Ivanti Endpoint Security 8.6

User Guide

ivanti | Endpoint Security
powered by HEAT

Notices

Version Information

Ivanti Endpoint Security User Guide - Ivanti Endpoint Security Version 8.6 - Published: Dec 2020 Document Number: 02_201_8.6_17130552

Copyright Information

Table of Contents

Chapter 1

Ivanti Endpoint Security Overview

In this chapter:

Ivanti Endpoint Security is an application that serves as a platform for other applications that protect your network from security risks.

These applications, called *modules*, use different approaches to protect your endpoint. For example, the Ivanti Patch and Remediation module protects your network by detecting software vulnerabilities and then patching them, while the Ivanti Application Control module protects your network by allowing only authorized applications to run on network endpoints. You may purchase any combination of these modules to best protect your network environment.

The Ivanti Endpoint Security Components

Ivanti Endpoint Securityconsists of components. These components include *platform components* and *module components*, and both work together to make Ivanti Endpoint Security operational.

Platform Components	form the basis for Ivanti Endpoint Security (Ivanti Endpoint Security) module components to operate. The Ivanti Endpoint Security components include: • The Ivanti Endpoint Security Web Console. The console is used to control Ivanti Endpoint Security. • The Ivanti Endpoint Security Database. The database stores Ivanti Endpoint Security values. • The Ivanti Installation Manager. Installation Manager is used to install module components. • Any modules that are listed as platform components within the Installation Manager. All Ivanti Endpoint Security platform components are included in the Ivanti Endpoint Security install.

Module Components	*Module components* are the 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. Each module stops security threats using a different approach. For example, Ivanti Patch and Remediation stops security threats by applying vendor-created software patches. You can install, upgrade, or uninstall any module you are licensed for with the Installation Manager. You can manage *modules* regardless of purchase time. For example, you may initially purchase only the Patch and Remediation module, but later add the Application Control module. For additional information about Installation Manager, refer to the following topics: • Ivanti Installation Manager on page 289 • Explaining Module Subcomponents on page 14 For information about purchasing additional modules, contact Ivanti Sales Support (sales@ivanti.com) .

Explaining Module Subcomponents

Ivanti Endpoint Security is a platform for *modules*, which are add-ons that protect your network using different methods. Each Ivanti Endpoint Security module is composed of two subcomponents: the server component and the endpoint component.

Server Component	This subcomponent is installed on the Ivanti Endpoint Security server. The server component must be installed before the endpoint component.
Endpoint Component	This subcomponent is installed on endpoints hosting a Ivanti Endpoint Security Agent. Endpoint components can be installed after the server component and agents are installed. Each installed endpoint subcomponent consumes an agent license for the applicable modules

Note: Ideally all endpoint agents should be the same version as the Ivanti Endpoint Security server.

New releases of the server support all currently supported versions of the endpoint agent. Older agent versions, however, are constrained to the features available when the agent was released and may not support new server functionality.

The Ivanti Endpoint Security Server/Client Relationship

To protect your network from security exposures, Ivanti Endpoint Security operates using a server/client relationship.

Through communication between the server (a server with the Ivanti Endpoint Security Server installed) and the client (an endpoint with the Ivanti Endpoint Security Agent installed), the Ivanti Endpoint Security system protects your network from various types of vulnerabilities.

The Ivanti Endpoint Security Server	This software, installed on a server in the network, is the platform for all Ivanti Endpoint Security modules. It detects endpoints in your networks, collects information from managed endpoints, and sends information and commands to those managed endpoints. You can control the server from a Web-based UI, accessible from any network endpoint. With no modules installed, Ivanti Endpoint Security offers the following functionality: • Asset Discovery • Agent Installation • Endpoint Management • Basic Reporting
The Ivanti Endpoint Security Agent	This software, installed on network endpoints, collects information about the endpoint and uploads it to the Ivanti Endpoint Security Server. Through communication with the server, the agent can control various endpoint functionality. As more modules are activated, agent responsibility increases.

Chapter 2

Getting Started

In this chapter:

Ivanti Endpoint Security (Ivanti Endpoint Security) is an application that contains several different programs, called modules. The modules are used to protect your network endpoints from security threats.

After installing the Ivanti Endpoint Security server, you need to perform several tasks to ensure that your network has the infrastructure for modules to protect your network. These initial tasks do not necessarily have to be performed in a particular order. Additionally, you should recognize that Ivanti Endpoint Security has many additional features to assist in securing your network.

Following completion of initial tasks, take some time to familiarize yourself with the Ivanti Endpoint Security Web console. The Ivanti Endpoint Security Web console contains many features and functions you can use to secure your network quickly and efficiently.

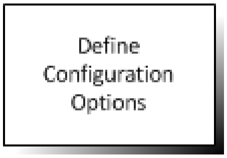
Ivanti Endpoint Security Workflow

After initial installation of the Ivanti Endpoint Security server, you must install the Ivanti Endpoint Security Agent on network endpoints to create an infrastructure to use Ivanti Endpoint Security modules and their functions.

The following chart lists the tasks you should perform after installing the Ivanti Endpoint Security server and logging in for the first time.

Discover network endpoints and install agents on them. To search for endpoints in your network, complete a Discovery Scan Job. After completing this scan, you can select which endpoints you want to install agents on. You can then install agents by completing an Agent Management Job. The agent communicates with the Ivanti Endpoint Security server to create an infrastructure for Ivanti Endpoint Security module functions. For additional information, refer to Discovering Endpoints and Installing Agents on page 21.

Create Groups. Groups are collections of endpoints. You can group endpoints by operating system, function, or any other method to suit your organization. After forming groups, you can manage them collectively. For additional information, refer to Creating a Group on page 23.



Define configuration options. These configuration options control how the Ivanti Endpoint Security server communicates with the Ivanti Endpoint Security Agent, as well as general configuration options. For additional information, refer to Defining Default Options on page 24.

Create users and user roles. Users are people who have access to Ivanti Endpoint Security, and user roles define the features Ivanti Endpoint Security users have access to. For additional information, refer to Creating New Users and Roles on page 25.

Create Email Notifications. Email notifications are alerts that Ivanti Endpoint Security sends to defined email addresses when certain system events occur. For additional information, refer to Creating Email Notifications on page 26.

Ivanti Endpoint Security at a Glance

Ivanti Endpoint Security is a software suite that contains numerous features that secure your network from various types of attacks.

Benefits

- Provides a platform to install modules, which are security solutions that snap in to Ivanti Endpoint Security (Ivanti Endpoint Security).
- Features *Discovery Scan Jobs*, which are scans that search your network for endpoints.
- Features *Agent Management Jobs*, which are jobs that remotely install the Ivanti Endpoint Security Agent on network endpoints.
- Features groups, which are endpoint collections that can be managed collections.
- Features *Agent Policy Sets*, which lists of behaviors that can be applied to groups.
- Create new users, which are profiles that can be used to access Ivanti Endpoint Security.
- Create custom user roles, which are sets of access rights that can be applied to users.
- Create email notifications, which are alert emails that Ivanti Endpoint Security sends to defined users to notify them of system events.
- View endpoint details and information. The Ivanti Endpoint Security Agent scans it host endpoint for system information, which is then sent to the Ivanti Endpoint Security server.

Key Terms

Agent Management Job	Jobs that let you install agents upon endpoints within your network remotely. The first function of this job is to discover the targeted endpoints as in a *Discovery Scan Job*. The second function of this job is to install agents upon endpoints discovered during the first function. These jobs access the targeted endpoints by providing credentials specified during job configuration.
Agent Policies	The agent rules for communicating with the server. These rules include: communication interval, deployment notification options, discovery agent mode, hours of operation, logging level, and reboot notification options. Agent policies are assigned to groups, but any group that has not been explicitly assigned an agent policy will use the default system policy, as defined within the Ivanti Endpoint Security server.
Agent Policy Sets	The combined selected agent policies as defined by the user. After their definition, these sets are then assigned to groups.
asset	An endpoint, along with all the hardware and software that is installed on that endpoint. Each endpoint, individual hardware device, and individual software application is considered an asset.
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.
Discovery Scan Job	A network-based scan run from the Ivanti Endpoint Security server that discovers assets in your network (endpoints, routers, switches, printers, and so on) by using user-specified IP addresses or asset names and/or domains. These jobs also discover additional information about assets (operating system, address information, and so on) through port scans, information queries, and address mask requests.
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.
Group	A targeted collection of computers created and named for the purpose of deploying distribution packages, defining agent policies, setting Mandatory Baselines, or reporting. Groups provide a simple way to manage computers that have similar requirements rather than managing each computer separately.

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.
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.
Module Components	Individual security solutions used to prevent various types of security breaches within your network. Each module plugs in to the Ivanti Endpoint Security platform and can be purchased individually. Some module components come installed with the Ivanti Endpoint Security platform and require no additional licensing.
Module Sub Components	The two parts that form a module component. Each module component consists of a server sub component and an endpoint subcomponent. These subcomponents work together to form a module's functionality.
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.

Logging In

Get started with Ivanti Endpoint Security by logging in.

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

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

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

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

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

   Tip: You can also use the server IP address.

   Step Result: A dialog prompting you for credentials opens.

3. Type your user name in the **User name** field.

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

Discovering Endpoints and Installing Agents

Before you can begin using Ivanti Endpoint Security's functions and features, you must first find the endpoints in your network, and then install agents on them. The Ivanti Endpoint Security Agent is software that communicates information about an endpoint to the Ivanti Endpoint Security server.

Prerequisites:

Complete Logging In on page 20.

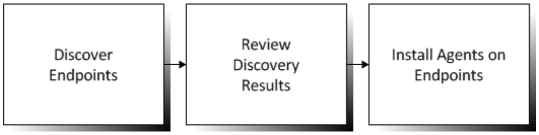


Figure 1: Discover Endpoints and Install Agents Process

Discover endpoints using the ***Discovery Scan Wizard***. Install agents using the ***Install Agents Wizard***.

1. Discover network endpoints using a Discovery Scan Job.

   A Discovery Scan Job is a network scan that searches your network for defined endpoints. These jobs find endpoints using IP addresses, endpoints names, network neighborhood, or other discovery methods. These scans can be configured to run at a specific time or immediately. To begin protecting your network, Ivanti recommends running an immediate Discovery Scan Job.

   a) From the navigation menu, select **Discover** > **Assets**.

      Step Result: The ***Discovery Scan Wizard*** opens.

   b) Complete the wizard.

      For detailed information about completing the wizard, refer to Discovering Assets by Discovery Scan Job on page 91.

   c) From the navigation menu, select **Review** > **Asset Discovery Job Results**.

   d) Select the ***Completed*** tab.

      Discovery scan job results display on this tab after the job finished. The job's completion time varies according to the job's configured scope.

   e) Review the job results. Click the job link for detailed job information.

2. Install agents on the desired endpoints.

   An Agent Management Job installs the agent on defined endpoints. Use the results from a completed Discovery Scan Job to designate endpoints for agent installation. The ***Agent Installation Wizard*** is similar to the ***Discovery Scan Wizard***.

   a) From the navigation menu, select **Discover** > **Assets and Install Agents**.

      Step Result: The ***Install Agents Wizard*** opens.

   b) Complete the wizard.

      For detailed information about completing the wizard, refer to Installing Agents by Agent Management Job on page 109.

      > **Tip:** You can also install the agent from endpoints locally using the Web console. For additional information, refer to Downloading the Agent Installer on page 173.

   c) Select the ***Completed*** tab after the job completes.

      The job's completion time varies according to the job's configured scope.

   d) Review the job results. Click the job link for detailed job information.

3. [Optional] Update the agent version number.

   > **Note:** You may have to wait for agents to complete the registration process before you can update them.

   a) Select **Manage** > **Endpoints**.

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

   b) Select the **Select All** check box.

   c) Click **Agent Versions**.

      Step Result: The ***Manage Agent Versions*** dialog opens.

   d) From the global drop-down list, select the latest agent version number.

   e) Click **Apply to All Agents**.

   f) Click **OK**.

Result: The agents are installed on the defined endpoints (and, if applicable, updated).

After Completing This Task:
Continue to Creating a Group on page 23.

Creating a Group

Within Ivanti Endpoint Security, you can organize endpoints into groups. Use groups to manage endpoint collectively. Groups are a key Ivanti Endpoint Security feature that greatly reduce administrative overhead.

Prerequisites:

Complete Discovering Endpoints and Installing Agents on page 21.

Figure 2: Group Diagram

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

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

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

   > **Note:** The group you create is added as a child group to the group selected within the directory tree.

3. Create a group.
   a) From the **View** list, select **Group Membership**.
   b) Click **Create**.
   c) In the **Name** field that displays, type a group name.
   d) In the **Description** field that displays, type a description.
   e) Click the **Save** icon.
4. Add endpoints to the group.
   a) From the **View** list, select **Endpoint Membership**.
   b) Click **Manage**.
   c) Assign endpoints to the group.
      For more detailed information, refer to Adding Endpoints to a Group on page 212.
   d) Click **OK**.
5. Define the group's settings.

   Group settings contain additional group controls.

   a) From the **View** list, select **Settings**.
   b) Define the settings.
      For more detailed information, refer to Editing Group Settings on page 232.

c) Click **Save**.

Result: The group is created and configured.

After Completing This Task:
Continue to Defining Default Options on page 24.

Defining Default Options

Default options control the initial settings for every time you log in to Ivanti Endpoint Security. These settings control a variety of settings: the number of list item that display in a list at one time, pre-selected wizard, values, agent communication intervals, and so on. Configuring default options customizes settings for your preferences.

Prerequisites:

Complete Creating a Group on page 23.

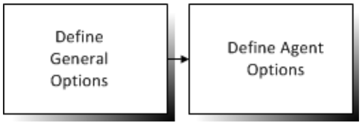


Figure 3: System Options

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

1. From the navigation menu, select **Tools** > **Options**.
2. Define the general options.

   These options define basic options, such as UI options, password options, and report and display options. For additional information, refer to Configuring the General Tab on page 58.
3. Select the ***Agents*** tab.
4. Define the agent options. These options include agent-to-server communication guidelines. They also include the options for pre-configuration of the ***Agent Installation Wizard***.

   For additional information, refer to Configuring the Agents Tab on page 60.

Result: Your default settings are defined.

After Completing This Task:
Continue to Creating New Users and Roles on page 25.

Creating New Users and Roles

You can add unlimited users and roles to Ivanti Endpoint Security. Users are profiles people can use to access the Web console. Roles, which are assigned to users, determine the users access rights within Ivanti Endpoint Security. Create new users to delegate Ivanti Endpoint Security duties to the appropriate colleagues.

Prerequisites:

Complete Defining Default Options on page 24.

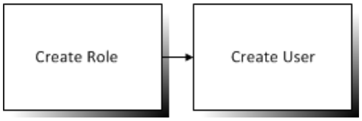


Figure 4: User and Role Creation Process

Create users and roles from the ***Users and Roles*** page.

1. From the navigation menu, select **Tools** > **Users and Roles**.

   Step Result: The ***Users and Roles*** page opens to the ***Users*** tab.

2. [Optional] Create a custom role.

   a) Select the ***Roles*** tab.
   b) Click **Create**.
   c) Complete the ***Create Role*** dialog.

      For more detailed information, refer to Creating User Roles on page 283.

3. Create or add a user.

   a) Click **Create**.
   b) Complete the ***Create User Wizard***.

      For more detailed information, refer to the following topics:

      - Creating New Users on page 262
      - Adding Existing Windows Users on page 264

Result: New users and roles are created.

After Completing This Task:
Continue to Creating Email Notifications on page 26.

Creating Email Notifications

You can configure Ivanti Endpoint Security to send email notifications when defined events occur. To create email notifications, define the email addresses you want to receive alerts, define the events that you want to trigger alerts, and then define the values that trigger alerts. Email notifications are useful for keeping your network maintained.

Prerequisites:

Complete Creating New Users and Roles on page 25.

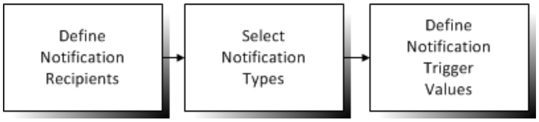

Define Notification Recipients
Select Notification Types
Define Notification Trigger Values

Figure 5: Email Notification Creation Process

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

1. Select **Tools** > **Email Notifications**.
2. Define addresses and the notifications the address will receive.
   a) Click **Create**.
   b) Type an email address in the **Notification Address**.
   c) Select the notifications you want the address to receive.
   d) Repeat the previous substeps to add more email addresses.
3. Define alert settings.

   Alert settings are the values that trigger email notifications. For additional information, refer to Configuring Alert Settings on page 67.
4. Click **Save**.

Result: Email notifications are configured. You will receive emails when the defined events occur.

Chapter 3

Using the Ivanti Endpoint Security Console

In this chapter:

- Common Functions
- The Home Page

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***.

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.

Screen Feature	Function
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.

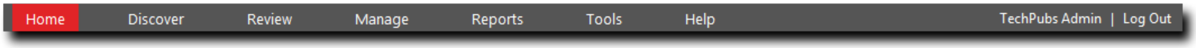


Figure 6: Navigation Menu

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.
Review	Contains menu items related to reviewing security content and discovery scan jobs.

Menu	Description
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.

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.

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
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.

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.
Groups	Opens the ***Groups*** page.
Agent Policy Sets	Opens the ***Agent Policy Sets*** page.

