Remote Systems Management 8.5 Update 1

User Guide

ivanti | Endpoint Security
powered by HEAT

Notices

Version Information

Ivanti Endpoint Security: Remote Systems Management User Guide - Ivanti Endpoint Security: Remote Systems Management Version 8.5 Update 1 - Published: May 2017

Document Number: 02_217_8.5 Update 1_171281142

Copyright Information

Table of Contents

Chapter 1

Remote Systems Management Overview

In this chapter:

- Remote Systems Management Workflow
- Advantages of Using Remote Systems Management

Ivanti Remote Systems Management works with Ivanti Endpoint Security to provide administrators a simple way to remotely manage devices.

Remote Systems Management Workflow

Ivanti Remote Systems Management is a Ivanti Endpoint Security platform component that provides administrators an effective way to remotely manage endpoints in an organization.

A typical Ivanti Remote Systems Management workflow consists of the following:

Install the RSM platform component on your Ivanti Endpoint Security (Ivanti Endpoint Security) server.

Install the RSM plug-in on your local computer (the system from which you are accessing Ivanti Endpoint Security).

Begin remotely managing endpoints from your local computer using the Ivanti Endpoint Security Web console.

Advantages of Using Remote Systems Management

The Ivanti Remote Systems Management provides a simple way to remotely manage endpoints from the Ivanti Endpoint Security Web console.

Remote Systems Management integrates with the following applications and utilities, allowing you to manage endpoints remotely:

- Windows® Remote Desktop Connection (RDC): A simple interface to access applications and data on a remote Windows computer over a network.
- Microsoft® Management Console (MMC): A presentation services that allows you to manage and monitor Windows systems on an endpoint computer.
- The `NSLOOKUP` MS-DOS® command: A utility that allows you to perform a reverse lookup on an IP address by querying the Domain Name System (DNS) server of the endpoint computer.
- The `Ping` MS-DOS® command: A utility that allows you to troubleshoot connectivity problems within your network.
- PuTTY ®: A remote management tool that allows you to remotely control Non-Windows computers over the Internet.
- Virtual Network Connection® (VNC): A platform-independent application that allows you to view and interact with another computer over a network or Internet.

Chapter 2

Getting Started with Ivanti Remote Systems Management

In this chapter:

To get started with Ivanti Remote Systems Management, install the module and then install the Remote Systems Management plug-in on your the computer from which you are accessing Ivanti Endpoint Security Web console.

Remote Systems Management at a Glance

Ivanti Remote Systems Management is a module that contains functions that allow you to remotely manage endpoints on your network.

Benefits

Ivanti Remote Systems Management performs the following functions:

- It provides the log in page for the Windows® Remote Desktop Connection (RDC), which is a simple interface to access applications and data on a remote Windows computer over a network.
- It allows you to launch the Microsoft® Management Console (MMC), which allows you to manage and monitor Windows systems on an endpoint computer.
- It provides you with the `NSLOOKUP` MS-DOS® command, which performs a reverse lookup on an IP address by querying the Domain Name System (DNS) server of the endpoint computer.
- It provides you with the `Ping` MS-DOS® command, therefore allowing you to troubleshoot connectivity problems within your network.
- It allows you to launch PuTTY ®, a remote management tool that allows you to remotely control a Non-Windows target computer over the Internet.
- It allows you to launch Virtual Network Connection® (VNC), a platform-independant application that allows you to view and interact with another computer over a network or Internet.

Key Terms

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.
browser	Software that allows the user to find, view, hear, and interact with material on a corporate Intranet or the World Wide Web.
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.
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. Although most modules are not considered part of the Ivanti Endpoint Security platform, there are exceptions. The following are considered platform components: • Ivanti Wake on LAN • Remote Systems Management • Support Tools • Core These modules are listed as platform components within Installation Manager and cannot be uninstalled.
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.

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.
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.
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.
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.
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.
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.
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.
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.
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.

Remote Systems Management Workflow

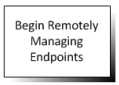
To use Remote Systems Management, Ivanti Endpoint Security must be installed along with the Ivanti Remote Systems Management platform component and the plug-in.

Refer to the following flow chart to determine tasks when using the Ivanti Remote Systems Management within Ivanti Endpoint Security (Ivanti Endpoint Security).

Install the Remote Systems Management platform component on your Ivanti Endpoint Security server. For additional information, refer to Installing the Remote Systems Management Module Server Component on page 14.

Notice: The Remote Systems Management module is listed as a platform component within Installation Manager.

Install the Remote Systems Management plug-in on your local computer (the system from which you are accessing Ivanti Endpoint Security Web console). For more information, see Installing the Remote Systems Management Plug-In on page 65.



Begin remotely managing endpoints from your local computer using the Ivanti Endpoint Security Web console. For more information on remote management menu items, see The Manage Remotely Menu on page 64.

Chapter 3

Remote Systems Management Installation

In this chapter:

Successful installation of the Ivanti Endpoint Security server is vital to installing Ivanti Remote Systems Management. All platform components are included in the Ivanti Endpoint Security install.

RSM is a platform component within the Ivanti Endpoint Security (Ivanti Endpoint Security).

Refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) for information on how to install the Ivanti Endpoint Security server.

Software Requirements

Ivanti Remote Systems Management requires supportive software to operate on endpoints.

Remote Systems Management requires the Remote Systems Management server module to be installed on the Ivanti Endpoint Security server.

