firewall is a set of related programs located at a network gateway server that protects the resources of a private network from unauthorized access.
fully qualified domain name (FQDN)	The domain name is a unique identifier for any resource located within a domain or network. A FQDN is the full name of any network entity starting with its hostname and ending with the exact domain name in which it resides. Example: johnq.accounting.acme.com

G

Global Subscription Service (GSS)	The central repository where security content is stored for retrieval by the Ivanti Endpoint Security server. The GSS also serves as the Ivanti Endpoint Security licensing server.
globally unique identifier (GUI)	A 128-bit number generated by Windows operating systems or one of its applications, which is assigned to any object in a two-way communication, be it user, application, or component. The algorithm used to generate GUIDs combines a few unique settings, such as IP Address, MAC Address, and clock date and time to create an even more unique identifier.
Group	A targeted collection of computers created and named for the purpose of deploying distribution packages, defining agent policies, setting Mandatory Baselines, or reporting. Groups provide a simple way to manage computers that have similar requirements rather than managing each computer separately.

H

hostname	The name given to identify each node of a network. The hostname usually describes either the user that operates the node, its position in a building, or its function. Hostname is intended to be more human friendly than numeric IP Addresses.
hours of operation (HOP)	When enabled, this value determines when the agents start and stop communicating with the Ivanti Endpoint Security server. If the agent is in the middle of a deployment and the agent's hours of operation expire (exceed the designated stop time) it will finish what it is currently working on and continue the rest of the deployment at the next hours of operation interval. This term applies to environments with the Patch and Remediation module installed.
HTML	The accepted publishing language of the World Wide Web. It is a universally accepted standard for displaying links, images, and text in a format that computers around the world can read. There are currently many advantages in HTML that allow for an increasing number of different types of objects to be added to and displayed in a browser page.
HTTP	The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
HTTPS	A Web protocol built into most browsers that encrypts and decrypts user page requests as well as the pages that are returned via HTTP over SSL by the Web server.

hyperlink	Generally a different color from the surrounding text, a hyperlink is a coded reference to another location in the document, or to a URL or network address, usually written in a form of HTML code or JAVA, and is most prevalent on Web pages.

I

Internet Assigned Numbers Authority (IANA)	An administrative organization that assigns internet host addresses and other numeric constants used in Internet protocols.
inventory	The hardware, software, services, and operating systems that operate on an endpoint. During scanning, the Ivanti Endpoint Security agent compiles a listing for each item in an endpoint's inventory. Some unclassifiable items, such as serial numbers, are also included in an endpoint's inventory. This term applies to environments with the Patch and Remediation module installed.
IP (Internet Protocol)	The best known and main protocol in a suite of protocols known as TCP/IP that carry all traffic on the internet currently. IP is a connectionless protocol, meaning it does not wait for confirmation that it was received before sending the next packet. It is designed for long distance carriage of packets of data, as was originally the plan with Arpanet, which later became the internet.
IP address	The 32-bit (4 dotted divisions of eight binary digits) numeric identifier for any device on a network that distinguishes it from other devices and allows for routers and switches to group devices and their communication packets. The 32-bit dotted format is soon to be replaced by IPv6, which will expand the number of available IP addresses to keep pace with the enormous growth of the internet in recent years. Example: IP address 192.168.0.1 would be read by a router as 11000000.10101000.00000000.00000001.

J

JAVA	A programming language invented by Sun Microsystems. It can be used as a general purpose application programming language with built-in networking libraries. It can also be used to write small applications called applets.
JAVA Runtime Environment (JRE)	Created by Sun Microsystems, it is the core set of files necessary to execute JAVA written programs in any OS environment. JAVA is used because it is cross-platform, which is increasingly necessary in the current Web-based world.