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.
Configuration	Opens the ***All Reports*** page with configuration reports expanded.
Inventory	Opens the ***All Reports*** page with inventory reports expanded.
Policy and Compliance	Opens the ***All Reports*** page with policy and compliance 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.
Launch Installation Manager...	Opens the ***Installation Manager*** in a new window.
Subscription Updates	Opens the ***Subscription Updates*** page.
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

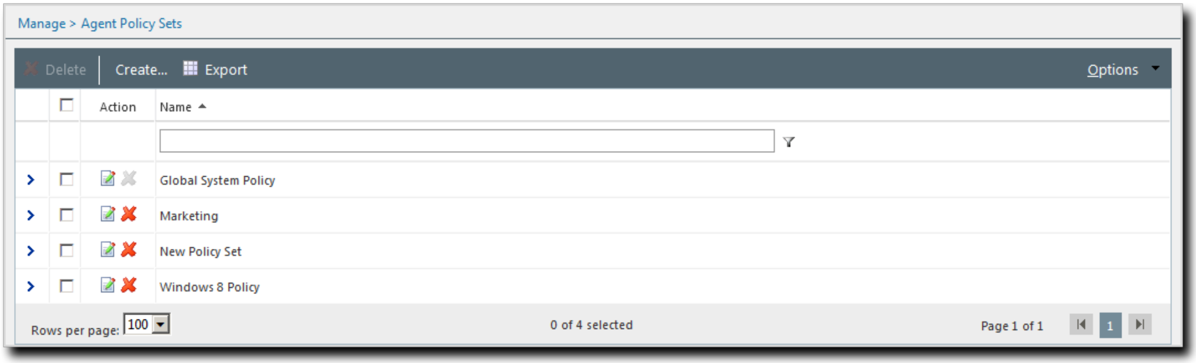
Menu Item	Description
Help Topics...	Opens the ***Help*** page.
Knowledge Base...	Opens the Ivanti knowledge base.

Menu Item	Description
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.
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.

List Pages

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



	□	Action	Name
>	□		Global System Policy
>	□		Marketing
>	□		New Policy Set
>	□		Windows 8 Policy

Figure 7: 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.

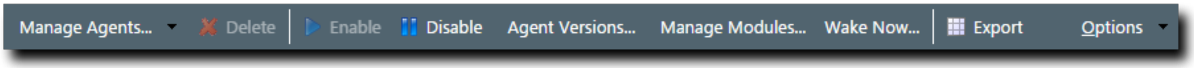


Figure 8: Toolbar

- 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 33.
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 35
Show Group By Row[2]	Toggles the **Show Group By Row** on and off. For additional information, refer to Group By on page 37.
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.

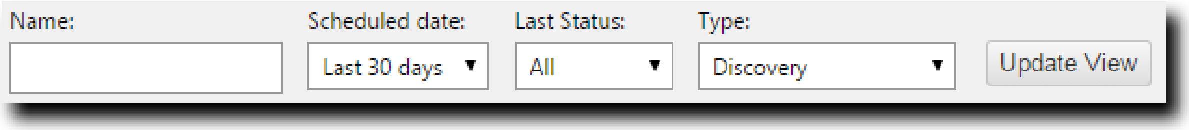


Figure 9: Filters

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.

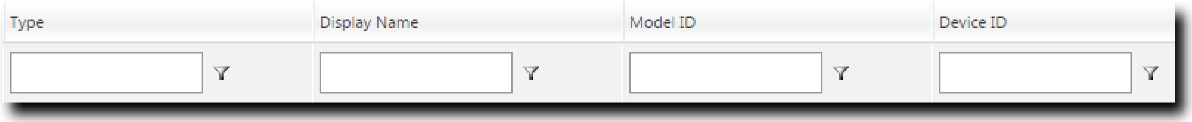


Figure 10: Filter Row

- 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 31.
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.

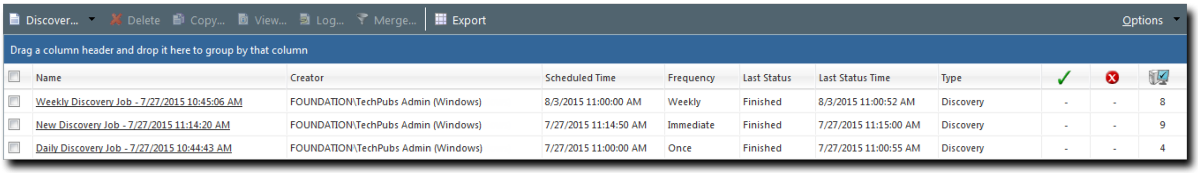
Result: The list column is filtered according to the criteria. If desired, repeat the process to filter additional columns.

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**.



Drag a column header and drop it here to group by that column

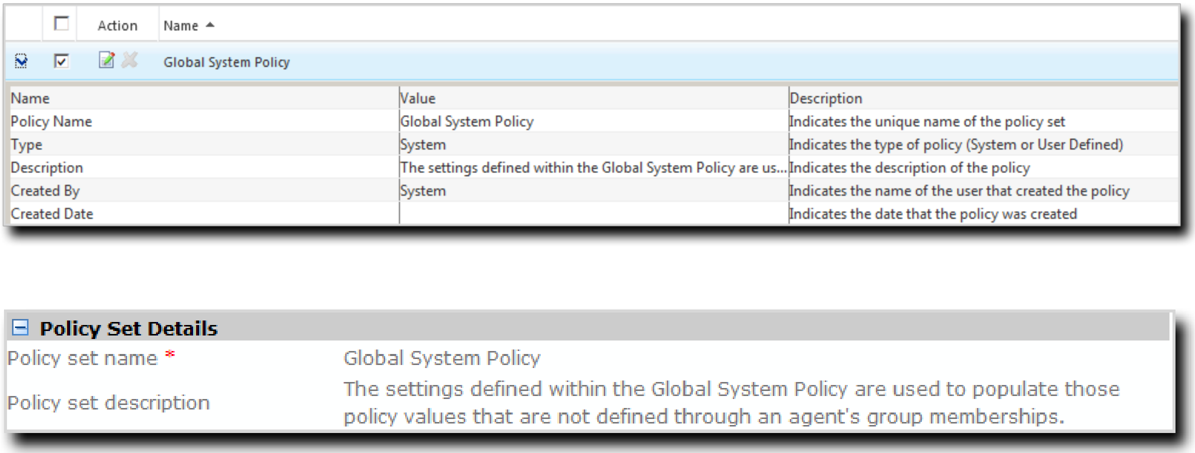
□	Name	Creator	Scheduled Time	Frequency	Last Status	Last Status Time	Type	✓	☒	
□	Weekly Discovery Job - 7/27/2015 10:45:06 AM	FOUNDATION\TechPubs Admin (Windows)	8/3/2015 11:00:00 AM	Weekly	Finished	8/3/2015 11:00:52 AM	Discovery	-	-	8
□	New Discovery Job - 7/27/2015 11:14:20 AM	FOUNDATION\TechPubs Admin (Windows)	7/27/2015 11:14:50 AM	Immediate	Finished	7/27/2015 11:15:00 AM	Discovery	-	-	9
□	Daily Discovery Job - 7/27/2015 10:44:43 AM	FOUNDATION\TechPubs Admin (Windows)	7/27/2015 11:00:00 AM	Once	Finished	7/27/2015 11:00:55 AM	Discovery	-	-	4

Figure 11: 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.



□	Action	Name ▲
☑		Global System Policy

Name	Value	Description
Policy Name	Global System Policy	Indicates the unique name of the policy set
Type	System	Indicates the type of policy (System or User Defined)
Description	The settings defined within the Global System Policy are us...	Indicates the description of the policy
Created By	System	Indicates the name of the user that created the policy
Created Date		Indicates the date that the policy was created

⊟ **Policy Set Details**

Policy set name *	Global System Policy
Policy set description	The settings defined within the Global System Policy are used to populate those policy values that are not defined through an agent's group memberships.

Figure 12: 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.

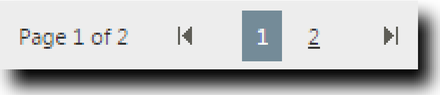


Figure 13: Pagination Feature

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.

Icon or Link	Title	Function
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**.

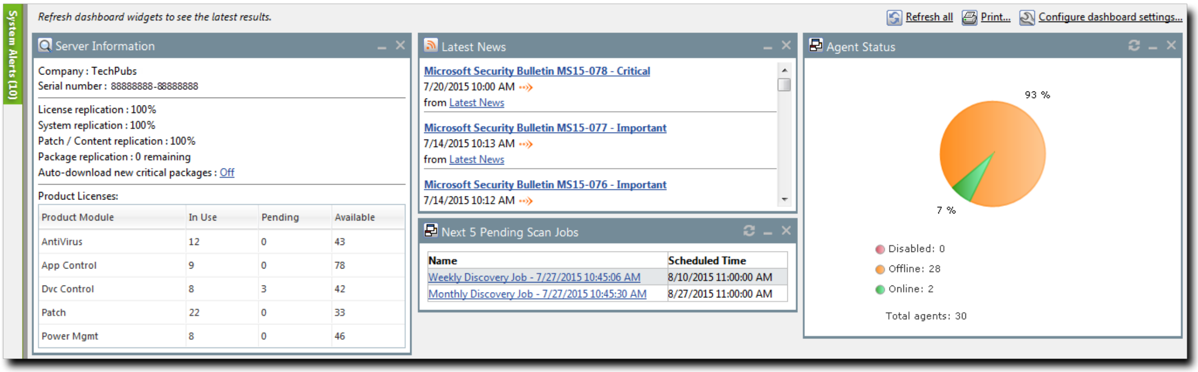
   Step Result: The ***File Download*** dialog opens.
4. Use the browser controls to complete the data export.

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.



Refresh dashboard widgets to see the latest results.

Company : TechPubs
Serial number : 88888888-88888888

License replication : 100%
System replication : 100%
Patch / Content replication : 100%
Package replication : 0 remaining
Auto-download new critical packages : Off

Product Licenses:

Product Module	In Use	Pending	Available
AntiVirus	12	0	43
App Control	9	0	78
Dvc Control	8	3	42
Patch	22	0	33
Power Mgmt	8	0	46

Microsoft Security Bulletin MS15-078 - Critical
7/20/2015 10:00 AM
from Latest News

Microsoft Security Bulletin MS15-077 - Important
7/14/2015 10:13 AM
from Latest News

Microsoft Security Bulletin MS15-076 - Important
7/14/2015 10:12 AM

Name	Scheduled Time
Weekly Discovery Job - 7/27/2015 10:45:06 AM	8/10/2015 11:00:00 AM
Monthly Discovery Job - 7/27/2015 10:45:30 AM	8/27/2015 11:00:00 AM

● Disabled: 0
● Offline: 28
● Online: 2

Total agents: 30

Figure 14: 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 on page 41
- The Agent Status Widget on page 41
- The Discovery Scan Results: Agents Widget on page 41
- The Last 5 Completed Scan Jobs Widget on page 42
- The Latest News Widget on page 42
- The Next 5 Pending Scan Jobs Widget on page 42
- The Server Information Widget on page 43

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 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 16: 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.

Field	Description
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 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 17: Last 5 Completed Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the name to open the ***Results*** page for the job.
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 Next 5 Pending Scan Jobs Widget

This widget displays information about the next five pending discovery scan jobs.

Table 18: 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 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 19: 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.

Table 20: Product Licenses Table Columns

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

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 21: Widget Setting and Behavior Icons

Icon	Action
🔧	Opens the ***Dashboard Settings*** dialog.
🖨	Opens the dashboard in print preview mode.
⊟	Collapses the associated widget.

Icon	Action
▣	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.

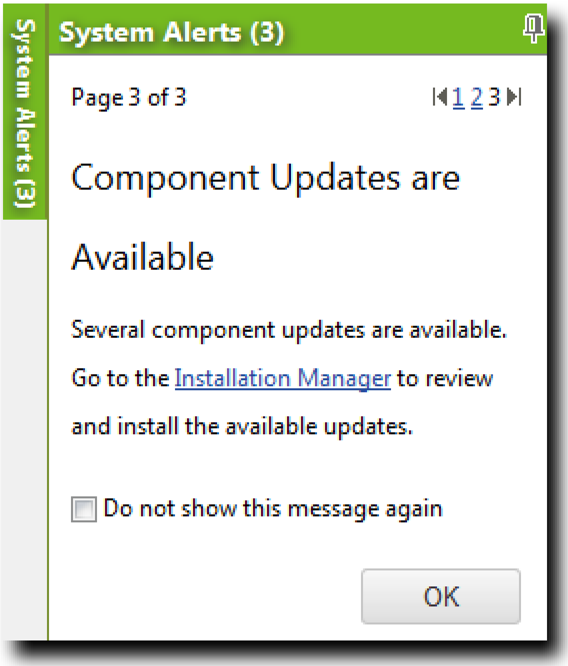
5. Display or hide widget descriptions.
   - Click ▤ to display descriptions.
   - Click ▭ to hide descriptions.
6. Choose a widget layout.
   - Click ◫ to display widgets in two columns.
   - Click ▦ to display widgets in three columns.
7. Click **OK**.

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.



Component Updates are Available

Several component updates are available. Go to the Installation Manager to review and install the available updates.

□ Do not show this message again

Figure 15: The System Alert Pane

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

Table 22: 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 38.
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 23: 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`.

Tip:

- You can view subscription service history from The Subscription Updates Page on page 80.
- You can also view license information from The Product Licensing Page on page 77.

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

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

Chapter

4

Configuring Options

In this chapter:

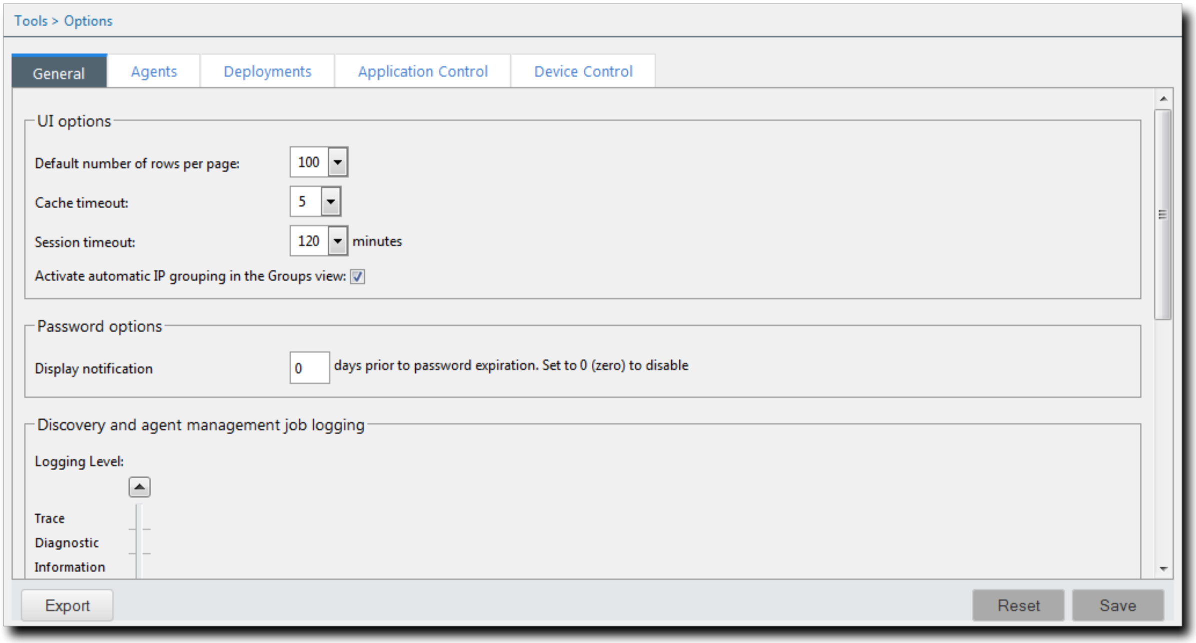
- The Options Page
- Working with Options

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

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

The Options Page

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



UI options

Default number of rows per page: 100

Cache timeout: 5

Session timeout: 120 minutes

Activate automatic IP grouping in the Groups view: ☑

Password options

Display notification 0 days prior to password expiration. Set to 0 (zero) to disable

Discovery and agent management job logging

Logging Level:

Trace

Diagnostic

Information

Figure 16: Options Page

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

- The General Tab on page 51
- The Agents Tab on page 54

The Options Page Buttons

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

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

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Reset	Cancels any edits made to the options since the tab was loaded.
Save	Saves the tab option settings (if any edits were made). You must click this button to implement your edits.

Viewing the Options Page

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

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

1. From the **Navigation Menu**, select **Tools** > **Options**.
2. Select a tab.
3. [Optional] Complete a task listed in Working with Options on page 58.

The General Tab

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

UI Options

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

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

Table 24: UI Options

Option	Description
Default number of rows per page	Defines the default number of rows that display in list pages (**25**, **50**, **100**, **200**, **500**).
Cache timeout	Defines the maximum number of minutes data is held in the memory before it needs to be reloaded from the database (**5**, **10**, **15**, **20**, **30**).
Session timeout	Defines the number of minutes before a repeat login is required due to inactivity (**20**, **40**, **60**, **80**, **100**, **120**).
Activate automatic IP grouping in the Groups view	Creates groups organized by IP address in the ***Groups*** page **Browser** named **IP Collection**.
Enhanced Reports URL	Defines the URL that is opened when **Reports** > **Enhanced Reports** is selected from the **Navigation Menu**. This feature is intended to open a third-party reporting solution, but you can use it to open any URL you want.

Password Options

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

Complete the field to configure the options.

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

Table 25: Password Options

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

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

Discovery and Agent Management Job Logging

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

Table 26: Discovery and Agent Management Job Logging Options

Option	Description
Logging Level	Defines the information recorded in the job during Discovery Scan Jobs and Agent Management Jobs. Options include: • **Trace** • **Diagnostic** • **Information** • **Warning** • **Error** • **Critical**
Include common troubleshooting information for	Defines whether the log include common troubleshooting information for a given part of a job. Options include: • **Agent Management** • **Discover** • **SOAP**

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

Report and Display Options

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

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

Table 27: Report and Display Options

Option	Description
Date format	Defines the date format displayed in text-based and graphical reports. Select from the following options: • **Default** (mm/dd/yyyy) • **MM/dd/yyyy** • **dd/MM/yyyy** • **yyyy-MM-dd** • **dd.MM.yyyy** • **dd-MM-yyyy** • **yyyy/MM/dd**
Time separator	Defines the character used to separate hours, minutes, and seconds in reports. Select from the following options: • **Default** (the current character in use) • **Colon** (**:**) • **Period** (**.**) This option also defines the time format used in reports. Select from the following options: • **12 Hour** • **24 Hour**
Time format	Displays the selected **Date Format** punctuated by the selected **Time Separator**. This field refreshes as you select different **Report and display options**.
Paper size for reports	Defines how reports are formatted for printing. Select from the following options: • **Default** (the currently saved formatting style) • **Letter** • **A4**

The Agents Tab

This tab contains default options related to the agent.