Remote Systems Management requires the Remote Systems Management endpoint module to be installed on the Ivanti Endpoint Security Agent. You can install Remote Systems Management on all supported agent operating systems.

The Remote Systems Management plug-in requires .NET Framework 3.5 SP1 or higher on endoints. If necessary, the Remote Systems Management installs .NET Framework with the module.

Important: When using .Net Framework 3.5 SP1 with Firefox, an additional add-on is required. For additional information, refer to Microsoft .Net Framework Assistant (https://addons.mozilla.org/en-US/firefox/addon/9449/).

Managed Operating Systems

Each managed operating system accepts specific remote systems management functionality.

The module can be installed on any endpoint hosting the Ivanti Endpoint Security Agent or the Patch Agent for Linux, The UNIX, or Mac.

Windows endpoint can have the following remote management functions installed:

- Remote Desktop Connection (RDC)
- Microsoft Management Console (MMC)
- NSLookup
- Ping
- VNC

Mac, Linux, and UNIX endpoints can have the following remote management functions installed:

- NSLookup
- Ping
- PuTTY
- VNC

Installing the Remote Systems Management Module Server Component

To begin using Ivanti Remote Systems Management, you must first install the server component on your Ivanti Endpoint Security server.

Install the Remote Systems Management server component using the Ivanti Installation Manager. For additional information, refer to the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Notice: The Remote Systems Management module is listed as a platform component within Installation Manager.

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

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

2. Select the **Remote Systems Management** check box for your version number of Ivanti Endpoint Security.
3. Click **Install**.

   Step Result: A dialog opens, notifying you that a database backup is recommended.

4. Click **Next**.
5. Complete the applicable steps according the dialog page that opens.

   The following table describes the steps for each dialog page.

Page	Step(s)
If the ***Prerequisites*** page opens:	Your server does not meet the recommended system requirements to install the selected content. • If you receive *failure(s)*, you must cancel the installation and resolve the failures before you can install the content. • If you receive *warning(s)*, you may proceed by clicking **Next**. Ivanti recommends resolving the warning(s) before proceeding. **Tip:** Click **Print** for a hard copy of prerequisite deficiencies. Click **Retry** to reassess the server.
If the ***Ready to Install*** page opens:	**1.** Review the content selected for installation. **2.** Click **Install**. **Tip:** Click the **terms and conditions link** to view the company terms and conditions.

6. Click **Finish**.

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

Result: The **Remote Systems Management** platform component is installed. To begin using the platform component, reopen Ivanti Endpoint Security.

Note: Platform components cannot be uninstalled.

After Completing This Task:
Complete Installing the Remote Systems Management Plug-In on page 65.

Updating the Ivanti Remote Systems Management Module

Periodically, Ivanti releases updates for Ivanti Remote Systems Management. Install the latest release to keep Ivanti Remote Systems Management up to date.

Ivanti recommends installing updates immediately. Update Ivanti Wake on LAN using the Ivanti Installation Manager.

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

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

2. Select a **Suite Version** radio button.
   - If you are updating the entire suite, select the radio button for the latest **Suite Version**.
   - If you are only installing new modules, leave the current suite version selected.

   Tip: When you select a **Suite Version**, other suite versions their components are greyed out to prevent mixing.

3. Select the **Ivanti Remote Systems Management** check box for your version of Ivanti Endpoint Security.

   Note: This check box is only available if there is an update for the module.

4. Click **Install**.

   Step Result: The ***Database backup recommended*** dialog opens.

   Note: During the module install, the installer will update your existing database(s). In the event of hardware failure or data corruption a database backup can ensure you still have functional data in order to restore database files. Refer to *Database Backup* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) for additional information.

5. Select **Next**.

   Step Result: The ***Ready to Install*** dialog opens.

   Tip: Click the **terms and conditions link** to view the company terms and conditions.

6. Click **Install**.

   The following table describes the steps for each dialog page.

Dialog	Step(s)
If the ***Prerequisites*** page opens:	Your server does not meet the recommended system requirements to install the selected content. • If you receive *failure(s)*, you must cancel the installation and resolve the failures before you can install the content. • If you receive *warning(s)*, you may proceed by clicking **Next**. Ivanti recommends resolving the warning(s) before proceeding. **Tip:** Click **Print** for a hard copy of prerequisite deficiencies. Click **Retry** to reassess the server.

Dialog	Step(s)
If the ***Install/Update Components*** page opens:	Click **OK** to begin the component(s) installation. **Tip:** When the **Don't show this again** check box is selected it collapses the ***Install/Update Components*** dialog and this dialog will no longer be shown.
If the ***Install Status*** page opens:	The installation of component(s) begins.

Step Result: The selected component(s) begin downloading and installing.

7. After installation completes, review the ***Confirmation*** page. Click **Finish** when you are done.

Tip:

- Click **View install log** to review the install log.
- Clear the **Launch** checkbox to cancel relaunch of the Web console.

8. Click **Finish**.

Step Result: The ***Confirmation*** page closes.

Result: The module is upgraded.

Chapter 4

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.

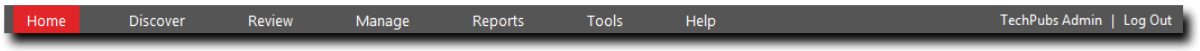


Figure 1: Navigation Menu

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 2: 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.