L

library	A collection of precompiled routines, sometimes called modules, that are stored in object format for reuse by a program.
Lightweight Directory Access Protocol (LDAP)	A software protocol that enables the use of Directory Services to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet.
limited broadcast	The broadcast method Ivanti Ivanti Wake on LAN uses to wake network endpoints. Limited broadcast uses the IP address 255.255.255.255 to send a wake request to all endpoints in your network.
localhost	The default name describing the computer address also known as the loopback address of the computer. On Web servers, this loopback can be used to test the default Web page. To access this page, type http://127.0.0.1 or http://localhost.
localprofile.txt	An XML file found in the `%Installation Directory%\HEAT Software\EMSSAgent\live\patch\`, this file is maintained by the Ivanti Endpoint Security agent and contains information on computer's name, services, software, hardware, operating system, and support pack level. The refresh inventory data system task uses the information in this file to populate computer inventory data on the Ivanti Endpoint Security server.
Local Authorization	A Trusted Change policy that allows a specified user/endpoint combination to temporarily authorize an application that is not currently on a whitelist or permitted by another trust mechanism.
Ivanti Content Wizard	Ivanti Content Wizard (HCW). An addition to Ivanti Endpoint Security that provides the ability to define custom detection reports, deployment packages, signatures, and fingerprints. It has an easy-to-use graphical interface that illustrates all associated subcomponents of the patch in a single view.
Ivanti Endpoint Security	An application that serves as a platform for other applications that protect your network from security risks. These applications, called *modules*, use different approaches to protect your endpoint. Ivanti Endpoint Security is composed of a server component and an agent component. The server component is installed on a server within your network. The agent component is installed on network endpoints you want to protect from security risks. Ivanti Endpoint Security is accessed via a Web UI.

Ivanti Endpoint Security administrator	Any user who is assigned any of the access rights that control the functionality of the Ivanti Endpoint Security server or its deployments is considered a Ivanti Endpoint Security administrator.
Ivanti Endpoint Security Agent	The Ivanti Endpoint Security agent is a service that runs on each node and queries the Ivanti Endpoint Security server to receive any deployments that become ready. The behavior of the agent is defined by the agent's policies, whether it is using the default agent policies of the Ivanti Endpoint Security server or the group's agent policies.
Ivanti Endpoint Security Server	The central system in Ivanti Endpoint Security that manages content retrieval, vulnerability detection, and package deployment to all registered computers on the network. As a sophisticated, automated central repository of the most current security content available for a network, it maintains communication with the Ivanti Endpoint Security agent on nodes, across many key networking platforms, on the network, and detects any vulnerabilities with the help of the agent on each node.
Ivanti Endpoint Security user	Any user who has access to authenticate in to the Ivanti Endpoint Security server is considered a Ivanti Endpoint Security user.

M

MAC address	A 12-digit hexadecimal address that is burned into network cards and networking devices to allow for unique reference.
macro	Within Ivanti Endpoint Security, a macro is an environment variable that represents a filename, directory path, or a series of commands, actions, or keystrokes that can only be executed by the Ivanti Endpoint Security agent.
Malware	Malicious software developed for the purpose of causing harm to a computer system, such as viruses, Trojan horses, spyware, and malicious active content. This term applies to environments with the AntiVirus module installed.
Managed Policy	An application control policy that creates or supplements a whitelist of authorized applications, or a blacklist of blocked applications. These policies include Easy Auditor, Easy Lockdown, Supplemental Easy Lockdown/Auditor, and Denied Applications.

Mandatory Baseline	The absolute minimum set of content or locally-created distribution packages that must be installed on the group's computer members. In terms of content reports, a Mandatory Baseline will continually verify that the content is actually installed, and, if it is not, it will deploy the necessary distribution packages to bring the computer into compliance. This feature is available in environments with the Patch and Remediation module installed.
Memory Injection Policy	An Application Control policy that monitors running processes for reflective memory injection. It can be configured to audit and/or stop a process when memory injection is detected.
Microsoft Management Console (MMC)	A Windows-based application, that allows administrators to perform management tasks of Windows-based hardware, software, and networking components. This feature is available in environments with the Remote Systems Management module installed.
Microsoft SQL Desktop Edition (MSDE)	An enabling technology that provides local data storage and is completely compatible with the SQL Server version 7.0 code base. This technology transforms Microsoft Access from a simple file-server database application into an extremely powerful and highly scalable client-server solution for any size organization.
Module Components	Individual security solutions used to prevent various types of security breaches within your network. Each module plugs in to the Ivanti Endpoint Security platform and can be purchased individually. Some module components come installed with the Ivanti Endpoint Security platform and require no additional licensing.
Module Sub Components	The two parts that form a module component. Each module component consists of a server sub component and an endpoint subcomponent. These subcomponents work together to form a module's functionality.
MSI installer	Designed for Windows networks that use the Windows software installer mechanism. The MSI installer can be edited to include the Ivanti Endpoint Security server name and serial number. In this way, the agent can be deployed through the use of group policy agents.

N

NetWare	Networking OS that has played a major role in the development of Local Area Networking over the past few decades, being an early Network OS to use the Directory Services concept.
Novell Directory Services (NDS)	The relational database that contains all the resources on a Novell network, and provides security, and access for all resources.