Default option sections include:

- Agent Installation on page 54
- Communication on page 55
- Absentee Agent Deletion on page 55
- Agent Versions on page 56

Agent Installation

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

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

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

Table 28: Agent Installation Options

Agent Installation Option	Description
Timeout (drop-down list)	Defines the default number of minutes before an agent installation job terminates due to non-responsive status (0-30).
Number of retries (drop-down list)	Defines the default number of attempts an agent installation will retry if initial and subsequent installations fails (1-10).
Number of simultaneous installs (drop-down list)	Defines the default maximum number of agents that can be installed or un-installed simultaneously during an Agent Management Job (1-25). A setting of `1` indicates that serial install/uninstalls should occur.
Server identity (field)	Defines the default text entered in the **Server Identity** field during agent installation jobs. **Server Identity** is the name agents list as their Ivanti Endpoint Security server.

<table>
<tr><th>Agent Installation Option</th><th>Description</th></tr>
<tr><td><b>Scan method for pre-selected targets</b>
(radio buttons)</td><td>Defines how endpoints pre-selected from a page list are added to a job's <b>targets</b> list (discovery scan or agent management) after launching a job configuration dialog. The options are:
<table>
<tr><td><b>IP Address</b></td><td>Adds the selected endpoint to a job's target list using its IP address.</td></tr>
<tr><td><b>Computer Name</b></td><td>Adds the selected endpoint to a job's target list using its endpoint name.</td></tr>
</table>
</td></tr>
</table>

Communication

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

Table 29: Communication Options

Option	Description
Agents should be shown offline when inactive for	Defines the time period (in minutes, hours, or days) before an agent is considered offline because it has not checked. A value of *0* disables this option. **Tip:** Disabled and uninstalled agents are not considered offline.

Absentee Agent Deletion

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

Table 30: Absentee Agent Deletion Option

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

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

Agent Versions

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

Table 31: Agent Version Options

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

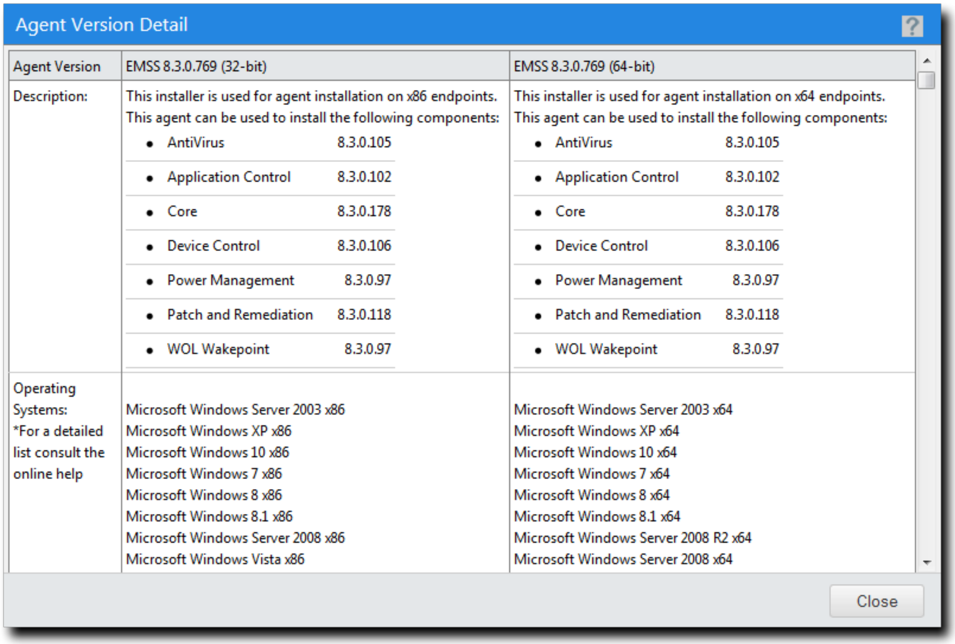
Note:

When selecting agent version options, remember the following information:

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

The Agent Version Detail Dialog

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



Agent Version	EMSS 8.3.0.769 (32-bit)	EMSS 8.3.0.769 (64-bit)
Description:	This installer is used for agent installation on x86 endpoints. This agent can be used to install the following components: • AntiVirus 8.3.0.105 • Application Control 8.3.0.102 • Core 8.3.0.178 • Device Control 8.3.0.106 • Power Management 8.3.0.97 • Patch and Remediation 8.3.0.118 • WOL Wakepoint 8.3.0.97	This installer is used for agent installation on x64 endpoints. This agent can be used to install the following components: • AntiVirus 8.3.0.105 • Application Control 8.3.0.102 • Core 8.3.0.178 • Device Control 8.3.0.106 • Power Management 8.3.0.97 • Patch and Remediation 8.3.0.118 • WOL Wakepoint 8.3.0.97
Operating Systems: *For a detailed list consult the online help	Microsoft Windows Server 2003 x86 Microsoft Windows XP x86 Microsoft Windows 10 x86 Microsoft Windows 7 x86 Microsoft Windows 8 x86 Microsoft Windows 8.1 x86 Microsoft Windows Server 2008 x86 Microsoft Windows Vista x86	Microsoft Windows Server 2003 x64 Microsoft Windows XP x64 Microsoft Windows 10 x64 Microsoft Windows 7 x64 Microsoft Windows 8 x64 Microsoft Windows 8.1 x64 Microsoft Windows Server 2008 R2 x64 Microsoft Windows Server 2008 x64

Figure 17: Agent Version Detail Dialog

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

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

Working with Options

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

- Configuring the General Tab on page 58
- Configuring the Agents Tab on page 60
- Exporting Option Data on page 61

Configuring the General Tab

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

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

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

   These options define general user interface behavior.

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

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

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

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

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

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

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

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

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

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

4. Define the **Password options**.

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

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

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

   a) Select a **Logging Level**.

      Logging levels include:

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

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

      Option include:

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

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

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

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

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

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

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

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

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

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

      This option defines how reports are formatted for printing.

7. Click **Save**.

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

Configuring the Agents Tab

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

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

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

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

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

   These options define the default values for Agent Management Jobs.

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

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

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

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

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

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

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

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

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

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

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

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

4. Define the **Communication** options.

   To define these options, complete the following substeps.

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

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

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

Select from the following values:

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

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

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

6. Define the **Agent Versions** options.

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

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

   a) Select a value from the **Windows 7 and newer agent version**.

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

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

   Note: This option only defines which agent version is available when working with the ***Manage Agent Versions*** dialog, the ***Download Agent Installers*** dialog, or the ***Install Agents Wizard***. It does not automatically install newly released agent versions on network endpoints. To ensure the newest agent version is installed on network endpoints, you must manually define the latest version. For additional information, refer to Upgrading Endpoints on page 173.

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

7. Click **Save**.

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

Exporting Option Data

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

For additional information, refer to Exporting Data on page 39.

Chapter 5

Configuring Notifications

In this chapter:

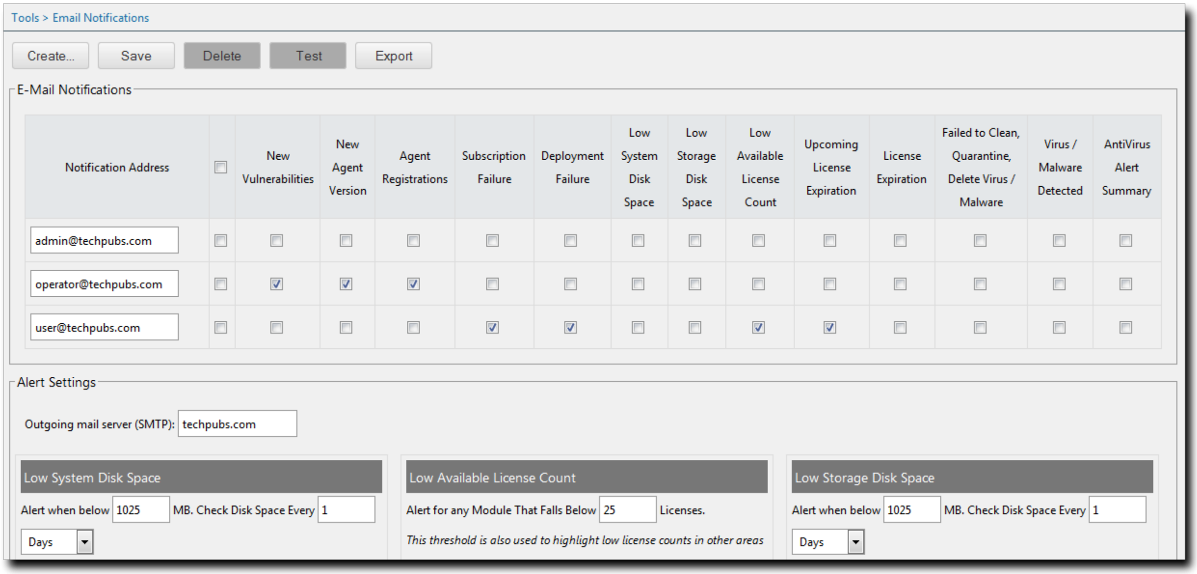
Ivanti Endpoint Security contains several features to notify users of system events and Global Subscription Service updates.

These features include:

- Email notifications. This feature uses your network mail server to send email that system events have occurred. For additional information, refer to The Email Notifications Page on page 64.
- Global Subscription Service notifications. You can subscribe to a RSS feed that lists updates posted to the Global Subscription Service. For additional information, refer to GSS Notifications on page 70.

The Email Notifications Page

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



E-Mail Notifications

Notification Address	□	New Vulnerabilities	New Agent Version	Agent Registrations	Subscription Failure	Deployment Failure	Low System Disk Space	Low Storage Disk Space	Low Available License Count	Upcoming License Expiration	License Expiration	Failed to Clean, Quarantine, Delete Virus / Malware	Virus / Malware Detected	AntiVirus Alert Summary
admin@techpubs.com	□	□	□	□	□	□	□	□	□	□	□	□	□	□
operator@techpubs.com	□	☑	☑	☑	□	□	□	□	□	□	□	□	□	□
user@techpubs.com	□	□	□	□	☑	☑	□	□	☑	☑	□	□	□	□

Alert Settings

Outgoing mail server (SMTP): techpubs.com

Low System Disk Space

Alert when below 1025 MB. Check Disk Space Every 1 Days

Low Available License Count

Alert for any Module That Falls Below 25 Licenses.

This threshold is also used to highlight low license counts in other areas

Low Storage Disk Space

Alert when below 1025 MB. Check Disk Space Every 1 Days

Figure 18: Email Notifications Page

From this page, you can perform the following actions:

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

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

Email Notification Page Buttons

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

Table 32: Email Notification Page Buttons

Button	Function
Create...	Creates a new item to **Email Notifications**. For additional information, refer to Creating Email Notifications on page 68.
Save	Saves any page edits made.

Button	Function
Delete	Deletes selected items from **Email Notifications**. For additional information, refer to Deleting Email Notification Addresses on page 69.
Test	Sends a test email to selected email addresses. For additional information, refer to Testing Email Notifications on page 70.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Email Notifications Table

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

Table 33: E-Mail Notification Table

Column	Description
Notification Address	Lists the email address that receives alert notifications. This address is not validated.
New Agent Version	Alerts when a new version of the agent is downloaded.
Agent Registrations	Alerts when an agent successfully registers or attempts and fails to register with the server.
Subscription Failure	Alerts when any subscription replication fails.
Low System Disk Space	Alerts when the available system drive space on the server falls below the defined minimum.
Low Storage Disk Space	Alerts when the available storage space on the drive where content is stored falls below the defined minimum.
Low Available License Count	Alerts when the number of licenses available to the server falls below the defined minimum.
Upcoming License Expiration	Alerts when licenses will expire within the defined time frame.
License Expiration	Alerts when a license expires.

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

Alert Settings

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

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

Table 34: Alert Settings Options

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

<table>
<tr><th>Option</th><th colspan="2">Definition</th></tr>
<tr><td rowspan="3">**Low Available License Count**</td><td colspan="2">Defines the threshold that initiates email notifications due to low available license count.</td></tr>
<tr><td>**Alert for any Module That Falls Below *x* Licenses**</td><td>Defines the number of available licenses that your server must drop below before an alert is sent (1-999).</td></tr>
<tr><td>**While License Count Remains Low, Send a Reminder E-mail Every *x* Days**</td><td>Defines if an alert is sent and the interval in days (1-99).</td></tr>
<tr><td rowspan="3">**Upcoming License Expiration**</td><td colspan="2">Defines the threshold that initiates email notifications due to upcoming license expiration.</td></tr>
<tr><td>**Alert for any License That Will Expire Within *x* Days**</td><td>Defines the number of days before an alert is generated due to upcoming license expiration (1-99).</td></tr>
<tr><td>**While Licenses Aren't Renewed After This Alert, Send a Reminder E-mail Every *x* Days**</td><td>Defines if an alert is sent and the interval in days (1-99).</td></tr>
</table>

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

Working with Email Notifications

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

- Configuring Alert Settings on page 67
- Creating Email Notifications on page 68
- Editing Email Notification Addresses on page 69
- Deleting Email Notification Addresses on page 69
- Testing Email Notifications on page 70

Configuring Alert Settings

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Click **Save**.

Result: Your alert setting values are saved.

Creating Email Notifications

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

Prerequisites:

Complete Configuring Alert Settings on page 67.

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

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

   Step Result: A new row displays in the **Email Notifications** table.

3. Type an email address in the **Notification Address** field of the new row.

   Note: The server does not validate email addresses.

4. Select the email notifications you want the address to receive.
5. Click **Save**.

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

Editing Email Notification Addresses

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

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

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

Deleting Email Notification Addresses

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

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

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

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

3. Click **Delete**.

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

4. Click **OK**.

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

Exporting Email Notification Data

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

All data on the page is exported. To export email notification data, select **Tools** > **Email Notifications** and click **Export**. For additional information, refer to Exporting Data on page 39.

Testing Email Notifications

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

Prerequisites:

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

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

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

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

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

3. Click **Test**.

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

GSS Notifications

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

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

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

Chapter 6

Licensing, Subscriptions, and Support

In this chapter:

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

View licensing information from the The Product Licensing Page on page 77. This page lists the Ivanti Endpoint Security modules you are licensed for.

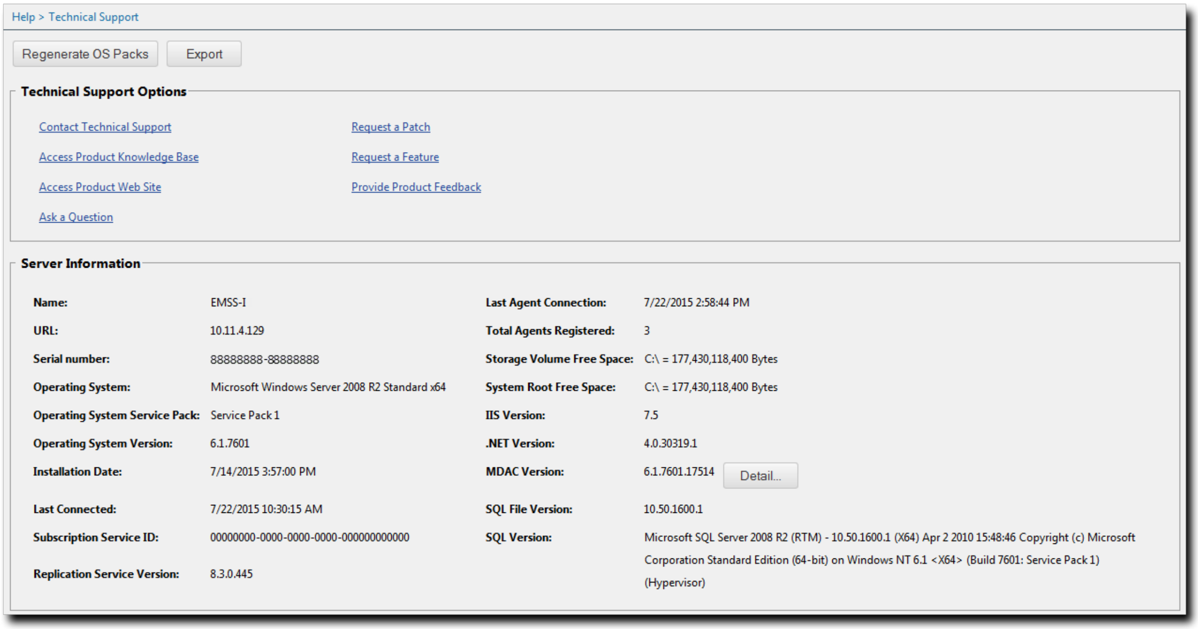
View your subscription history from the The Subscription Updates Page on page 80. This page lists a history of replications with the Global Subscription Service.

Request technical support from the The Technical Support Page on page 72. From this page you can request technical support and review technical information about your Ivanti Endpoint Security server.

The Technical Support Page

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

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



Technical Support Options

- Contact Technical Support
- Access Product Knowledge Base
- Access Product Web Site
- Ask a Question
- Request a Patch
- Request a Feature
- Provide Product Feedback

Server Information

Name:	EMSS-I	**Last Agent Connection:**	7/22/2015 2:58:44 PM
URL:	10.11.4.129	**Total Agents Registered:**	3
Serial number:	88888888-88888888	**Storage Volume Free Space:**	C:\ = 177,430,118,400 Bytes
Operating System:	Microsoft Windows Server 2008 R2 Standard x64	**System Root Free Space:**	C:\ = 177,430,118,400 Bytes
Operating System Service Pack:	Service Pack 1	**IIS Version:**	7.5
Operating System Version:	6.1.7601	**.NET Version:**	4.0.30319.1
Installation Date:	7/14/2015 3:57:00 PM	**MDAC Version:**	6.1.7601.17514 Detail...
Last Connected:	7/22/2015 10:30:15 AM	**SQL File Version:**	10.50.1600.1
Subscription Service ID:	00000000-0000-0000-0000-000000000000	**SQL Version:**	Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64) Apr 2 2010 15:48:46 Copyright (c) Microsoft Corporation Standard Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
Replication Service Version:	8.3.0.445		

Figure 19: Technical Support Page

Viewing the Technical Support Page

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

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

Technical Support Page Buttons

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

The following table describes each button.