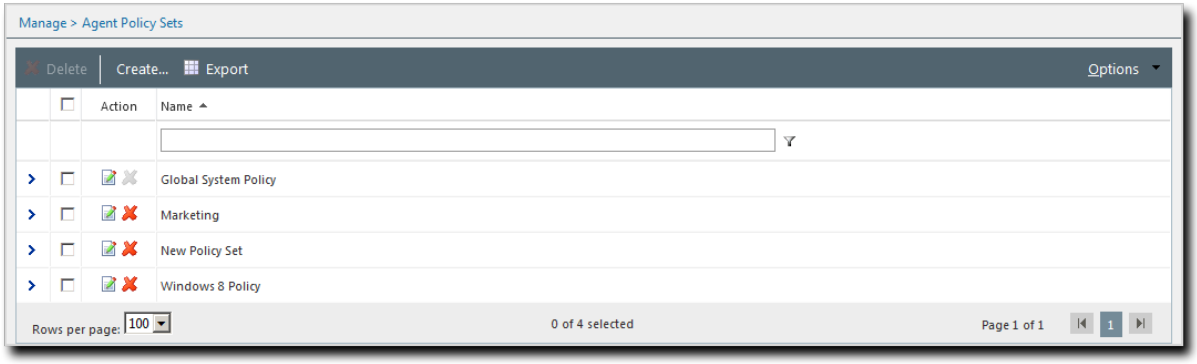


Figure 3: List Page

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.

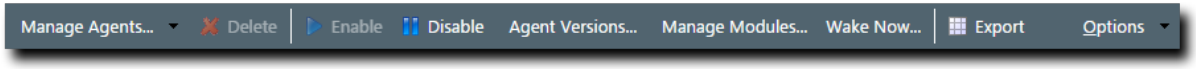


Figure 4: Toolbar

- 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 30.
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 32
Show Group By Row[2]	Toggles the **Show Group By Row** on and off. For additional information, refer to Group By on page 34.
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.

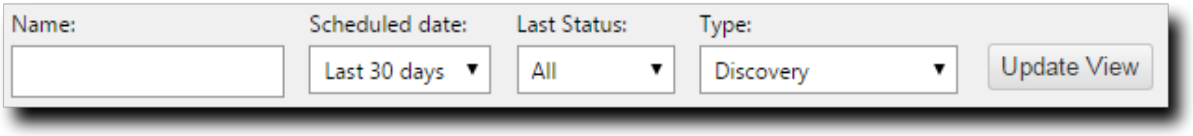


Figure 5: Filters

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.

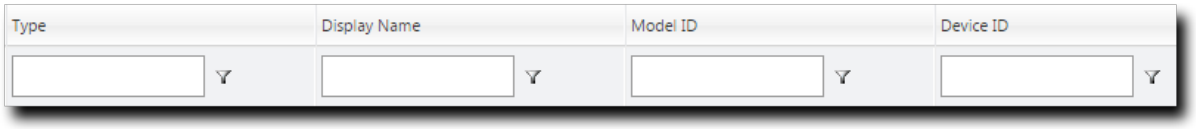


Figure 6: Filter Row

- 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 28.
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**.

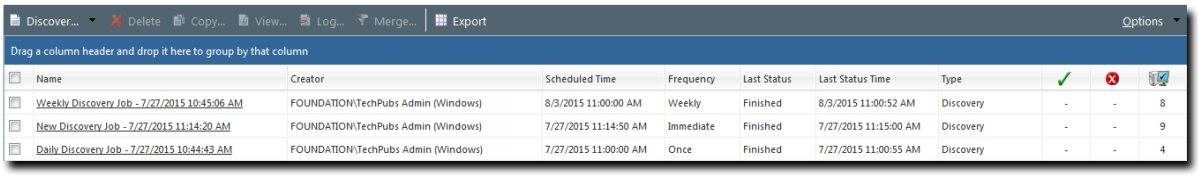


Figure 7: Group By Row

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.

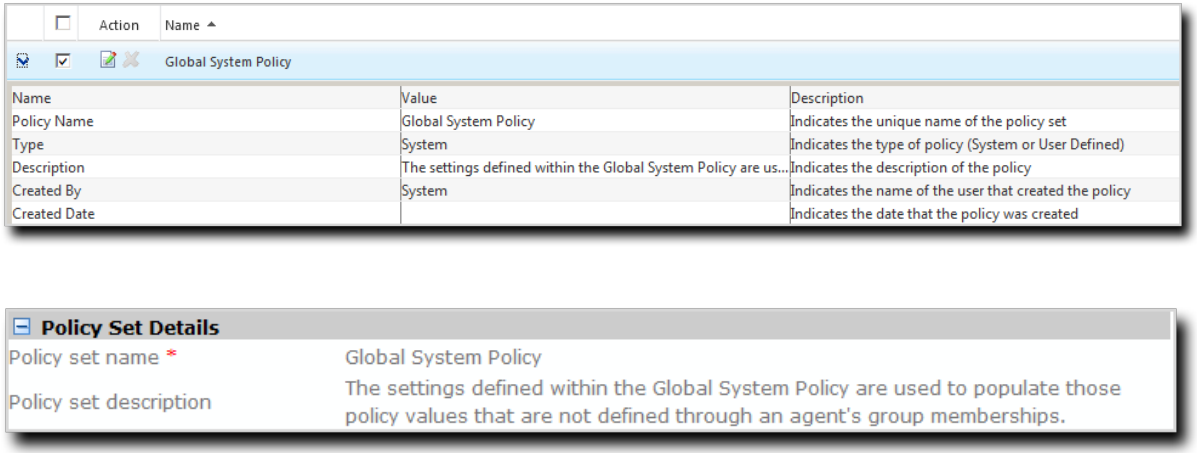


Figure 8: Expandable Structure Examples

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.