NSLOOKUP MS-DOS® command	A command line function, which performs a reverse lookup on an IP address by querying the Domain Name System (DNS) server of an endpoint computer. This feature is available in environments with the Remote Systems Management module installed.

O

Open Software Description (OSD)	Creates a standard way to describe software components, their versions, underlying structure and relationships to other components. OSD is the standard language used when performing automatic software distributions and updates over the Internet.
Operating System Pack (OSP)	Contains all vulnerability detection information needed by an agent for a given operating system. It is generated by the DS and is passed to the agent during the DAU task. When a vulnerability replication executes, it checks to see if any operating systems received new data and it will automatically schedule the DS to regenerate the OS Packs for those operating systems.
Open Vulnerability Assessment Language (OVAL)	The common language for security experts to discuss and agree upon technical details about how to check for the presence of vulnerabilities on computer systems. The vulnerabilities are identified using gold-standard tests, OVAL vulnerability definitions in XML, and queries in Structure Query Language (SQL) that can be used by end users or implemented in scanning tools.

P

package	A package contains all the actual patch software and executable code for deployment. A package can run tasks or scripts, install software applications, place files (or directories of files) in a specified location, change the configuration of applications or services, or perform various other tasks that can be done in an unattended manner. The majority of packages contain the patches for vulnerabilities, defects, or bugs. This term applies to environments with the Patch and Remediation module installed.
package script	The script that performs the functions required to start package installation. Can be written using Microsoft VBScript, Microsoft JScript, or command line script. This term applies to environments with the Patch and Remediation module installed. Documentation regarding these languages can be found at MSDN Library: Scripting (http://msdn2.microsoft.com/en-us/library/ms950396).
parent hierarchy	Refers to the entire group hierarchy above a specific group within the group hierarchy.

Patch and Remediation	A Ivanti Endpoint Security module you can use to apply hotfixes, patches, service packs, and other content to agent-managed endpoints. Content is first deployed from the Ivanti Endpoint Security Server, and is then installed on endpoints by the Ivanti Endpoint Security Agent.
patch management	The systematic deployment, installation, and auditing of applicable hotfixes, patches, and service packs to operating systems and software applications. This process must incorporate the organization or people needed to administer the patches, the processes needed to ensure the proper testing, the inventorying of existing patch levels, the identification of needed patches, and the technology to deploy and apply the appropriate patches.
Ping MS-DOS® command	A command line function that verifies that an IP address exists and can accept requests, and is commonly used to help troubleshoot connectivity problems within a network. This feature is available in environments with the Remote Systems Management module installed.
Platform components	The essential components needed for Ivanti Endpoint Security operation. These components include the Ivanti Endpoint Security Web console, the Ivanti Endpoint Security database, and the Ivanti Installation Manager.
policy server	In a network designed with protections against unauthorized admission, it is where the rules and policies are stored that are the standards by which admission decisions are made. Rules can then be enforced by routers or some other form of firewall protection.
port number	The port number is carried in internet transport protocols to identify which service or program is to receive an incoming packet. Certain port numbers are permanently assigned to particular protocols by the IANA. For example, e-mail uses port 25 and Web services use port 80.
portable encryption	The encoding of data on a portable device or media into a form in which meaning cannot be assigned without the use of a confidential process or key.
posture	A term used by Cisco to refer to the state of readiness of a node requesting admission to a network, which will determine, when compared to the rules on the policy server, what degree of access if any, the node may be granted to the network. No access is usually termed as quarantine.
prerequisite	A requirement, such as the existence of a software package, file, and/or registry entry, that must be met prior to the deployment or installation of a patch.

proxy server	In an enterprise that uses one of the Internet protocols, a proxy server is a server that acts as an intermediary between a client and an Internet server. The proxy server allows an enterprise to ensure security and administrative control.
PuTTY	A free and open source terminal emulator application, that allows Windows users to connect to remote systems over the Internet using SSH, Telnet, and Rlogin network protocols. This feature is available in environments with the Remote Systems Management module installed.

Q

Q-chain (QChain.exe)	The utility Microsoft provides to chain hotfixes on Microsoft Windows NT, 2000, 2003, 2008, XP, or Vista.
Quarantine	A secure folder that holds files suspected of containing a virus or other suspicious code. An Administrator can review the contents to decide what items are safe (for example, false positives) or should be deleted. This term applies to environments with the AntiVirus module installed.
quiet mode	When set to quiet mode, a deployment package will suppress all user interfaces during installation.