Table 35: Technical Support Page Buttons

Button	Function
Regenerate OS Packs	Regenerates and synchronizes the relevant information for each of the operating systems supported by Ivanti Endpoint Security. For additional information, refer to Regenerating OS Packs on page 76.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Detail...	Opens a dialog that displays a detailed list of Microsoft Directory Access Components product and file versions. For additional information, refer to MDAC File Version Information on page 75.

Technical Support Options

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

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

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

Server Information

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

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

Table 36: Server Information Fields

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

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

Viewing the MDAC File Version Information Dialog

Navigate to this dialog to view MDAC file version information.

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

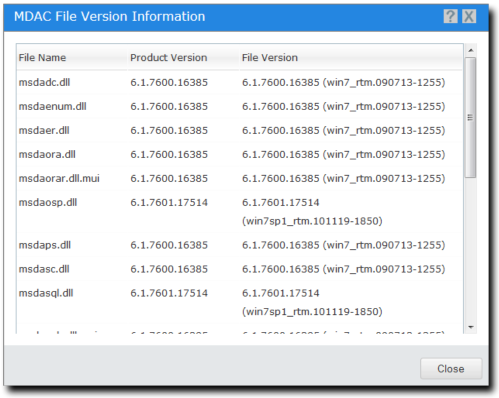
1. From the **Navigation Menu**, select **Help** > **Technical Support**.
2. Click **Detail**.

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

3. View the MDAC file version data.

MDAC File Version Information

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



File Name	Product Version	File Version
msdadc.dll	6.1.7600.16385	6.1.7600.16385 (win7_rtm.090713-1255)
msdaenum.dll	6.1.7600.16385	6.1.7600.16385 (win7_rtm.090713-1255)
msdaer.dll	6.1.7600.16385	6.1.7600.16385 (win7_rtm.090713-1255)
msdaora.dll	6.1.7600.16385	6.1.7600.16385 (win7_rtm.090713-1255)
msdaorar.dll.mui	6.1.7600.16385	6.1.7600.16385 (win7_rtm.090713-1255)
msdaosp.dll	6.1.7601.17514	6.1.7601.17514 (win7sp1_rtm.101119-1850)
msdaps.dll	6.1.7600.16385	6.1.7600.16385 (win7_rtm.090713-1255)
msdasc.dll	6.1.7600.16385	6.1.7600.16385 (win7_rtm.090713-1255)
msdasql.dll	6.1.7601.17514	6.1.7601.17514 (win7sp1_rtm.101119-1850)

Figure 20: MDAC File Version Information Dialog

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

Table 37: MDAC File Version Information

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

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

Suite Version Information

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

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

Table 38: Suite Version Information Fields

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

Regenerating OS Packs

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

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

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

   Step Result: A dialog displays, asking you to acknowledge the regeneration.

3. Click **OK**.

   Step Result: A dialog displays, asking you to acknowledge that the regeneration has been scheduled.

4. Acknowledge the scheduling by clicking **OK**.

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

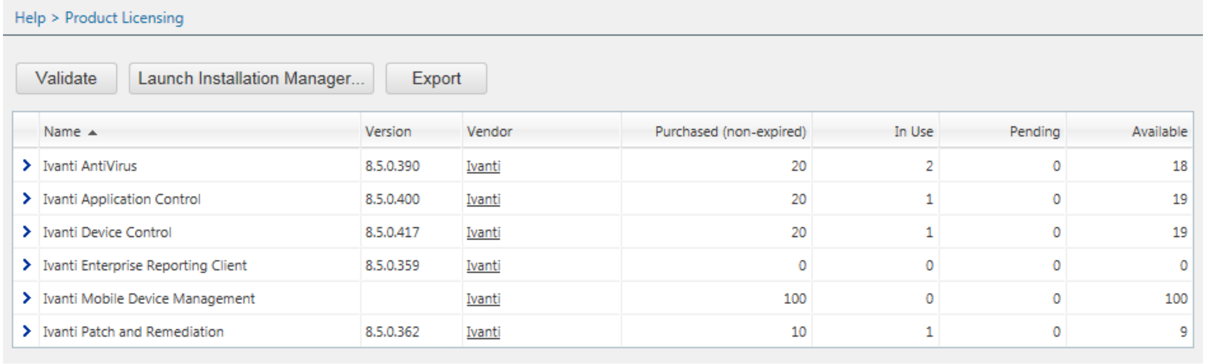
Exporting Technical Support Data

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

Exported data includes **Technical Support Options**, **Server Information**, and **Suite Version Information**. To export this data, select **Help** > **Technical Support** and click **Export**. For additional information, refer to Exporting Data on page 39.

The Product Licensing Page

Use this page to view, validate, and export license information. It summarizes product component licenses applicable to your endpoint management activities.



	Name ▲	Version	Vendor	Purchased (non-expired)	In Use	Pending	Available
>	Ivanti AntiVirus	8.5.0.390	Ivanti	20	2	0	18
>	Ivanti Application Control	8.5.0.400	Ivanti	20	1	0	19
>	Ivanti Device Control	8.5.0.417	Ivanti	20	1	0	19
>	Ivanti Enterprise Reporting Client	8.5.0.359	Ivanti	0	0	0	0
>	Ivanti Mobile Device Management		Ivanti	100	0	0	100
>	Ivanti Patch and Remediation	8.5.0.362	Ivanti	10	1	0	9

Figure 21: Product Licensing Page

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

Viewing the Product Licensing Page

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

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

The Product Licensing Page Buttons

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

The following table describes each button.

Table 39: Product Licensing Page Buttons

Button	Function
Validate	Initiates license replication. For additional information, refer to Initiating Subscription License Replication on page 79.
Launch Installation Manager...	Opens Ivanti Installation Manager. For additional information, refer to Using Ivanti Installation Manager on page 289 .
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Product Licensing Page List

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

Table 40: Product Licensing Page List

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

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

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

Table 41: Expanded Product Licensing List Item

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

Initiating Subscription License Replication

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

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

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

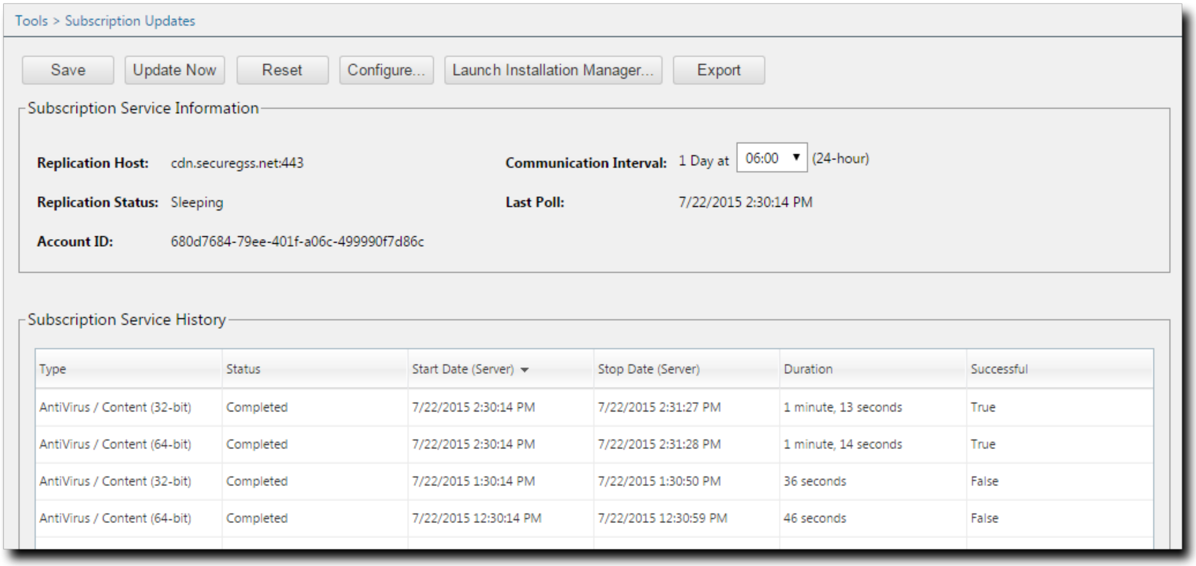
   Step Result: A dialog opens, prompting you to acknowledge the validation initiation.

3. Click **OK**.

Result: Replication begins. Completion may take several minutes.

The Subscription Updates Page

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


Tools > Subscription Updates
Save
Update Now
Reset
Configure...
Launch Installation Manager...
Export
Subscription Service Information
Subscription Service History

Replication Host: cdn.securegss.net:443

Communication Interval: 1 Day at 06:00 ▼ (24-hour)

Replication Status: Sleeping

Last Poll: 7/22/2015 2:30:14 PM

Account ID: 680d7684-79ee-401f-a06c-499990f7d86c

Type	Status	Start Date (Server) ▼	Stop Date (Server)	Duration	Successful
AntiVirus / Content (32-bit)	Completed	7/22/2015 2:30:14 PM	7/22/2015 2:31:27 PM	1 minute, 13 seconds	True
AntiVirus / Content (64-bit)	Completed	7/22/2015 2:30:14 PM	7/22/2015 2:31:28 PM	1 minute, 14 seconds	True
AntiVirus / Content (32-bit)	Completed	7/22/2015 1:30:14 PM	7/22/2015 1:30:50 PM	36 seconds	False
AntiVirus / Content (64-bit)	Completed	7/22/2015 12:30:14 PM	7/22/2015 12:30:59 PM	46 seconds	False

Figure 22: Subscription Updates Page

From this page, you can perform the following actions:

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

Viewing the Subscription Updates Page

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

You can access this page from the navigation menu.

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. [Optional] Perform a task listed in Working with Subscription Updates on page 86.

Subscription Updates Page Toolbar

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

The following table describes each button's function

Table 42: Subscription Updates Page Buttons

Button	Function
Save	Saves the page edits.
Update Now	Replicates all license, system, changes since the last replication with the Global Subscription Service (GSS). For additional information, refer to Updating Ivanti Endpoint Security System Files and Content on page 86.
Configure...	Configures subscription communication settings. For additional information, refer to The Subscription Service Configuration Dialog on page 83.
Launch Installation Manager...	Opens Ivanti Installation Manager. For additional information, refer to Using Ivanti Installation Manager on page 289 .
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Subscription Service Information

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

Table 43: Subscription Service Information

Field	Description
Replication Host	The name and port of the Global Subscription Service (GSS).
Replication Status	The current replication status. Replication ensures that your server remains current with the latest license information.
Account ID	Your account ID. The ID is uploaded to the GSS, which validates the update request. The account ID is created by your server when it registers with the GSS.

Field	Description
Communication Interval	The time your server connects to the GSS for replication. For additional information, refer to Editing the Communication Interval on page 86.
Last Poll	The date and time your server last replicated with the GSS.

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

Subscription Service History

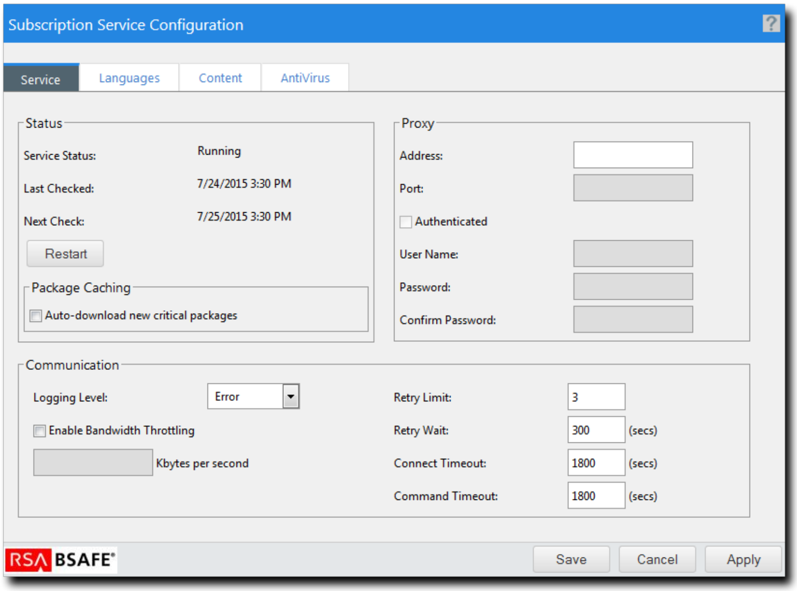
This table lists a record of subscription license replications and content replications. Additional details for each replication are included.

Table 44: Subscription Service History Table

Column	Description
Type	The type of replication. The types include: **Licenses** – Verifies the validity of your system licenses. **System** – Downloads new core system files, including operating system definitions and agent upgrades.
Status	The status of the replication task. The statuses include: `Initializing Replication` – Replications are initializing. `Downloading` – Replications are downloading. `Completed` – Replications are complete.
Start Date (Server)	The date and time on the server that the replication started.
Stop Date (Server)	The date and time on the server that the replication completed.
Duration	The duration of the replication.
Successful	The replication completion status (`True`, `False`, or `Failed`).

The Subscription Service Configuration Dialog

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



Service Status: Running

Last Checked: 7/24/2015 3:30 PM

Next Check: 7/25/2015 3:30 PM

□ Auto-download new critical packages

Address:

Port:

□ Authenticated

User Name:

Password:

Confirm Password:

Logging Level: Error

□ Enable Bandwidth Throttling

Kbytes per second

Retry Limit: 3

Retry Wait: 300 (secs)

Connect Timeout: 1800 (secs)

Command Timeout: 1800 (secs)

Figure 23: Subscription Service Configuration Dialog

Viewing the Subscription Service Configuration Dialog

Use this dialog to configure subscription service settings.

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

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

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

The Service Tab

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

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

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

Status

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

Table 45: Status Fields and Controls

Field or Control	Description
Service Status	The current status of the replication service on your server.
Last Checked	The last date and time on your server that the replication service last communicated with the GSS.
Next Check	The next scheduled date and time that the replication service will communicate with the GSS.
Restart	Restarts the replication service. For additional information, refer to Restarting the Replication Service on page 88.

Proxy

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

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

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

Table 46: Proxy Setting Descriptions

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

Setting	Description
Confirm Password (field)	The password retyped.

Communication

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

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

Table 47: Communication Option Descriptions

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

Working with Subscription Updates

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

- Updating Ivanti Endpoint Security System Files and Content on page 86
- Editing the Communication Interval on page 86
- Restarting the Replication Service on page 88

Updating Ivanti Endpoint Security System Files and Content

You can update the latest Ivanti Endpoint Security system components and content by completing a process call *Replication*. Replication downloads any system components, content definitions, or licensing information posted to the Global Subscription Service since the previous replication. Although the system automatically replicates once daily, you may occasionally need to replicate manually from time to time.

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

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

   Step Result: A notification dialog opens.

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

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

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

Editing the Communication Interval

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

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

1. From the **Navigation Menu**, select **Tools** > **Subscription Updates**.
2. Select a time from the **Communication Interval** list.

   This list includes a value for every half-hour.

3. Click **Save**.

   Step Result: A dialog opens, notifying that the new setting was saved.

4. Click **OK**.

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

Configuring the Service Tab

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

Prerequisites:

Configure the ***Service*** tab from the ***Subscription Service Configuration*** dialog.

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

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

3. Ensure the ***Service*** tab is selected.
4. Define **Proxy** options.

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

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

5. Define **Communication** options.

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

   Tip:

   - For additional information about each option, refer to Communication on page 85.
   - Under most conditions, the **Retry Limit**, **Retry Wait**, **Connect Timeout**, and **Command Timeout** options require no editing.

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

6. Click **Save** to apply your changes.

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

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

After Completing This Task:
If you edited the **Logging Level**, you must restart the replication service before the changes take place. For additional information, refer to Restarting the Replication Service on page 88.

Restarting the Replication Service

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

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

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

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

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

Result: The replication service is restarted on your server.

Chapter 7

Discovering Assets

In this chapter:

Use the Ivanti Endpoint Security to discover *assets*. Assets are endpoints (computers and laptops) and other devices (printers, routers, and so on).

Ivanti Endpoint Security discovers assets using a *Discovery Scan Job*.

After discovering assets, you can detect endpoints and then remotely install agents on the endpoints. Following agent installation, communication between agents and the Ivanti Endpoint Security server begins, leading to security management activity.

About Discovery Scan Jobs

Ivanti Endpoint Security uses network-based scanning to detect endpoints (computers, laptops, and so on) and devices (routers, printers, and so on) on your network. These scans are called *Discovery Scan Jobs*.

The primary purpose of *Discovery Scan Jobs* is to detect endpoints that have no agents installed. After these unprotected endpoints are detected, you can install agents on them, ensuring your endpoints are safe from potential security breaches. The secondary purpose of the Discovery Scan Job is to provide a census of network assets and other information. This census includes:

- Endpoints
- Endpoint address information
- Endpoint operating system information
- Devices (printers, routers, and so on)

The Discovery Scan Job is fully customizable. When configuring a Discovery Scan Job, you can control the following job behavior:

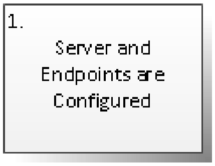
- Job date and time
- Job recurrence
- Job discovery methods used to define scan targets
- Job discovery options used to acquire asset information
- Job credentials used to acquire asset information

Important: You must have **Network discovery** and **File sharing** enabled to successfully discover endpoints. For additional information on enabling these security features, refer to Configuring Endpoints for Discovery on page 370.

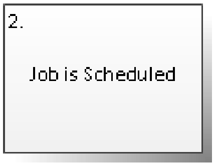
The Discovery Scan Process

A Discovery Scan Job locates endpoints in your network and scans them for endpoint information. To discover endpoints, you first schedule a job, and then the scan discovers the endpoints in an automated process.