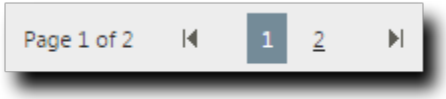


Figure 9: Pagination Feature

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.

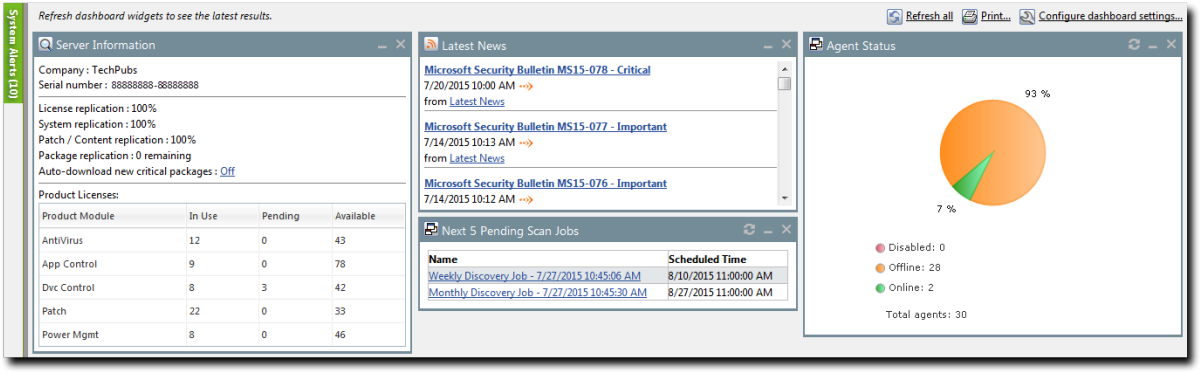


Figure 10: The Home Page

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 Application Library File Assessment Widget

This widget displays a summary of the verification levels of the Application Library files that have been submitted to the Ivanti Endpoint Integrity Service for assessment.

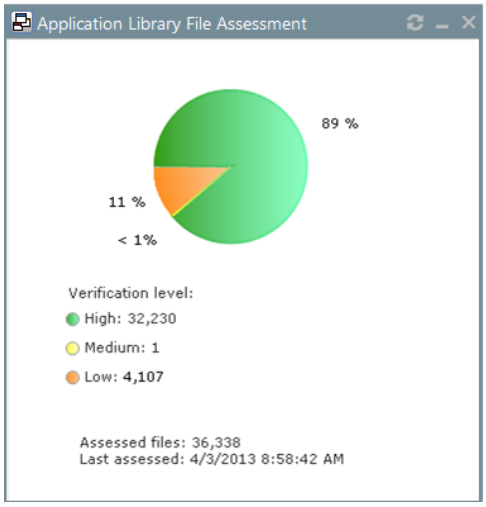


Figure 11: Application Library File Assessment Widget

Each pie chart segment corresponds to a file verification level. The following table describes the ***Application Library File Assessment*** widget fields.

Table 18: Application Library File Assessment Widget Fields

Field	Description
High (Green)	Files have matches in the Ivanti Endpoint Integrity Service. This is a web service maintained by Ivanti that contains a database of verified application files.
Medium (Yellow)	Files have one or both of the following: • A high-prevalence match in the user network (the collection of servers that have sent files to Endpoint Integrity Service for assessment). • A match in the National Software Reference Library (NSLR), a project of the National Institute of Standards and Technology that maintains a reference data set of known software hashes.
Low (Orange)	Files have low-prevalence matches in the user network, or no match was found.
Assessed files	The total number of files in Application Library that have been submitted to Endpoint Integrity Service for assessment.
Last assessed	The date and time that a file assessment was last performed.

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.

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).

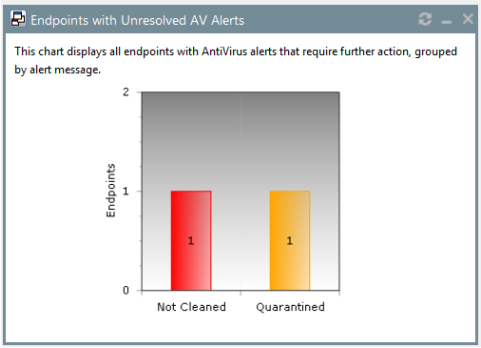


Figure 12: Endpoints with Unresolved AV Alerts Widget

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.

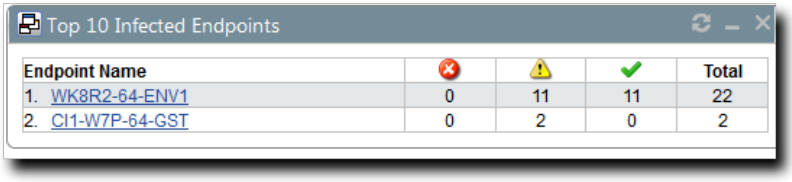


Figure 13: Top 10 Infected Endpoints Widget

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).