R

Reflective Memory Injection	A technique for excuting external code within an authorized process, bypassing an endpoint's whitelist enforcement mechanism. This is sometimes (though not always) the result of a malware attack.
Refresh Inventory Data (RID)	Prevents certain log files from getting too large. RID is handled differently on the various platforms; some delete the files when they reach a certain size, while others will trim the file, leaving the most recent data but shrinking the file size.
registry	The registry serves as a central data repository for system and application-specific configuration data on a Windows machine. A registry contains keys, which are like directories in a Windows file system. Each key can contain values (the registry equivalent of a data file) or nested subkeys (the registry equivalent of a nested folder). Just as with files or folders, you can identify a registry key by building a full path to it.
remediation	Installing a countermeasure to reduce or neutralize the risks associated with a vulnerability. This term applies to environments with the Patch and Remediation module installed.

Remote Systems Management	A platform component within Ivanti Endpoint Security that provides administrators a simple way to remotely manage devices from the Ivanti Endpoint Security Web console. This feature is available in environments with the Remote Systems Management module installed.
replication	The process whereby the Ivanti Endpoint Security server receives daily scheduled updates of patches from the GSS. The schedule replication time of day can be manually overridden daily by clicking **Update Now**.
report	Records that document activity and information pertaining to your network environment. Within the Ivanti Endpoint Security server, you can generate reports for virtually every function that the server and agent performs: endpoint inventory, the results of discovery scan jobs, the status of a deployment, and so on.
Reverse Address Resolution Protocol (RARP)	Literally, the reverse of Address Resolution Protocol, RARP resolves an IP address from a given hardware, or MAC address.
rules	Statements of conditions that must be met or parameters that will determine an action to be taken. Rules can be positive or negative, but usually are stated simply and clearly such as "if member of group ADMIN, run superuser.bat."

S

Sandbox	A behavior-based technology that examines files for suspicious activities. It can detect new viruses or variants that do not yet have a signature, and delete or quarantine them. This term applies to environments with the AntiVirus module installed.
Secure File Transfer Protocol (SFTP)	A secure version of FTP, SFTP is designed to provide some encryption capabilities for file transfer over a network. Functionally similar to FTP, SFTP instead uses SSH to transfer files, so it cannot be used with a standard FTP client.
Secure Sockets Layer (SSL)	A security protocol that provides data encryption, message integrity, and client/server authentication for the transmission of private information and documents over the internet. SSL is available with either 40-bit or 128-bit encryption. However, 40-bit has been compromised in recent years, making 128-bit the lowest level anyone should go for secure encryption.
Self-Updating Trusted Updater	A Trusted Updater application that can update itself and continue functioning as an updater that can add files to an endpoint's whitelist.

server	A server is a computer or software application that provides data to client computers or software applications. A single computer running multiple software applications can simultaneously perform the function of multiple servers, multiple clients, or any combination thereof.
signature	Used to recognize a specific combination of installed software applications, services, and operating systems. A signature typically contains multiple fingerprints.
snapshot	A snippet of data taken at a pre-configured interval.
source group	Groups that automatically assigned managed endpoints to associated custom groups.
Spyware	Software that obtains information from a user's computer without their knowledge or consent. This term applies to environments with the AntiVirus module installed.
SQL Server	A trademark for a Microsoft database server that uses SQL. SQL Server is a popular database management system for Windows NT environments.
structured query language (SQL)	A database language used by administrators of relational databases to query, update, and mange data. It enables the administrator to use clear syntax that is descriptive of whatever action is wanted.
SSL Certificate	An electronic certificate consisting of a set of keys, one public, one private, exchanged between a Web server and a requesting client. A session is created, and a unique session key ensures a high level of encryption of any sensitive data passed between the client and server, preventing interception or unauthorized use of that data by any other entity.
standard deployment	The deployment of a standard, non-chainable package, or the deployment of a chainable package in a non-chainable state. This function is available in environments with the Patch and Remediation module installed.
Supplemental Easy Lockdown/Auditor policy	A managed policy that adds an application to an endpoint's existing whitelist of applications that are permitted to run. This type of policy is used to authorize an application after Easy Auditor or Easy Lockdown has been applied.