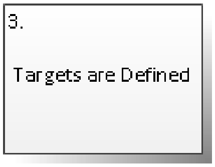
The following flowchart describes the sequence of events during the process of scanning for endpoints.



Configure your server and endpoints for scanning. To scan for endpoints, your Ivanti Endpoint Security server and your network endpoints must be configured for scanning.



Schedule a Discovery Scan Job. You can schedule scan jobs to run immediately or at a defined day and time.



Define targets for scanning. During scanning, your scan job searches for the targets you define.

4.
Job Activates

At the defined time, your Discovery Scan Job activates and begins scanning for defined targets. Jobs can either begin immediately following job configuration or at a scheduled date and time.

When your job completes, you can review your scan job results from the ***Job Results*** page. The ***Job Results*** page contains information on scheduled, active, and completed scans.

Working with Discovery Scan Jobs

The **Assets** menu item allows you to discover network assets. This task is available from the navigation menu under **Discover**.

To discover network assets using a Discovery Scan Job , refer to the following items:

- Discovering Assets by Discovery Scan Job on page 91
- Editing Targets on page 103

Discovering Assets by Discovery Scan Job

Use a Discovery Scan Job to finds endpoints and devices in your network. You can use this job type to schedule future jobs, recurring jobs, or jobs that only use certain discovery options.

Prerequisites:

- Ivanti Endpoint Security is installed and initial replication has completed.
- Windows endpoints must be configured to allow discovery scanning. For additional information about configuring Windows endpoints for discovery, refer to Configuring Endpoints for Discovery on page 370.

> **Important:** Windows operating systems can have security features that block a Discovery Scan Job. On Windows platforms, the target endpoints must have both **Network discovery** and **File sharing** enabled. If the target endpoints do not have these security features enabled, they are not discovered during a Discovery Scan Job.Installing Agents by Agent Management Job on page 109

You can create a Discovery Scan Job from the navigation menu or by clicking a toolbar button on the ***Job Results*** page.

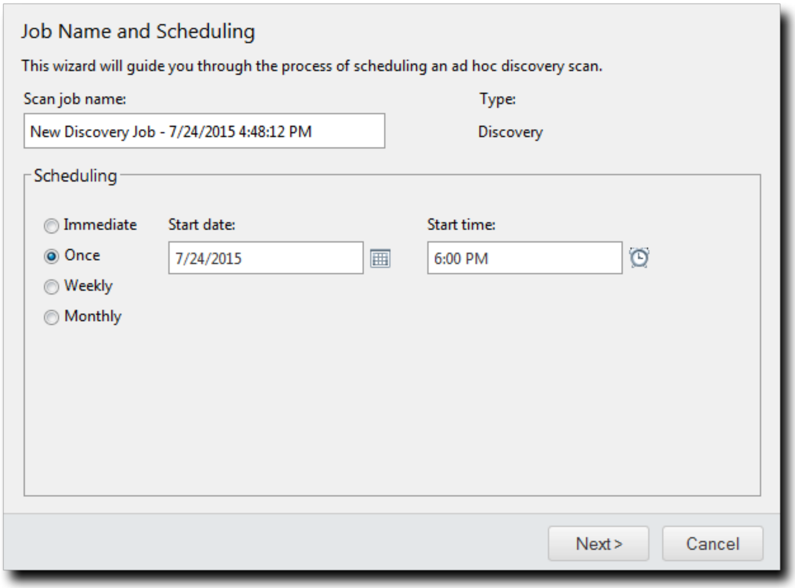
1. Select **Discover** > **Assets** to begin using the wizard.

   Complete one of the following steps to begin configuration.

Context	Steps
To open the Wizard from the toolbar:	Select **Discover** > **Assets**.

Context	Steps
To open the Wizard from the Asset Discovery Job Results page:	1. Select **Review** > **Asset Discovery Job Results**. 2. Select either the ***Scheduled***, ***Active***, or ***Completed*** tab. 3. Select **Discover** > **Assets**.
To open the Wizard from the Agent Management Job Results page:	1. Select **Review** > **Agent Management Job Results**. 2. Select either the ***Scheduled***, ***Active***, or ***Completed*** tab. 3. Select **Discover** > **Assets**.

Step Result: The wizard opens to the ***Job Name and Scheduling*** page.



Job Name and Scheduling

This wizard will guide you through the process of scheduling an ad hoc discovery scan.

Scan job name: New Discovery Job - 7/24/2015 4:48:12 PM

Type: Discovery

Scheduling

○ Immediate
● Once
○ Weekly
○ Monthly

Start date: 7/24/2015

Start time: 6:00 PM

Figure 24: Job Name and Scheduling Page

2. [Optional] Type a new name in the **Scan job name** field.

Note: By default, new Discovery Scan Jobs are named New Discovery Job, followed by the server date and time, which is formatted according to your server's ClientAdmin user locale setting.

3. Schedule the job.

   Use one of the following methods.

> **Tip:** During job scheduling, you can use the following shortcuts:
>
> - Click the **Calender** icon to select a **Start date**. Selecting a date automatically fills the **Start date** field.
> - Click the **Clock** icon to select a **Start time**. Selecting a time automatically fills the **Start time** field.

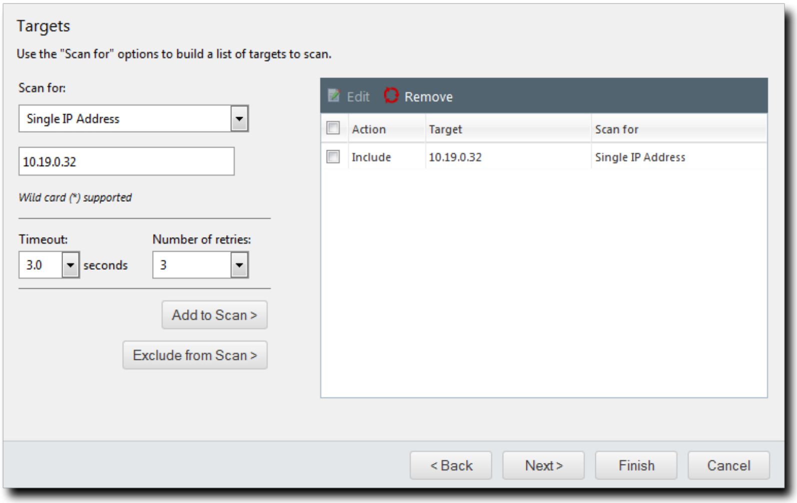
Method	Steps
To schedule an immediate job:	Select the **Immediate** option.
To schedule a one-time job:	**1.** Ensure the **Once** option is selected. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **Tip:** Scheduling a one-time job for a past date and time will launch the job immediately.
To schedule a recurring weekly job:	**1.** Select the **Weekly** option. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **4.** Define the day of the week the job runs by selecting a day from the **Run every week on the following day** list.

Method	Steps
To schedule a recurring monthly job:	1. Select the **Monthly** option. 2. Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. 3. Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. 4. Define the day of the month the job runs by typing a day in the **Run every month on the following day** field.

Tip: One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

4. Click **Next**.

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



Targets

Use the "Scan for" options to build a list of targets to scan.

Scan for: Single IP Address

10.19.0.32

Wild card (*) supported

Timeout: 3.0 seconds

Number of retries: 3

□	Action	Target	Scan for
□	Include	10.19.0.32	Single IP Address

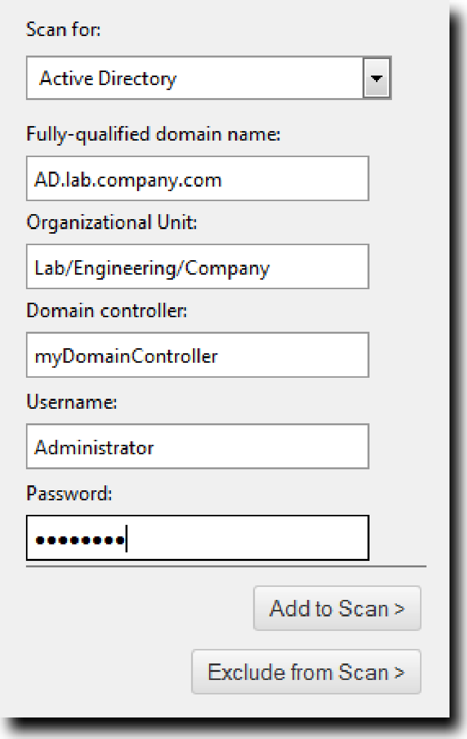
Figure 25: Targets Page

5. Define targets (endpoints) for the job to locate.
   Use one or more of the following discovery methods.

Method	Steps
To define targets using a single IP address:	1. From the **Scan for** list, select **Single IP Address**. 2. Type an IP address in the empty field. Wildcards are supported. **Note:** For additional information, refer to Defining Targets Using Wildcards on page 106. 3. Select an item in the **Timeout** list. **Note:** The Timeout list defines the number of seconds before a scan fails per attempt due to inactivity for a particular target. Under most network conditions, the Timeout field does not require editing. 4. Edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.
To define targets using an IP range:	1. From the **Scan for** list, select **IP Range**. 2. In the first empty field, type the beginning of IP range. **Note:** Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 106. 3. In the second empty field, type the ending of the IP range. 4. Select an item in the **Timeout** list. **Note:** The Timeout list defines the number of seconds per attempt before a scan fails due to inactivity for that particular target. Under most network conditions, the Timeout field does not require editing. 5. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.
To define targets using a computer name:	1. From the **Scan for** list, select **Computer name**. 2. In the empty field, type an endpoint name in one of the following formats: `computername` or `domain\computername`.

Method	Steps
To define targets using network neighborhood:	**1.** From the **Scan for** list, select **Network Neighborhood**. **2.** From the second list, select the desired network neighborhood.
To define targets using active directory:	**1.** From the **Scan for** list, select **Active Directory**. **2.** In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. **Tip:** For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field. **3.** Optionally, in the **Organizational Unit** field, type the active directory organizational unit string from specific to broad, separating each string with front slashes (such as `Techpubs/Engineering/Corporate`). **Tip:** The omission of this field returns job results containing the full contents of all the active directory organizational units. **4.** In the **Domain controller** field, type the domain controller IP address. **5.** In the **Username** field, type a user name that authenticates with the domain controller. **Note:** Type the user name in one of the following format: `domainname\username` or `username`. **6.** In the **Password** field, type the password associated with the user name.

Method	Steps
To define targets using an imported file:	**1.** From the **Scan for** list, select **Import file**. **2.** Click **Browse**. **3.** Browse to the file you want to use for target discovery. **Note:** The following file types are supported: .txt and .csv. **4.** Click **Open**. **Tip:** For additional information about how to define targets within an imported file, refer to Defining Targets Within an Imported File on page 358.



Scan for: Active Directory

Fully-qualified domain name: AD.lab.company.com

Organizational Unit: Lab/Engineering/Company

Domain controller: myDomainController

Username: Administrator

Password: ••••••••

Figure 26: Active Directory Input Example

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

   Note: You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

Method	Steps
To include defined targets in the job:	Click **Add to Scan**.
To exclude defined targets from the job:	Click **Exclude from Scan**.

   Tip: Repeat this step to add additional targets to the list.

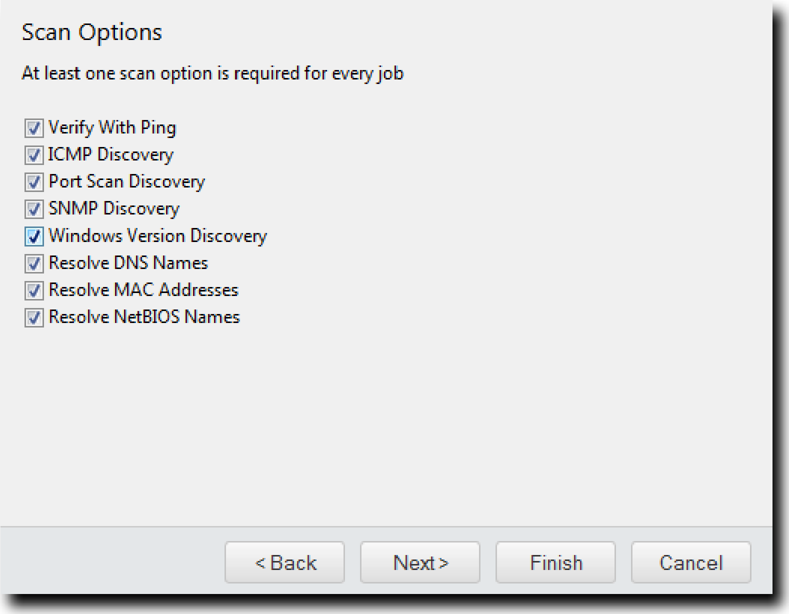
7. [Optional] Edit the **Targets** list.

   - To remove targets from the list, select the list item(s) and click **Remove**.
   - To edit targets on the list, select the list item(s) and click **Edit**.

   Note: For additional information, refer to Editing Targets on page 103.

8. Click **Next**.

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



Scan Options

At least one scan option is required for every job

- ☑ Verify With Ping
- ☑ ICMP Discovery
- ☑ Port Scan Discovery
- ☑ SNMP Discovery
- ☑ Windows Version Discovery
- ☑ Resolve DNS Names
- ☑ Resolve MAC Addresses
- ☑ Resolve NetBIOS Names

Figure 27: Scan Options

9. Select or clear the desired **Scan Options**.

   The following table defines each **Scan Option**.

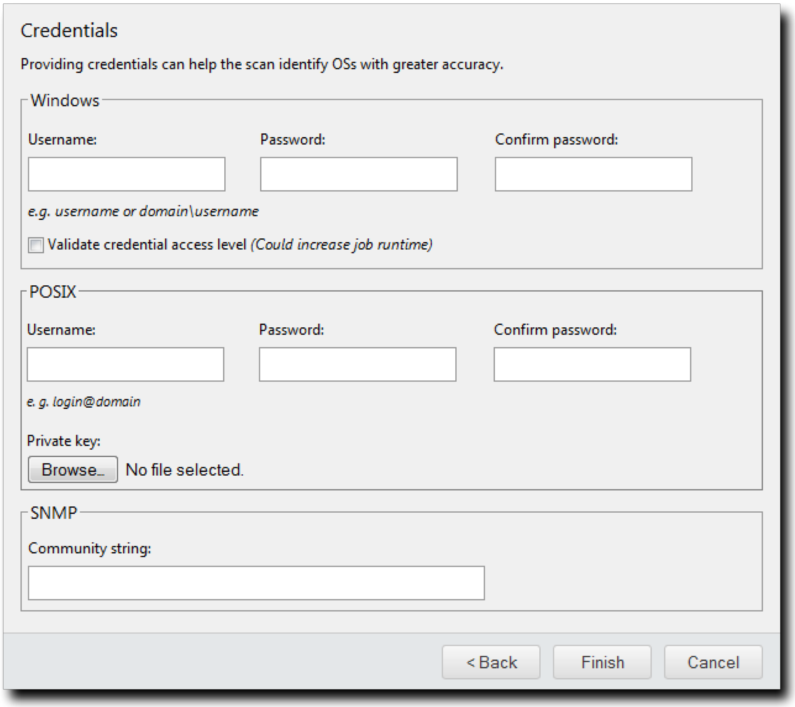
Option	Description
Verify With Ping	Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options. **Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust any antivirus and firewall configurations to permit ping requests.

Option	Description
ICMP Discovery	Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems. **Note:** **ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
Port Scan Discovery	Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified. **Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
SNMP Discovery	Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified. **Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default.
Windows Version Discovery	Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**. **Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**.
Resolve DNS Names	Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification.

Option	Description
Resolve MAC Addresses	Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification. **Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results.
Resolve NetBIOS Names	Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.

10. Click **Next**.

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



Credentials

Providing credentials can help the scan identify OSs with greater accuracy.

Figure 28: Credentials Page

11.[Optional] Define **Windows** credentials for the target.

Type the applicable information in the following fields.

Field	Description
Username	A user name that authenticates with Windows endpoints. Type the user name in a local format (`username`) or a domain format (`domain\username`).
Password	The password associated with the **Username**.
Confirm password	The **Password** retyped.

12.[Optional] Select the **Validate credentials access level** check box.

Selecting this check box validates the access levels that the entered credentials achieve on scan targets. This information is useful when determining if credentials provided the access necessary for Agent Management Jobs.

Note: Selecting this option could increase job run time.

13. If necessary, define **POSIX** credentials (credentials for UNIX-based operating systems).

Type the applicable information in the following fields.

Field	Description
Username	A user name that authenticates with POSIX endpoints. Type the user name in the following format: `login@domain`.
Password	The password associated with the **Username**.
Confirm password	The **Password** retyped.

14. If necessary, define a **POSIX** private key.

a) Click **Browse**.
b) Browse to the applicable `.txt` file.
c) Click **Open**.

15. If necessary, define an **SNMP** community string that authenticates with network devices.

a) Type the applicable community string in the **Community string** field.

16. Click **Finish**.

Result: The ***Discover Assets Wizard*** closes. Depending on how you scheduled the job, the Discover Scan Job moves to either the ***Job Results*** page's ***Scheduled*** or ***Active*** tab.

Editing Targets

While configuring jobs, you can edit items included in the **Targets** list.

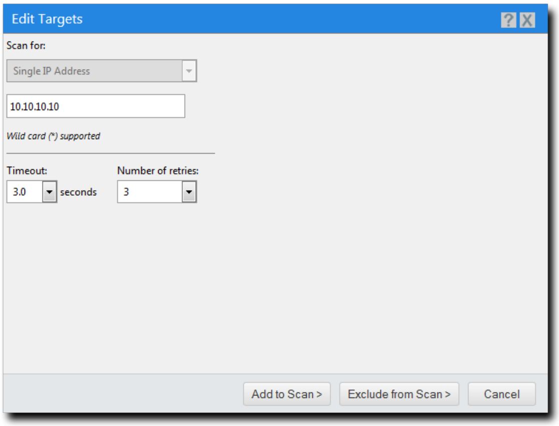
Edit **Target** list items from the ***Targets*** page of the wizard.