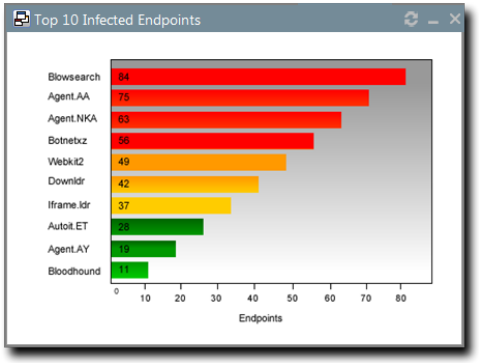


Figure 14: Top 10 Virus/Malware Threats

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.

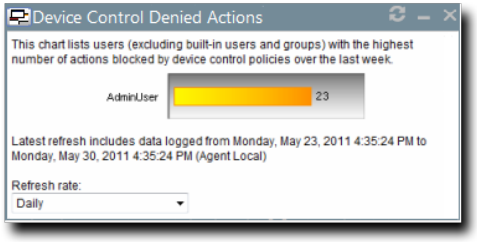


Figure 15: Device Control Denied Actions Widget

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.

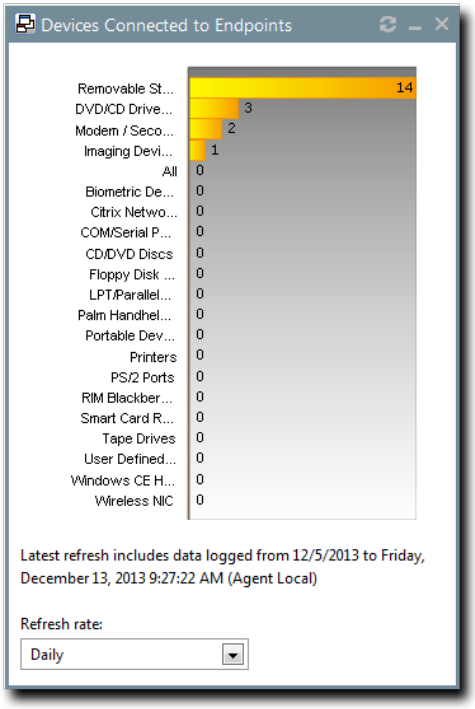


Figure 16: Devices Connected to Endpoints Widget

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.

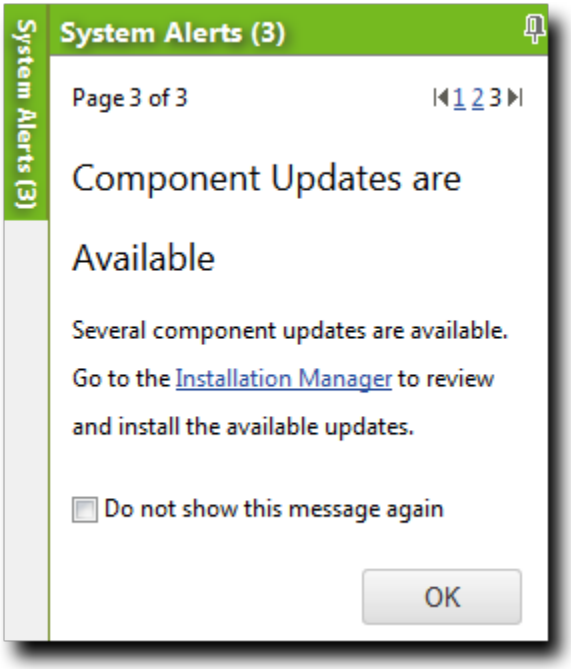


Figure 17: The System Alert Pane

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 36.
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 5

Using Ivanti Remote Systems Management

In this chapter:

The Remote Systems Management functionality is accessed by selecting **Manage Remotely** on the ***Endpoint Details*** page.

The ***Endpoints*** page contains a listing of all endpoints that have an agent registered with the Ivanti Endpoint Security.

Tip: The ***Manage Remotely*** option can be found by selecting **Manage** > **Endpoints**. Click the **Name** link to open the ***Endpoint Details*** page.

Management Options

The ***Endpoint Details*** page contains tabs which allow access to endpoint details.

The ***Information*** tab toolbar contains the **Manage Remotely** menu, which contains menu items allowing you to remotely manage endpoints.

Note: To access the **Manage Remotely** menu, the Remote Systems Management platform component must be installed. For additional information, refer to Installing the Remote Systems Management Plug-In on page 65.

The Manage Remotely Menu

The **Manage Remotely** menu provides menu items you can use to connect to remote endpoints.

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

Table 42: Manage Remotely Menu Items

Menu Item	Description
Launch Remote Desktop...	Launches the log in page for the Windows Remote Desktop Connection (RDC), which allows you connect to a computer in another location.
Launch MMC: Computer Management...	Launches the Microsoft Management Console (MMC), which allows you to manage and monitor Windows systems.
Launch NSLookup...	Launches the `NSLookup` MS-DOS command, which displays a reverse lookup on an IP address by querying the Domain Name System (DNS) server of the endpoint computer.
Launch Ping...	Launches the `Ping` MS-DOS command, which verifies that a particular IP address exists and can accept requests.
Launch PuTTY...	Launches PuTTY, a remote management tool that allows you to remotely control targeted computers over the Internet.
Launch VNC...	Launches the log in page for the Virtual Network Connection (VNC), which allows you to remotely access another computer.

Remote Systems Management Plug-In

The Remote Systems Management plug-in is downloaded from the Ivanti Endpoint Security server and installed on the client computer.

Once installed on the client computer, the plug-in allows you to remotely manage endpoints from the Ivanti Endpoint Security Web console.