T

TCP/IP (Transmission Control Protocol/Internet Protocol)	The main suite of communications protocols used to connect hosts on the Internet, and now the prevalent LAN protocol even when other protocols are available.

transaction log	A Web server file that records a history of actions such as data changes. This log is used to roll the Web server back to a stable condition should the database be found in an inconsistent state.
trust	In domains, a trust relationship will allow members of one domain, when properly logged in and authenticated, to access services available on another domain.
Trusted Change policy	Any of the four policies that use the concept of trusted change to manage and authorize applications that are not on an endpoint's whitelist. These policies include Trusted Updater, Trusted Publisher, Trusted Path, and Local Authorization.
Trusted Path	A Trusted Change policy that specifies a file system path such that any executable files it contains can be run by the users/endpoints that have been assigned this Trusted Path policy.
Trusted Publisher	A Trusted Change policy that allows applications with a digital signature from a recognized, trusted source to execute on an endpoint.
Trusted Updater	A Trusted Change policy that allows an application (typically a software distribution or update tool) to add or modify files on an endpoint. These files are added to the endpoint's whitelist and are thereby authorized to run. Trusted Path is the only trust mechanism that adds applications to the whitelist.
trust mechanism	Any of the mechanisms that form the basis of the four Trusted Change policies - Trusted Updater, Trusted Publisher, Trusted Path, and Local Authorization.

U

URL (Universal Resource Locater)	The address that is the formal access name for a network or Internet resource. It usually begins with the protocol identifier, such as http or ftp. Thus, http://www.yahoo.com is a URL for the domain yahoo.com.
user	A profile used to access the Ivanti Endpoint Security server. These profiles include credentials (a user name and password) and an assigned role that determines the user's access rights within the system.
User Datagram Protocol (UDP)	A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses *Internet Protocol*. It is one of the most common connection based protocols in use on the internet, the other being TCP.

user name	The unique name used to gain access to a computer and/or network. User names and passwords are required in multi-user systems.

V

VeriSign certificate	A VeriSign certificate is issued by VeriSign, Inc. to verify a company's identity and enables the company to digitally sign programs and prove the authenticity of a Web site address.
Virtual Network Connection (VNC)	A graphical desktop sharing application, that allows you to view and interact with another computer over a network or Internet. This feature is available in environments with the Remote Systems Management module installed.
vulnerability	A weakness in a system that would allow an attacker to compromise system confidentiality, integrity, or availability. Alternatively, it can also be a breach from the original design, concept, or intended behavior of a computer's hardware or software that leaves the computer, or any piece of it, in an exposed state. Malicious users can use this to force other unintended actions to be performed. Vulnerabilities are often caused by defects or bugs, though this is not always the case. Many times the very configuration may result in unexpected exposures. Even out of date documentation may be labeled as a vulnerability, as not informing a user of how to perform actions in the preferred manner may result in systems being widely exposed. This term applies to environments with the Patch and Remediation module installed.
vulnerability report	A series of signatures and fingerprints designed to determine if a computer is a susceptible to a vulnerability and if the computer has been patched.

W - Z

Ivanti Wake on LAN	A Ivanti Endpoint Security module that uses magic packet technology to power on managed-endpoints.
Wake Request	A network packet containing code that wake recipient endpoints from a suspended, hibernating, of powered-off state. Ivanti Ivanti Wake on LAN sends these requests to network endpoints. This term applies to environments with the Ivanti Wake on LAN module installed.
wakepoint	An endpoint that receives wake requests from Ivanti Ivanti Wake on LAN and relays it to other network endpoints using limited UDP broadcast. One wakepoint must be defined within the network to wake agent-managed endpoints remotely.

Web server	A program that publishes content using the HTTP protocol so that it can be viewed using any type of compliant browser from any location on the connected Intranet or Internet.
whitelist	A list of executable files (stored in the form of hash values) that are authorized to run on an endpoint. A whitelist is created when an application scan is performed on the endpoint during Easy Auditor or Easy Lockdown.
widget	A graph or chart displayed on the Ivanti Endpoint Security ***Home*** page that depicts Ivanti Endpoint Security and Ivanti Endpoint Security module activities.
Windows Remote Desktop Connection (RDC)	A Microsoft proprietary tool, whose function is to provide a simple interface to access applications and data on a remote Windows computer via a network. This feature is available in environments with the Remote Systems Management module installed.
World Wide Web (WWW)	A commonly used name for the Internet, the WWW is a Web of connected Domains of local computers, which can share information with authorized users whom connect from anywhere else on the Web. Due to the exponential growth in recent years, a good way to check on current standards is to visit the World Wide Web Consortium (http://www.w3.org).
XML (extensible markup language)	A flexible way to create common information formats and share both the format and the data on the World Wide Web, Intranets, and elsewhere.
Zero-day exploit	A software vulnerability that security researchers and software developers are not yet aware of. They pose a higher risk to users than other vulnerabilities of penetrating a system undetected and unnoticed. This term applies to environments with the AntiVirus module installed.