1. From the **Targets** list, select the check box associated with the item you want to edit.

   Step Result: The **Edit** button becomes active.

2. Click **Edit**.

   Step Result: The ***Edit Targets*** dialog opens.



Scan for: Single IP Address

10.10.10.10

Wild card (*) supported

Timeout: 3.0 seconds

Number of retries: 3

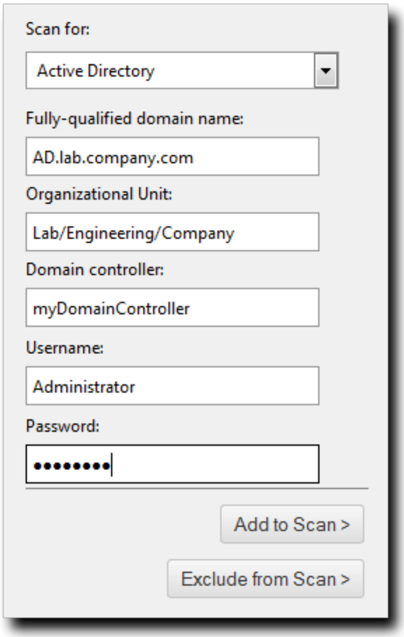
Figure 29: Edit Targets Dialog

3. Based on the type of discovery method, edit the item.

Discovery Method	Steps
Single IP Address	1. Type a new IP address in the field. Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 106. 2. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity. Under most network conditions, the **Timeout** field does not require editing. 3. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a discover assets scan retries if the scan times out.

Discovery Method	Steps
IP Range	1. In the field, type the beginning of IP range. Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 106. 2. In the field, type the ending of the IP range. 3. If necessary, edit the **Timeout** list. The **Timeout** list defines the number of seconds before a scan fails due to inactivity. Under most network conditions, the **Timeout** field does not require editing. 4. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a discover assets scan retries if the scan times out.
Computer Name	In the empty field, type a new endpoint name in one of the following formats: `endpointname` or `domain\endpointname`.
Network Neighborhood	From list, select the desired network neighborhood.

Discovery Method	Steps
Active Directory	**1.** In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. For example, if your domain controller's DNS name was *box.domain.company.local*, you would type *domain.company.local* in this field. **2.** Optionally, in the **Organizational Unit** field, type the active directory organizational unit string from specific to broad, separating each string with front slashes (such as `Techpubs/Engineering/Corporate`). The omission of this field returns job results containing the full contents of *all* the active directory organizational units. View the following figure for an example of how to enter data using **Active Directory**. **3.** In the **Domain controller** field, type the domain controller's IP address. **4.** In the **Username** field, type user name that will authenticate with the domain controller. Type the user name in one of the following format: `domainname\username` or `username`. **5.** In the **Password** field, type the password associated with the user name.



Scan for: Active Directory

Fully-qualified domain name: AD.lab.company.com

Organizational Unit: Lab/Engineering/Company

Domain controller: myDomainController

Username: Administrator

Password: ••••••••

Figure 30: Active Directory Input Example

4. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

Method	Steps
To include defined targets in the job:	Click **Add to Scan**.
To exclude defined targets from the job:	Click **Exclude from Scan**.

5. Review the **Targets** list.

Result: The **Targets** list reflects your changes.

Defining Targets Using Wildcards

When configuring a Discovery Scan Job or Agent Management Job, you can define scan targets using *wildcard* IP addresses. Wildcards are characters that can be used to substitute for any other character or characters in a string. In otherwords, you can use wildcards to scan for numerous IP address instead of just one. Use wildcards to scan specific IP address ranges.

The following table lists examples of how to define targets using wildcards.

Table 48: Wildcard Examples

Discovery Method	Step	Example	Targets Defined
To define wildcard IP addresses:	Type a wildcard IP address using commas (,). Type a wildcard IP address using dashes (-). Type a wildcard IP address using asterisks (*).	10.1.1.2,9 10.1.1.2-5 10.1.1.*	10.1.1.2 and 10.1.1.9 10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5 10.1.1.0 through 10.1.1.255
To define wildcard IP addresses using dashes in various octets:	Type a wildcard IP address using dashes, placing the dashes where applicable. You can use dashes in any octet.	10.2-4.5.9	10.2.5.9, 10.3.5.9, 10.4.5.9

Discovery Method	Step	Example	Targets Defined
To define wildcard IP addresses using asterisks in various octets:	Type a wildcard IP address using asterisks, placing the asterisks where applicable. You can use asterisks in any octet.	*.6.65.92 10.25.*.*	1.6.65.92 through 255.6.65.92 10.25.0.0 through 10.25.255.255
To define wildcard IP addresses using commas in various octets:	Type a wildcard IP address using commas, placing the commas where applicable. You can use commas in any octet.	10,12,19.2.5.9	10.2.5.9, 12.2.5.9, 19.2.5.9
To define wildcard IP addresses using a combination of wildcard characters:	Type a wildcard IP address using dashes, commas, and asterisks.	10-13.*.12.2,4,7 10.2-4.5,23.*	10, 11, 12, 13.0-255.12.2, 4, 7 10.2, 3, 4.5, 23.0-255

About Agent Management Jobs

An *Agent Management Job* lets you install the Ivanti Endpoint Security Agent remotely on multiple Windows endpoints within your network. An Agent Management Job eases the task of agent installation by letting you install agents from within the Ivanti Endpoint Security Web console.

These jobs are configured in the ***Agent Management Job Wizard***, which is similar in appearance to the ***Discovery Scan Job Wizard***.

consists of the following:

1. The first phase of an Agent Management Job is identical to a Discovery Scan Job; it detects endpoints and their operating systems within your network using a scan.

2. The second phase is agent installation and consists of the following:
   - Based on the operating system information found during scanning, the Agent Management Job determines that you can install an agent on a endpoint that contains a supported Windows operating system.
   - To access the endpoint, the Agent Management Job provides the endpoint with applicable credentials. These credentials are entered during job configuration.
   - After the endpoint authenticates the offered credentials, the Agent Management Job begins agent installation. Installation occurs silently in an endpoint's background; endpoint users are unaware of the installation.
   - Following configuration of an Agent Management Job, you can view it on the ***Job Results*** page. Based on how you scheduled the job, it appears on either the ***Scheduled*** tab or the ***Active*** tab. After the job finishes scanning and agent install has completed, it moves to the ***Completed*** tab.

Note: Remember the following information when working with an Agent Management Job:

- Verify that your target endpoints are Windows endpoints.

  Refer to the Ivanti Endpoint Security: Requirements Guide (https://help.ivanti.com) for a complete list of supported Windows platforms for endpoints.

  Important: Linux, UNIX, and Mac endpoints cannot have agents installed using an Agent Management Job.

- Ensure any anti-virus software installed on your target endpoints is disabled.
- Gather the built-in Administrator credentials for endpoints you are installing agents on. Successful job outcome is contingent upon authenticated credentials for this account.
- Configure your server to allow an Agent Management Job. For additional information, refer to Configuring the Ivanti Endpoint Security Server for Discovery Scanning on page 368.
- Configure your targets to allow an Agent Management Job. For additional information, refer to Configuring Endpoints for Agent Management Jobs on page 380

Working with Agent Management Jobs

The Ivanti Endpoint Security console utilizes an Agent Management Job to install or uninstall agents on Windows endpoints. The tasks to do this is available from the navigation menu under **Discover**.

To work with Agent Management Jobs, refer to the following items:

- Installing Agents by Agent Management Job on page 109
- Uninstalling Agents by Agent Management Job on page 122

For additional information on Agents, refer to the Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .

Installing Agents by Agent Management Job

You can install agents on network endpoints remotely by using Agent Management Jobs. Installing agents remotely substantially eases your workload, since you do not have to install agents locally.

Prerequisites:

- Verify that your target endpoints are Windows endpoints.

  Refer to the Ivanti Endpoint Security: Requirements Guide (https://help.ivanti.com) for a complete list of supported Windows platforms for endpoints.

  > **Important:** Linux, UNIX, and Mac endpoints cannot have agents installed using an Agent Management Job.

- Ensure any anti-virus software installed on your target endpoints is disabled.
- Gather the built-in Administrator credentials for endpoints you are installing agents on. Successful job outcome is contingent upon authenticated credentials for this account.
- Configure your server to allow an Agent Management Job. For additional information, refer to Configuring the Ivanti Endpoint Security Server for Discovery Scanning on page 368.
- Configure your targets to allow an Agent Management Job. For additional information, refer to Configuring Endpoints for Agent Management Jobs on page 380

Configuration of an Agent Management Job is similar to configuration of a Discovery Scan Job. Configuration occurs in the ***Install Agents Wizard***.

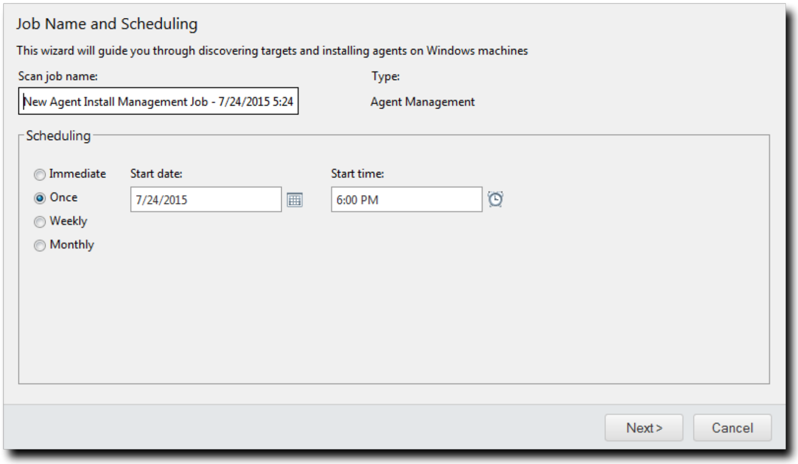
1. Begin configuration of the ***Install Agent Wizard***.

   Complete one of the following steps to begin configuration.

Context	Steps
To open the Wizard without targets predefined:	Select **Discover** > **Assets and Install Agents**.

Context	Steps
To open the Wizard with target predefined:	1. Select **Manage** > **Endpoints**. 2. Select the endpoints you want to install the agent on. 3. From the toolbar, select **Manage Agents** > **Install Agents**.

Step Result: The wizard opens to the ***Job Name and Scheduling*** page.



Job Name and Scheduling

This wizard will guide you through discovering targets and installing agents on Windows machines

Scan job name: New Agent Install Management Job - 7/24/2015 5:24

Type: Agent Management

Scheduling

○ Immediate
● Once
○ Weekly
○ Monthly

Start date: 7/24/2015

Start time: 6:00 PM

Figure 31: Job Name and Scheduling Page

2. [Optional] Type a new name in the **Scan job name** field.

Note: By default, a new Agent Management Job for installation is named `New Agent Install Management Job`, followed by the server's date and time.

3. Schedule the job.

   Use one of the following methods.

Tip: During job scheduling, you can use the following shortcuts:

- Click the **Calender** icon to select a **Start date**. Selecting a date automatically fills the **Start date** field.
- Click the **Clock** icon to select a **Start time**. Selecting a time automatically fills the **Start time** field.

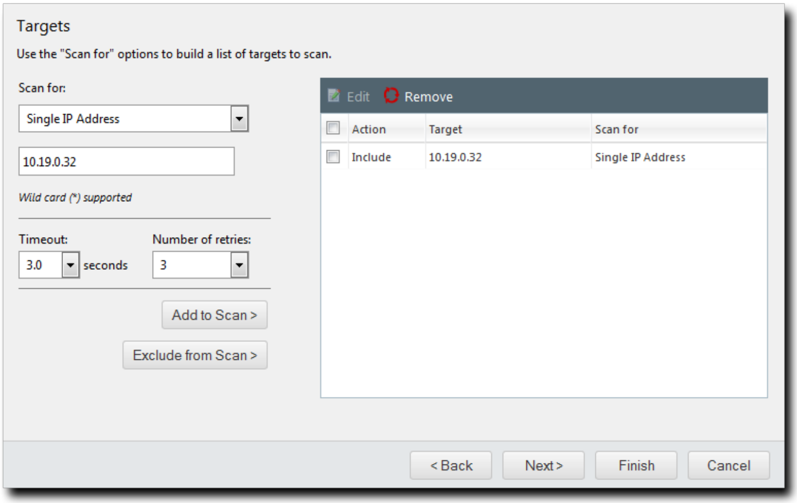
Method	Steps
To schedule an immediate job:	Select the **Immediate** option.

Method	Steps
To schedule a one-time job:	1. Ensure the **Once** option is selected. 2. Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. 3. Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **Tip:** Scheduling a one-time job for a past date and time will launch the job immediately.
To schedule a recurring weekly job:	1. Select the **Weekly** option. 2. Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. 3. Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. 4. Define the day of the week the job runs by selecting a day from the **Run every week on the following day** list.
To schedule a recurring monthly job:	1. Select the **Monthly** option. 2. Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. 3. Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. 4. Define the day of the month the job runs by typing a day in the **Run every month on the following day** field.

Tip: One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

4. Click **Next**.

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



Targets

Use the "Scan for" options to build a list of targets to scan.

Scan for: Single IP Address

10.19.0.32

Wild card (*) supported

Timeout: 3.0 seconds

Number of retries: 3

☐	Action	Target	Scan for
☐	Include	10.19.0.32	Single IP Address

Figure 32: Targets Page

5. Define targets (endpoints) for the job to locate.

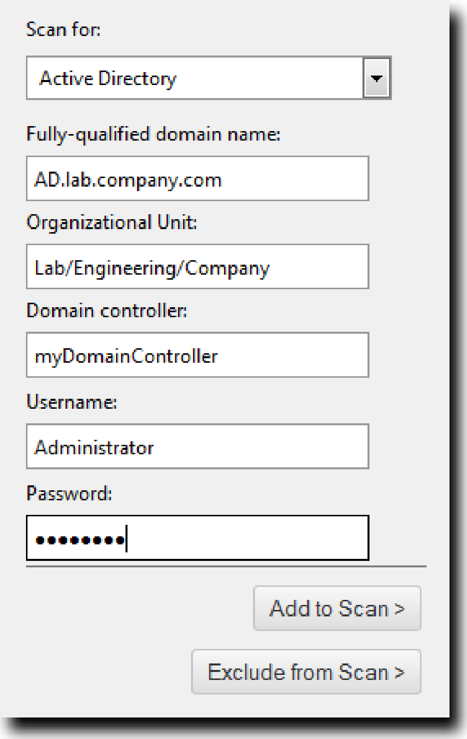
   Use one or more of the following discovery methods.

Method	Steps
To define targets using a single IP address:	1. From the **Scan for** list, select **Single IP Address**. 2. Type an IP address in the empty field. Wildcards are supported. **Note:** For additional information, refer to Defining Targets Using Wildcards on page 106. 3. Select an item in the **Timeout** list. **Note:** The Timeout list defines the number of seconds before a scan fails per attempt due to inactivity for a particular target. Under most network conditions, the Timeout field does not require editing. 4. Edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.

Method	Steps
To define targets using an IP range:	1. From the **Scan for** list, select **IP Range**. 2. In the first empty field, type the beginning of IP range. **Note:** Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 106. 3. In the second empty field, type the ending of the IP range. 4. Select an item in the **Timeout** list. **Note:** The Timeout list defines the number of seconds per attempt before a scan fails due to inactivity for that particular target. Under most network conditions, the Timeout field does not require editing. 5. If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.
To define targets using a computer name:	1. From the **Scan for** list, select **Computer name**. 2. In the empty field, type an endpoint name in one of the following formats: `computername` or `domain\computername`.
To define targets using network neighborhood:	1. From the **Scan for** list, select **Network Neighborhood**. 2. From the second list, select the desired network neighborhood.

Method	Steps
To define targets using active directory:	1. From the **Scan for** list, select **Active Directory**. 2. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. **Tip:** For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field. 3. Optionally, in the **Organizational Unit** field, type the active directory organizational unit string from specific to broad, separating each string with front slashes (such as `Techpubs/Engineering/Corporate`). **Tip:** The omission of this field returns job results containing the full contents of all the active directory organizational units. 4. In the **Domain controller** field, type the domain controller IP address. 5. In the **Username** field, type a user name that authenticates with the domain controller. **Note:** Type the user name in one of the following format: `domainname\username` or `username`. 6. In the **Password** field, type the password associated with the user name.

Method	Steps
To define targets using an imported file:	1. From the **Scan for** list, select **Import file**. 2. Click **Browse**. 3. Browse to the file you want to use for target discovery. **Note:** The following file types are supported: .txt and .csv. 4. Click **Open**. **Tip:** For additional information about how to define targets within an imported file, refer to Defining Targets Within an Imported File on page 358.



Scan for: Active Directory

Fully-qualified domain name: AD.lab.company.com

Organizational Unit: Lab/Engineering/Company

Domain controller: myDomainController

Username: Administrator

Password: ••••••••

Figure 33: Active Directory Input Example

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

   Note: You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

Method	Steps
To include defined targets in the job:	Click **Add to Scan**.
To exclude defined targets from the job:	Click **Exclude from Scan**.

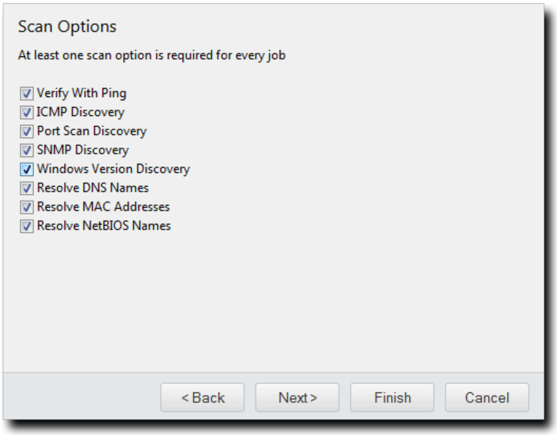
   Tip: Repeat this step to add additional targets to the list.

7. [Optional] Edit the **Targets** list.

   - To remove targets from the list, select the list item(s) and click **Remove**.
   - To edit targets on the list, select the list item(s) and click **Edit**. For additional information, refer to Editing Targets on page 103. .