Installing the Remote Systems Management Plug-In

If the Remote Systems Management plug-in is not already installed on the client computer, you are prompted to install the plug-in when you select a management link from the **Manage Remotely** option.

Prerequisites:

- Installing the Remote Systems Management Plug-In on page 65
- Managed Operating Systems on page 13
- If you are using Mozilla Firefox, download and install the plug-in available at https://addons.mozilla.org/en-US/firefox/addon/microsoft-net-framework-assist/.

Install the Remote Systems Management plug-in on the local computer.

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

   Step Result: The ***Endpoint Details*** page opens.

2. Click the desired **Name** link to open the ***Endpoint Details*** page.

   Step Result: The ***Endpoint Details*** page displays with the ***Information*** tab selected by default.

3. Click **Manage Remotely** and select one of the following options:

   Table 43: Manage Remotely Options

Option	Description
Launch Remote Desktop...	The Windows Remote Desktop (RDC) application. For more information, refer to The Remote Desktop Connection on page 67.
Launch MMC: Computer Management...	The Microsoft Management Console (MMC) application. For more information, refer to MMC: Computer Management on page 68.
Launch NSLookup...	Launches the `NSLookup` MS-DOS command. For more information, refer to The NSLookup MS-DOS Command on page 70.
Launch Ping...	Launches the `Ping` MS-DOS command. For more information, refer to The Ping MS-DOS Command on page 71.
Launch PuTTY...	The PuTTY application. For more information, refer to PuTTY: Remote Management Tool on page 72.

Option	Description
Launch VNC...	The Virtual Network Connection (VNC) application. For more information, refer to The Virtual Network Connection on page 73.

Note: Option access depends on the compatible operating system of the endpoint selected. For additional information, refer to Managed Operating Systems on page 13.

Attention: For Mozilla Firefox 3.x browser users, to successfully install the Remote Systems Management plug-in and turn off the ***Save File*** dialog, Mozilla Firefox 3.x requires .NET Framework 3.5 SP1 additional add-on for Firefox. For additional information, see Microsoft .Net Framework Assistant (http://addons.mozilla.org/en-US/firefox/addon/9449/).

4. Choose the applicable option:

Dialog	Step
If the *Remote Systems Management* plug-in dialog opens:	Click **Run** to install the Remote Systems Management plug-in.
If the *.NET Framework 3.5 SP1* dialog opens:	Install the .Net Framework and Remote Systems Management plug-in. 1. Click **Install Now** to begin the install of .NET Framework 3.5 SP1. 2. Click **Install** to complete the install of the .NET Framework 3.5 SP1. 3. Click **Run** to install the Remote Systems Management plug-in.

Step Result: The Remote Systems Management plug-in installs and the selected option automatically launches on the local computer.

Manage Remotely Access Right

The Remote Systems Management adds an access right to the Ivanti Endpoint Security.

The *Manage Remotely* access right is automatically added to the ***Access Rights*** tab in the ***Edit Role*** window.

Once Remote Systems Management is installed, the Administrator and Manager roles have the *Manage Remotely* access right selected by default. Custom role users may be granted the access right if needed. The following table describes the Manage Remotely roles and the icons that denote them.

Table 44: Manage Remotely Roles

Role	Icon	Description
Administrator		The Manage Remotely access right is assigned by default.
Guest		The Manage Remotely access right is not assigned by default, and this predefined system role cannot be edited.
Manager		The Manage Remotely access right is assigned by default.
Operator		The Manage Remotely access right is not assigned by default, and this predefined system role cannot be edited.
Custom		The Manage Remotely access right is not assigned by default, but can be manually assigned if needed.

Note: For additional information regarding access rights, refer to *Defining Access Rights* in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

The Remote Desktop Connection

The Windows Remote Desktop Connection (RDC) allows you to connect to a remote computer.

Starting the Remote Desktop Connection

The **Launch Remote Desktop** option opens the Windows Remote Desktop Connection (RDC) so you can connect to a target endpoint.

Prerequisites:

- The local computer must have network access to the endpoint computer.
- The Ivanti Remote Systems Management plug-in must be installed on the local computer. For additional information, refer to Installing the Remote Systems Management Plug-In on page 65.
- The endpoint must be turned on.
- The *Windows Remote Desktop Connection* component must be enabled on the endpoint system. For additional information, refer to Connect to another computer using Remote Desktop Connection (http://windows.microsoft.com/en-US/windows-vista/Connect-to-another-computer-using-Remote-Desktop-Connection).
- The endpoint must run a Windows supported operating system. For additional information, refer to Managed Operating Systems on page 13.
- For permission to connect to the endpoint, you must have Administrative rights or membership in the Remote Desktop Users Group on the endpoint.

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

   Step Result: The ***Endpoints*** page displays.

2. Click the desired **Name** link to open the ***Endpoint Details*** page.

   Step Result: The ***Endpoint Details*** page displays with the ***Information*** tab selected.

3. Click **Manage Remotely** > **Launch Remote Desktop**.

   Attention: The endpoint must be Windows supported operating system in order for the **Launch Remote Desktop** menu item to display. For additional information, refer to Managed Operating Systems on page 13.

   Step Result: The ***Windows Security*** dialog opens.

4. Type the **Windows** credentials in the following fields.

Field	Description
Username	A valid user name for the endpoint. Type the user name in local format (`username`) or domain format (`domain\username`).
Password	The password associated with the **Username**.