8. Click **Next**.

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



Scan Options

At least one scan option is required for every job

☑ Verify With Ping
☑ ICMP Discovery
☑ Port Scan Discovery
☑ SNMP Discovery
☑ Windows Version Discovery
☑ Resolve DNS Names
☑ Resolve MAC Addresses
☑ Resolve NetBIOS Names

Figure 34: Scan Options Page

9. Select or clear the desired **Scan Options**.

   The following table defines each **Scan Option**.

Option	Description
Verify With Ping	Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options. **Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust any antivirus and firewall configurations to permit ping requests.
ICMP Discovery	Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems. **Note:** **ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
Port Scan Discovery	Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified. **Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
SNMP Discovery	Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified. **Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default.

Option	Description
Windows Version Discovery	Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**. **Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**.
Resolve DNS Names	Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification.
Resolve MAC Addresses	Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification. **Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results.
Resolve NetBIOS Names	Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.

10. Click **Next**.

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

11. Select the desired **Agent Options**.

These options control which version of the agent is installed on Windows-based endpoints.

a) Select an agent version from the **Agent version** list.

> **Note:** The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab. For additional information, refer to Agent Versions on page 56

b) Select the modules you want to install with the agent.

Select the check box associated with the module(s) you want to install.

c) [Optional] Select the **Overwrite existing agents** check box.

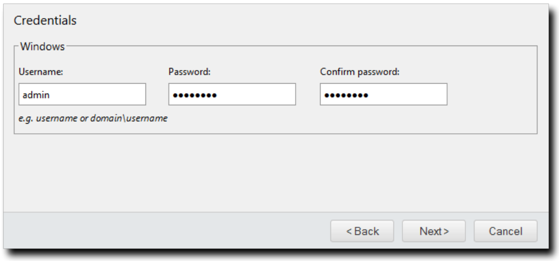
This option controls whether the Agent Management Job skips targets that already have agents installed.

> **Attention:** Selecting this option will cause data loss when an endpoint's Ivanti Endpoint Security Agent is overwritten.

12. Click **Next**.

> **Note:** If a dialog opens that notifies you that an endpoint reboot is required following agent installation, click **Continue** to dismiss the dialog.

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



Credentials

Windows

Username: admin

Password: ••••••••

Confirm password: ••••••••

e.g. username or domain\username

Figure 35: Credentials Page

13. Define **Windows** credentials for the target.

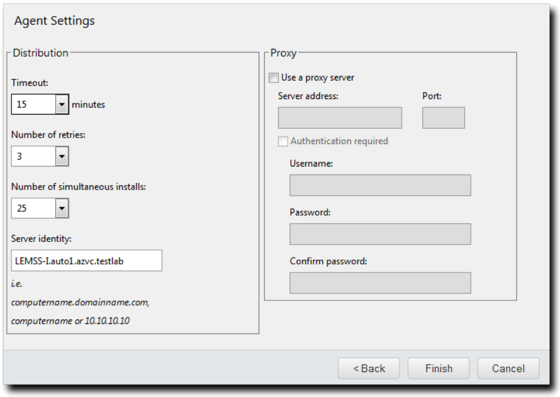
Type the applicable information in the following fields.

> **Note:** When configuring an Agent Management Job, you must define valid Windows credentials.

Field	Description
Username	A user name that authenticates with Windows-based endpoints. Type the user name in a local format (*`UserName`*) or a domain format (*`DOMAIN\UserName`*). **Note:** When configuring Agent Management Jobs, Ivanti recommends using the built-in Administrator account.
Password	The password associated with the **Username**.
Confirm password	The **Password** retyped.

14. Click **Next**.

Step Result: The ***Agent Settings*** page opens.



Agent Settings

Distribution

Timeout: 15 minutes

Number of retries: 3

Number of simultaneous installs: 25

Server identity: LEMSS-I.auto1.azvc.testlab

i.e.

computername.domainname.com,

computername or 10.10.10.10

Proxy

□ Use a proxy server

Server address:

Port:

□ Authentication required

Username:

Password:

Confirm password:

Figure 36: Agent Settings Page

15. Define the **Distribution** options.

The following table describes each list their available values.

List	Description
Timeout **(list)**	Defines the number of minutes before the Agent Management Job terminates an install attempt due to a non-responsive agent installation or removal (0-30).
Number of retries **(list)**	Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10).
Number of simultaneous installs **(list)**	Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of `1` indicates that serial installs or removals should occur.

16. Define the Ivanti Endpoint Security server that the agent will report to using the **Server Identity** field.

Define the **Server identity** using one of the following formats.

- DNS name (*`computername.domainname.com`*)
- Computer name (*`computername`*)
- IP address (*`10.10.10.10`*)

Tip: The wizard fills this field with the server computername by default.

17. If the target endpoints will communicate with the Ivanti Endpoint Security server through a proxy server following initial agent installation, select the **Use a proxy server** check box and define the following fields.

> **Note:** In many network environments, although a proxy is used for Internet access, a proxy bypass is used for all access within the corporate network. Therefore, only enter proxy information if your agents will be required to use a proxy to access your Ivanti Endpoint Security server.

Field	Description
Server address	The applicable proxy IP address.
Port	The applicable proxy port number used to communicate.

18. If the target endpoints will use a proxy for agent to server communication, and that proxy requires authentication, select the **Authentication required** check box and define the following fields.

Field	Description
Username	A user name that authenticates with the proxy.
Password	The password associated with the **Username**.
Confirm password	The **Password** retyped.

19. Click **Finish**.

Result: The ***Install Agents Wizard*** closes. Depending on how you configured the job, it moves to either the ***Scheduled*** tab or ***Active*** tab on the ***Job Results*** page. The job will run at the applicable time, installing agents on the defined targets, and move to ***Completed*** tab when finished.

After Completing This Task:

- If you installed an endpoint module that requires a reboot, reboot the endpoint(s) when the Agent Management Job completes.
- After the Agent Management Job completes, install agent modules if necessary. For additional information, refer to Installing Endpoint Modules on page 177.

Uninstalling Agents by Agent Management Job

You can remotely uninstall agents from endpoints in your network using an Agent Management Job. These jobs prevent administrators from having to uninstall agents locally.

Prerequisites:

- Verify that your target endpoints are Windows endpoints.

  Refer to the Ivanti Endpoint Security: Requirements Guide (https://help.ivanti.com) for a complete list of supported Windows platforms for endpoints.

  > **Important:** Linux, UNIX, and Mac endpoints cannot have agents installed using an Agent Management Job.

- Ensure any anti-virus software installed on your target endpoints is disabled.
- Gather the built-in Administrator credentials for endpoints you are installing agents on. Successful job outcome is contingent upon authenticated credentials for this account.
- Configure your server to allow an Agent Management Job. For additional information, refer to Configuring the Ivanti Endpoint Security Server for Discovery Scanning on page 368.
- Configure your targets to allow an Agent Management Job. For additional information, refer to Configuring Endpoints for Agent Management Jobs on page 380

You complete the Agent Management Job within the Ivanti Endpoint Security Web console using an easy-to-use wizard. Configuration of the Agent Management Job is similar to configuration of a Discovery Scan Job. Configuration occurs in the ***Uninstall Agents Wizard***.

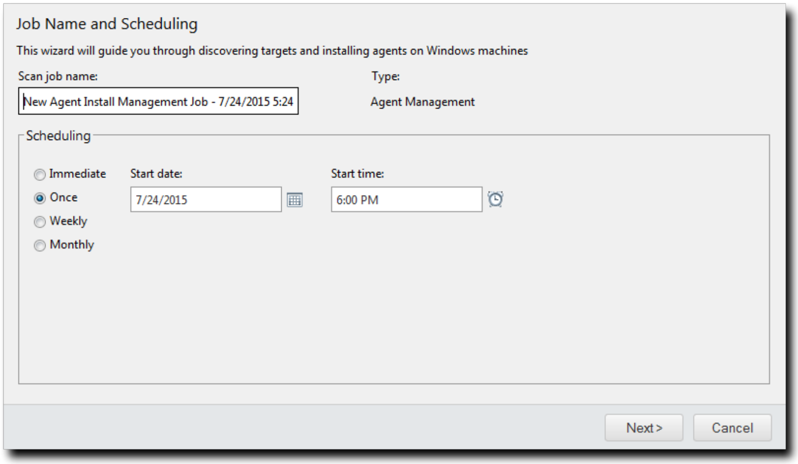
1. Begin configuration of the ***Uninstall Agent Wizard***.

   Complete one of the following steps sets to begin configuration.

Context	Steps
To open the Wizard without targets predefined:	Select **Discover** > **Assets and Uninstall Agents**

Context	Steps
To open the Wizard with target predefined:	**1.** Select **Manage** > **Endpoints**. **2.** Select the endpoints you want to uninstall agents from. **3.** From the toolbar, select **Manage Agents** > **Uninstall Agents**

Step Result: The wizard opens to the ***Job Name and Scheduling*** page.



Job Name and Scheduling

This wizard will guide you through discovering targets and installing agents on Windows machines

Scan job name: New Agent Install Management Job - 7/24/2015 5:24

Type: Agent Management

Scheduling

○ Immediate
● Once
○ Weekly
○ Monthly

Start date: 7/24/2015

Start time: 6:00 PM

Figure 37: Job Name and Scheduling Page

2. [Optional] Type a new name in the **Scan job name** field.

Note: By default, a new Agent Management Job for uninstallation is named `New Agent Uninstall Management Job`, followed by the server's date and time, which is formatted according to your browser's locale setting.

3. Schedule the job.

Use one of the following methods.

Tip: During job scheduling, you can use the following shortcuts:

- Click the **Calender** icon to select a **Start date**. Selecting a date automatically fills the **Start date** field.
- Click the **Clock** icon to select a **Start time**. Selecting a time automatically fills the **Start time** field.

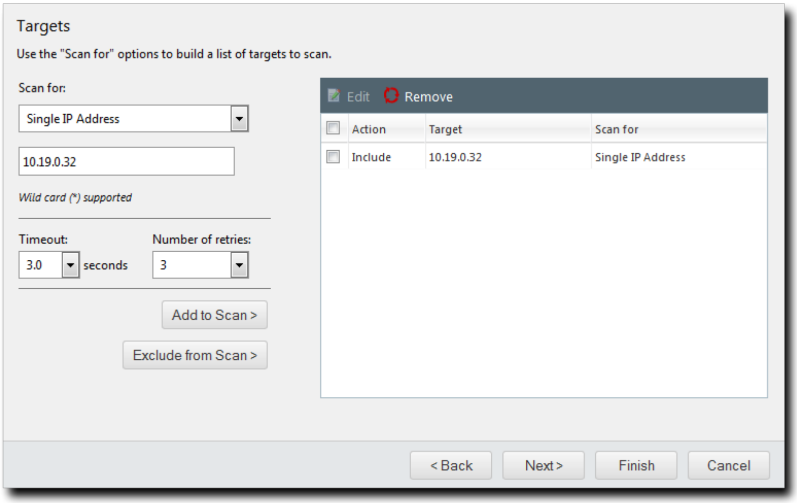
Method	Steps
To schedule an immediate job:	Select the **Immediate** option.

Method	Steps
To schedule a one-time job:	**1.** Ensure the **Once** option is selected. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **Tip:** Scheduling a one-time job for a past date and time will launch the job immediately.
To schedule a recurring weekly job:	**1.** Select the **Weekly** option. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **4.** Define the day of the week the job runs by selecting a day from the **Run every week on the following day** list.
To schedule a recurring monthly job:	**1.** Select the **Monthly** option. **2.** Define a start date by typing a date in the **Start date** field. **Note:** Type the date in a `mm/dd/yyyy` format. **3.** Define a start time by typing a time in the **Start time** field. **Note:** Type the time in `hh:mm` format followed by `AM` or `PM` (if necessary). This field supports both 12- and 24-hour time. **4.** Define the day of the month the job runs by typing a day in the **Run every month on the following day** field.

Tip: One-time and recurring jobs scheduled for the last day of a 31-day month are automatically rescheduled for the last day of shorter months.

4. Click **Next**.

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



Targets

Use the "Scan for" options to build a list of targets to scan.

Scan for: Single IP Address

10.19.0.32

Wild card (*) supported

Timeout: 3.0 seconds

Number of retries: 3

☐	Action	Target	Scan for
☐	Include	10.19.0.32	Single IP Address

Figure 38: Targets Page

5. Define targets (endpoints) for the job to locate.

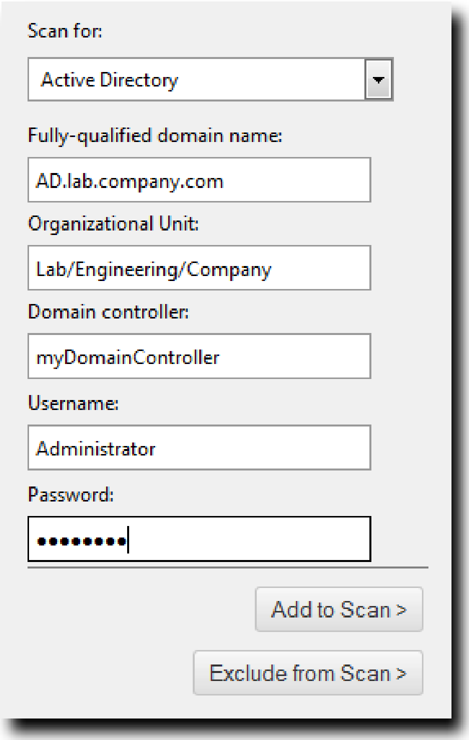
   Use one or more of the following discovery methods.

Method	Steps
To define targets using a single IP address:	1. From the **Scan for** list, select **Single IP Address**. 2. Type an IP address in the empty field. Wildcards are supported. **Note:** For additional information, refer to Defining Targets Using Wildcards on page 106. 3. Select an item in the **Timeout** list. **Note:** The Timeout list defines the number of seconds before a scan fails per attempt due to inactivity for a particular target. Under most network conditions, the Timeout field does not require editing. 4. Edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.

Method	Steps
To define targets using an IP range:	**1.** From the **Scan for** list, select **IP Range**. **2.** In the first empty field, type the beginning of IP range. **Note:** Wildcards are supported. For additional information, refer to Defining Targets Using Wildcards on page 106. **3.** In the second empty field, type the ending of the IP range. **4.** Select an item in the **Timeout** list. **Note:** The Timeout list defines the number of seconds per attempt before a scan fails due to inactivity for that particular target. Under most network conditions, the Timeout field does not require editing. **5.** If necessary, edit the **Number of retries** list. The **Number of retries** list defines the number of times a scan retries on that target if the scan times out.
To define targets using a computer name:	**1.** From the **Scan for** list, select **Computer name**. **2.** In the empty field, type an endpoint name in one of the following formats: `computername` or `domain\computername`.
To define targets using network neighborhood:	**1.** From the **Scan for** list, select **Network Neighborhood**. **2.** From the second list, select the desired network neighborhood.

Method	Steps
To define targets using active directory:	1. From the **Scan for** list, select **Active Directory**. 2. In the **Fully-qualified domain name** field, type the DNS domain name of the domain controller you want to scan. **Tip:** For example, if your domain controller DNS name is *box.domain.company.local*, you would type *domain.company.local* in this field. 3. Optionally, in the **Organizational Unit** field, type the active directory organizational unit string from specific to broad, separating each string with front slashes (such as `Techpubs/Engineering/Corporate`). **Tip:** The omission of this field returns job results containing the full contents of all the active directory organizational units. 4. In the **Domain controller** field, type the domain controller IP address. 5. In the **Username** field, type a user name that authenticates with the domain controller. **Note:** Type the user name in one of the following format: `domainname\username` or `username`. 6. In the **Password** field, type the password associated with the user name.

Method	Steps
To define targets using an imported file:	1. From the **Scan for** list, select **Import file**. 2. Click **Browse**. 3. Browse to the file you want to use for target discovery. **Note:** The following file types are supported: .txt and .csv. 4. Click **Open**. **Tip:** For additional information about how to define targets within an imported file, refer to Defining Targets Within an Imported File on page 358.



Scan for:

Active Directory

Fully-qualified domain name:

AD.lab.company.com

Organizational Unit:

Lab/Engineering/Company

Domain controller:

myDomainController

Username:

Administrator

Password:

••••••••

Figure 39: Active Directory Input Example

6. Add targets to the wizard list. This list indicates whether defined targets are included in or excluded from the job.

   Use one of the following methods.

   Note: You must include at least one target for **Next** to become available. You can also delete targets from the list by selecting the applicable check boxes and clicking **Remove**.

Method	Steps
To include defined targets in the job:	Click **Add to Scan**.
To exclude defined targets from the job:	Click **Exclude from Scan**.

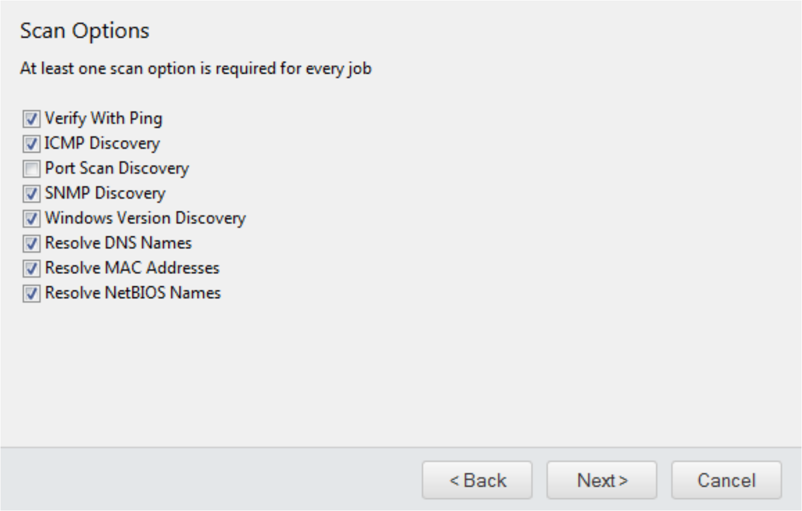
   Tip: Repeat this step to add additional targets to the list.