5. Click **OK**.

   Step Result: The **Remote Desktop** connects to the endpoint.

MMC: Computer Management

Microsoft Management Console (MMC) is an application that provides Windows management services for hosting administrative tools to administer networks, computers, services, and other system components on target endpoints.

Starting the Microsoft Management Console

Starting Microsoft Management Console (MMC) allows you to connect to a target endpoint.

Prerequisites:

- The local computer must have network access to the endpoint computer.
- The Ivanti Remote Systems Management plug-in must be installed on the local computer. For additional information, refer to Installing the Remote Systems Management Plug-In on page 65.
- The client computer must have access to the Computer Management snap-in. For additional information, refer to Restrict users to the explicitly permitted list of snap-ins (http://technet.microsoft.com/en-us/library/cc975962.aspx).
- The endpoint must be turned on.
- The endpoint must have a Windows supported operating system. For additional information, refer to Managed Operating Systems on page 13.
- For permission to connect to the endpoint, you must have Administrative rights on the endpoint.

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

   Step Result: The ***Endpoints*** page displays.

2. Click the desired **Name** link to open the ***Endpoint Details*** page.

   Step Result: The ***Endpoint Details*** page displays with the ***Information*** tab selected by default.

3. Click**Manage Remotely** > **Launch MMC: Computer Management**.

   Attention: The endpoint must be Windows supported operating system in order for the **Launch MMC: Computer Management** menu item to display. For additional information on remote systems management functionality by operating system, refer to Managed Operating Systems on page 13.

   Step Result: The ***Computer Management*** dialog opens.

The NSLookup MS-DOS Command

The `NSLookup` command is a standard MS-DOS command that enables an administrator to query a Domain Name System (DNS) server to find DNS details.

The `NSLookup` MS-DOS command window displays two sections. The first section specifies the server name and IP address of the host server and the second section is the endpoints' DNS server name and IP address.

- Host
  - `Server: Example.Company.Demo`
  - `Address: 19.19.195.19`
- Endpoint
  - `Name: Example.Endpoint.Demo`
  - `Address: 10.10.0.10`

Accessing the NSLookup MS-DOS Command

Accessing the `NSLOOKUP` MS-DOS administrative tool displays the host server name and IP address and also the endpoints' Domain Name System (DNS) server name and IP address.

Prerequisites:

- The local computer must have network access to the endpoint computer.
- The Ivanti Remote Systems Management plug-in must be installed on the local computer. For additional information, refer to Installing the Remote Systems Management Plug-In on page 65.
- The endpoint must be turned on.
- The endpoint must have a supported operating system. For additional information, refer to Managed Operating Systems on page 13.

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

   Step Result: The ***Endpoints*** page displays.

2. Click the desired **Name** link to open the ***Endpoint Details*** page.

   Step Result: The ***Endpoint Details*** page displays with the ***Information*** tab selected by default.

3. Click **Manage Remotely** > **Launch NSLookup**.

   Step Result: The ***Command Prompt*** window opens.

The Ping MS-DOS Command

The `PING` command is a standard MS-DOS command that allows you to view the computer name and the IP address of an endpoint computer.

Sample `Ping` MS-DOS command window syntax is described in the following table.

Table 45: Ping MS-DOS Command Syntax

Value	Description
`Pinging 10.10.0.10 with 32 bytes of data:`	Ping sends an Internet Control Message Protocol (ICMP) echo packet (with the Time To Live [TTL] value set to the host default) to the host listed on the ping command line.
`Reply from 10.10.0.10: bytes=32 time<1ms TTL=128`	The ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss.
`Ping Statistics`	The statistics from pinging the host. They include how many packets were sent, received, and lost. Also shown are round trip times and averages.

Accessing the PING MS-DOS Command

Accessing the `Ping` MS-DOS command allows you to verify that a particular address exists and can accept requests.

Prerequisites:

- The local computer must have network access to the endpoint computer.
- The Ivanti Remote Systems Management plug-in must be installed on the local computer. For additional information, refer to Installing the Remote Systems Management Plug-In on page 65.
- The endpoint must be turned on.
- The endpoint must have a supported operating system. For additional information, refer to Managed Operating Systems on page 13.

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

   Step Result: The ***Endpoints*** page displays.

2. Click the desired **Name** link to open the ***Endpoint Details*** page.

   Step Result: The ***Endpoint Details*** page displays with the ***Information*** tab selected by default.

3. Click**Manage Remotely** > **Launch Ping**.

   Step Result: The ***Command Prompt*** window opens.

PuTTY: Remote Management Tool

PuTTY is an open source communications tool that uses Secure Shell (SSH) and Teletype Network (Telnet) protocols to remotely control a targeted computer over the Internet. When installed on a computer running a Windows operating system, PuTTY allows you to remotely control a computer running a non-Windows operating system.

The PuTTY communication tool needs to be installed on the client computer prior to its usage within the Ivanti Endpoint Security Web console.

Note: For additional information about installing PuTTY, refer to PuTTY: A Free Telnet/SSH Client (http://www.chiark.greenend.org.uk/~sgtatham/putty/).

Using PuTTY on the client computer allows you to remotely control an endpoint.

Starting the PuTTY Communication Tool

Starting the PuTTY communication tool creates a connection to the target endpoint.

Prerequisites:

- The local computer must have network access to the endpoint computer.
- The Ivanti Remote Systems Management plug-in must be installed on the local computer. For additional information, refer to Installing the Remote Systems Management Plug-In on page 65.
- The PuTTY communication tool is installed on the client computer. For installation information about PuTTY, refer to PuTTY: A Free Telnet/SSH Client (http://www.chiark.greenend.org.uk/~sgtatham/putty/).
- The endpoint must be turned on.
- The endpoint must have a Non-Windows supported operating system. For additional information, refer to Managed Operating Systems on page 13.
- For permission to connect to the endpoint, you must have Administrative rights on the endpoint.

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

   Step Result: The ***Endpoints*** page displays.

2. Click the desired **Name** link to open the ***Endpoint Details*** page.

   Step Result: The ***Endpoint Details*** page displays with the ***Information*** tab selected by default.

3. Click **Manage Remotely** > **Launch PuTTY**.

   Attention: The endpoint must be a non-Windows supported operating system in order for the **PuTTY** menu item to display. For additional information on remote systems management functionality by operating system, refer to Managed Operating Systems on page 13.

   Step Result: The ***PuTTY Launch Parameters*** dialog opens with the default endpoint ***IP Address*** information completed.

   Tip: Ivanti recommends that you use the default path location when installing the applicable PuTTY application. Using a alternative path results in having to re-locate the PuTTY tool each time **Manage Remotely** > **Launch PuTTY** is selected.

4. In the **User ID** field, type the user name specific to the target IP address.
5. Click **Launch**.

   Step Result: The ***Command Prompt*** window opens.

Result: The PuTTY communication tool creates a connection to the target endpoint.

Note: If connection fails, then verify that a firewall on either the endpoint or local computer is not blocking the connection. For additional troubleshooting information, refer to PuTTY FAQ (http://www.chiark.greenend.org.uk/~sgtatham/putty/faq.html).

The Virtual Network Connection

The Virtual Network Connection (VNC) is a platform-independent application that allows remote access to another computer. Using computers installed with VNC gives administrators the ability to view and interact with computers over a network or the Internet.

VNC connectivity requires two components: *Server* and *Viewer*. The server component runs on the endpoint you want to remotely access and the viewer component runs on the system used by the administrator. To get started with VNC, you need to configure the server component and then connect using a viewer. VNC is platform-independent, a VNC viewer on one operating system may connect to a VNC server on the same or any other operating system.

Install the VNC server on all endpoint computers you may need to connect to and then install the VNC viewer on the Ivanti Endpoint Security client computer. Once installed, VNC allows an administrator using Ivanti Endpoint Security Web console to connect to the client VNC viewer, therefore allowing a connection to the endpoint.

Note: There are a number of variants of VNC which offer their own particular functionality. For information on VNC®, refer to Getting Started with VNC (http://www.realvnc.com/support/getting-started.html).

Starting the Virtual Network Connection Tool

Starting the Virtual Network Connection (VNC) tool allows remote access to the target endpoint.

Prerequisites:

- Install the VNC server component on the endpoint computer. For installation information, refer to VNC® Server Free Edition 4.1 for Windows (http://www.realvnc.com/products/free/4.1/winvnc.html).
- Install the VNC client component on the Ivanti Endpoint Security client computer. For more information, refer to VNC® Viewer Free Edition 4.1 for Windows (http://www.realvnc.com/products/free/4.1/winvncviewer.html).
- The local computer must have network access to the endpoint computer.
- The Ivanti Remote Systems Management plug-in must be installed on the local computer. For additional information, refer to Installing the Remote Systems Management Plug-In on page 65.
- The endpoint must be turned on.
- The endpoint must have a supported operating system. For additional information, refer to Managed Operating Systems on page 13.
- For permission to connect to the endpoint, you must have Administrative rights on the endpoint.

Note: VNC® Free Edition 4.1 is used in the following step-by-step procedure. For additional information on this VNC variant, refer to VNC® Viewer Free Edition 4.1 - VNC Windows Documentation (http://www.realvnc.com/products/free/4.1/).

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

   Step Result: The ***Endpoints*** page displays.

2. Click the desired **Name** link to open the ***Endpoint Details*** page.

   Step Result: The ***Endpoint Details*** page displays with the ***Information*** tab selected by default.

3. Click **Manage Remotely** > **VNC**.

   Step Result: The ***VNC Launch Parameters*** dialog opens with the default endpoint ***IP Address*** and VNC ***Port***.

   Note: Ivanti recommends that you use the default path location when installing the applicable VNC Viewer. Using a alternative path results in having to re-locate the VNC client each time **Manage Remotely** > **VNC** is selected.

4. Set the applicable settings.

   a) In the **Program** field, click the **Ellipses** button (...) and browse to the applicable VNC Viewer application.
   b) Verify the IP address of the endpoint.
   c) Verify the Port of the endpoint.

5. Click **Launch**.

   Step Result: The ***VNC Viewer Authentication*** dialog opens.

6. In the **Password** field, type the password.

   Note: VNC® Viewer Free Edition can be used to connect to servers configured for No Authentication or VNC Password Authentication. If VNC Password Authentication is configured then you will be prompted to enter the password. VNC Free Edition does not currently support usernames.

7. Click **OK**.

   Step Result: The connection to the target endpoint is created and the target endpoint's desktop appears. You can use your keyboard and mouse to control the connected endpoint.

   Note: If connection fails, then verify that a firewall on either the endpoint or local computer is not blocking the connection. For additional troubleshooting information, refer to VNC® Knowledge Base (http://kb.realvnc.com/).