7. [Optional] Edit the **Targets** list.

   - To remove targets from the list, select the list item(s) and click **Remove**.
   - To edit targets on the list, select the list item(s) and click **Edit**. For additional information, refer to Editing Targets on page 103 .

8. Click **Next**.

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



Scan Options

At least one scan option is required for every job

☑ Verify With Ping
☑ ICMP Discovery
□ Port Scan Discovery
☑ SNMP Discovery
☑ Windows Version Discovery
☑ Resolve DNS Names
☑ Resolve MAC Addresses
☑ Resolve NetBIOS Names

Figure 40: Options Page

9. Select or clear the desired **Scan Options**.

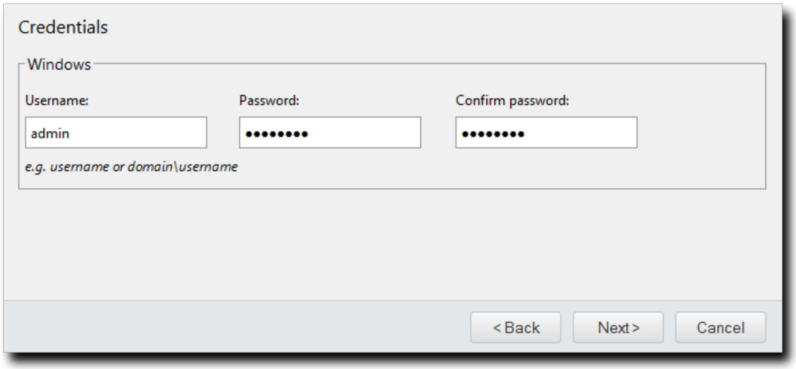
   The following table defines each **Scan Option**.

Option	Description
Verify With Ping	Jobs using this option send ping requests to all network endpoints targeted for discovery. Endpoints that respond to the request are flagged for scanning; unresponsive endpoints are skipped. Endpoints unresponsive to **Verify With Ping** are not scanned by other selected discovery options. **Note:** Anti-virus software and host firewalls may block **Verify With Ping**. If necessary, adjust any antivirus and firewall configurations to permit ping requests.
ICMP Discovery	Jobs using this option request a series of echoes, information, and address masks from endpoints. Endpoint responses are then compared to a list of known ICMP fingerprints to identify endpoint operating systems. **Note:** **ICMP Discovery** is ineffective on endpoints configured to ignore ICMP requests. For best results identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
Port Scan Discovery	Jobs using this option perform a limited scan on endpoint FTP, Telnet, SSH, SMTP, and HTTP ports. Based on the application banners found in these ports, endpoint operating systems are generically identified. **Note:** For best results in identifying Windows operating systems, use this option in conjunction with **Windows Version Discovery**.
SNMP Discovery	Jobs using this option request system properties for SNMP devices (routers, printers, and so on) from the management information base. Following credential authentication, SNMP devices are identified. **Note:** Without authenticated credentials, SNMP devices ignore **SNMP Discovery** requests. In this event, one of two outcomes occur: the SNMP device is misidentified as a UNIX endpoint or the SNMP device is not detected. Jobs with no SNMP credentials use the *public* credential by default.

Option	Description
Windows Version Discovery	Jobs using this option identify an endpoint's specific version of Windows following generic operating system identification during **ICMP** or **Port Scan Discovery**. **Note:** Correct operating system identification is contingent upon authenticated credentials. This option must be used in conjunction with either **ICMP** or **Port Scan Discovery**.
Resolve DNS Names	Jobs using this option acquire the endpoint DNS name through a local DNS server query. These names are displayed in job results for easy endpoint identification.
Resolve MAC Addresses	Jobs using this option acquire endpoint MAC addresses through endpoint queries. These addresses are displayed in job results for easy endpoint identification. **Note:** Monitor network inventory reports to prevent MAC address spoofing that may alter the **Resolve MAC Addresses** results.
Resolve NetBIOS Names	Jobs using this option acquire endpoint NetBIOS names through WINS NetBIOS mapping. These names are displayed in job results for easy endpoint identification.

10. Click **Next**.

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



Credentials

Windows

Username: admin

Password: ••••••••

Confirm password: ••••••••

e.g. username or domain\username

Figure 41: Credentials Page

11. Define **Windows** credentials for the target.

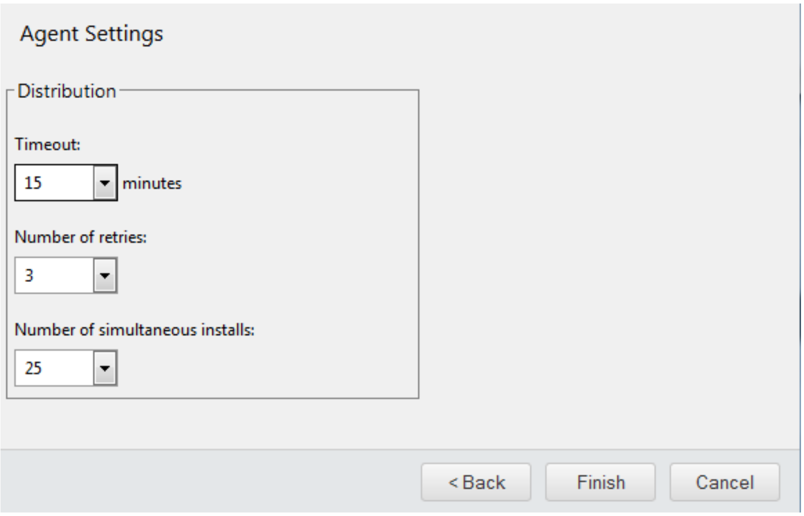
Type the applicable information in the following fields.

Note: When configuring an Agent Management Job, you must define valid Windows credentials.

Field	Description
Username	A user name that authenticates with Windows-based endpoints. Type the user name in a local format (*UserName*) or a domain format (*DOMAIN*\UserName). **Note:** When configuring Agent Management Jobs, Ivanti recommends using the built-in Administrator account.
Password	The password associated with the **Username**.
Confirm password	The **Password** retyped.

12. Click **Next**.

Step Result: The ***Agent Settings*** page opens.



Agent Settings

Distribution

Timeout: 15 minutes

Number of retries: 3

Number of simultaneous installs: 25

Figure 42: Agent Settings Page

13. Define the **Distribution** options.

The following table describes each list their available values.

List	Description
Timeout **(list)**	Defines the number of minutes before the Agent Management Job terminates an install attempt due to a non-responsive agent installation or removal (0-30).
Number of retries **(list)**	Defines the number of attempts an agent installation or removal will retry if the initial attempt fails (1-10).
Number of simultaneous installs **(list)**	Defines the maximum number of agents that can installed or removed simultaneously during the job (1-25). A value of `1` indicates that serial installs or removals should occur.

14. Click **Finish**.

Result: The ***Uninstall Agents Wizard*** closes. Depending on how you configured the job, it moves to either the ***Scheduled*** tab or ***Active*** tab on the ***Job Results*** page. The job will run at the applicable time, uninstalling agents on the defined targets, and move to the ***Completed*** tab when finished.

Chapter

8

Reviewing Jobs and Job Results

In this chapter:

Following the configuration of a Discovery Scan Job or Agent Management Job, they move to the ***Job Results*** page. This tabbed page organizes jobs based on status. You can view or edit job information for any Discovery Scan Job or Agent Management Job from this page.

This page is divided into the following tabs:

- The ***Scheduled*** tab
- The ***Active*** tab
- The ***Completed*** tab

Tip: Each tab features a list of jobs and you may click the job name to open detailed information about the job.

About Reviewing Jobs

The ***Job Results*** page lists all Discovery Scan Jobs and Agent Management Jobs. From this page, you can view jobs before, during, and after configuration activity.

Depending on how a job is scheduled during configuration, it will move to either the ***Scheduled*** tab or the ***Active*** tab. Jobs configured to run at a scheduled date and time move to the ***Scheduled*** tab. Jobs configured to run immediately move to the ***Active*** tab.

Any job on the ***Scheduled*** tab waits for its activation based on the scheduled date and time. Following activation, the job moves to the ***Active*** tab.

Note: Any jobs canceled when on the ***Scheduled*** tab move to the ***Completed*** tab with a `Cancelled` status. In addition, all recurring jobs remain listed on the ***Scheduled*** tab until they are canceled or deleted.

The jobs on the ***Active*** tab are performing their intended tasks:

1. The Discovery Scan Job detects and scans its defined targets.
2. The Agent Management Job scans and then performs the additional agent management tasks.

During activity, you can view partial job results. Job results update as the job progresses and page refreshes. After completion, all jobs move to the ***Completed*** tab.

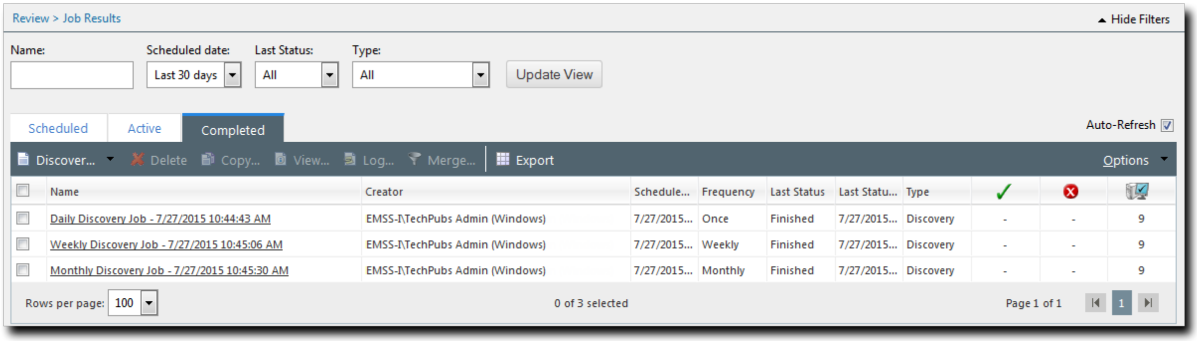
All jobs on the ***Completed*** tab have either been canceled or have finished activity. Once a job moves to the ***Completed*** tab, you can view job details. All jobs remain on the ***Completed*** tab until they are deleted.

The Job Results Page

The ***Job Results*** page is a tabbed page that organizes jobs based on status. Each tab features a list of jobs and a summary of their configurations. Links to each job's ***Job Results*** page are also available.

Tip: You can view the ***Job Results*** page from the navigation menu:

- Select **Review** > **Asset Discovery Job Results** to exclusively display Asset Discovery Job.
- Select **Review** > **Agent Management Job Results** to exclusively display Agent Management Job.



Name:
Scheduled date: Last 30 days
Last Status: All
Type: All

□	Name	Creator	Schedule...	Frequency	Last Status	Last Statu...	Type	✓	☒	
□	Daily Discovery Job - 7/27/2015 10:44:43 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015...	Once	Finished	7/27/2015...	Discovery	-	-	9
□	Weekly Discovery Job - 7/27/2015 10:45:06 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015...	Weekly	Finished	7/27/2015...	Discovery	-	-	9
□	Monthly Discovery Job - 7/27/2015 10:45:30 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015...	Monthly	Finished	7/27/2015...	Discovery	-	-	9

Rows per page: 100

0 of 3 selected

Page 1 of 1

Figure 43: Job Results Page

The ***Job Results*** page contains the following tabs:

- The Scheduled Tab on page 137
- The Active Tab on page 139
- The Completed Tab on page 142

Viewing the Job Results Page

Navigate to this page to view the configurations and results of Discovery Scan Jobs and Agent Management Jobs.

You can also use this page to create new jobs.

1. Based on the type of jobs you want to review, select an item from the navigation menu.
   Use one of the following methods to select jobs for review.

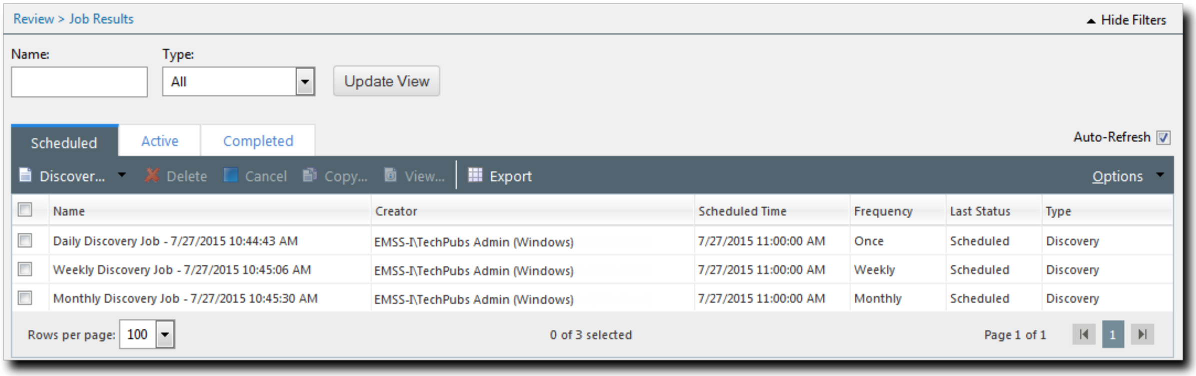
Method	Step
To review Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To review Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the ***Scheduled***, ***Active***, or ***Completed*** tab.
3. [Optional] Define filter criteria and click **Update View**.
4. [Optional] Complete a task listed in Working with Jobs on page 144.

Result: The ***Job Results*** page opens to the selected tab.

The Scheduled Tab

This tab lists all pending Asset Discovery Jobs and Agent Management Jobs. View this tab to see when scheduled jobs will become active.



Review > Job Results

Name:

Type: All

Auto-Refresh ☑

□	Name	Creator	Scheduled Time	Frequency	Last Status	Type
□	Daily Discovery Job - 7/27/2015 10:44:43 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015 11:00:00 AM	Once	Scheduled	Discovery
□	Weekly Discovery Job - 7/27/2015 10:45:06 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015 11:00:00 AM	Weekly	Scheduled	Discovery
□	Monthly Discovery Job - 7/27/2015 10:45:30 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015 11:00:00 AM	Monthly	Scheduled	Discovery

Rows per page: 100

0 of 3 selected

Page 1 of 1

Figure 44: Scheduled Tab

Pending jobs move to the ***Active*** tab at their scheduled dates and times. Additionally, recurring jobs remain listed on this ***Scheduled*** tab until they are canceled or deleted.

The Scheduled Tab Toolbar

This toolbar contains buttons related to the creation, viewing, and management of Discovery Scan Jobs and Agent Management Jobs.

Some functions on the ***Scheduled*** tab toolbar are common to all ***Job Results*** page tabs.

Table 49: Scheduled Tab Toolbar

Button	Function
Discover... (menu)	Opens the **Discover...** menu.
Assets... (**Discover ...** menu item)	Creates a custom Discovery Scan Job. For additional information, refer to Discovering Assets by Discovery Scan Job on page 91.
Assets and Install Agents... (**Discover...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 109.
Assets and Uninstall Agents... (**Discover...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.
Delete	Deletes the selected job from the list. For additional information, refer to Deleting Jobs on page 147.
Cancel	Cancels the selected job. For additional information, refer to Canceling Jobs on page 148.
Copy...	Duplicates the selected job. For additional information, refer to Copying Jobs on page 145.
View...	Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to Viewing Job Configurations on page 146.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Button	Function
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Scheduled Tab List

This list contains configuration overviews of scheduled jobs. The number of items in the list depends on how many jobs are pending.

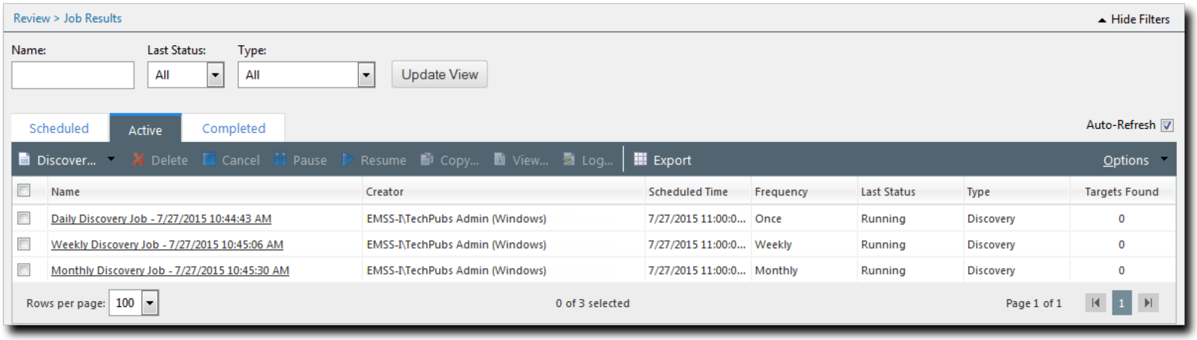
The following table describes each column in the ***Scheduled*** tab list.

Table 50: Scheduled Tab List

Column	Description
Name	The job name.
Creator	The user account used to create the job.
Scheduled Time	The scheduled date and time for the job.
Frequency	The schedule type the job uses (`Once`, `Weekly`, `Monthly`).
Last Status	The last known status of a job.
Type	The job type (`Discovery` or `Agent Management`).

The Active Tab

This tab lists Discovery Scan Jobs and Agent Management Jobs that are in progress. View this tab to see job results in real time.



Name:

Last Status: All

Type: All

Auto-Refresh ☑

□	Name	Creator	Scheduled Time	Frequency	Last Status	Type	Targets Found
□	Daily Discovery Job - 7/27/2015 10:44:43 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015 11:00:0...	Once	Running	Discovery	0
□	Weekly Discovery Job - 7/27/2015 10:45:06 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015 11:00:0...	Weekly	Running	Discovery	0
□	Monthly Discovery Job - 7/27/2015 10:45:30 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015 11:00:0...	Monthly	Running	Discovery	0

Rows per page: 100

0 of 3 selected

Page 1 of 1

Figure 45: Active Tab

The ***Active*** tab also lists active job configuration overviews. Click a job name link to view partial results during job progress. Following completion, active jobs move to the ***Completed*** tab.

The Active Tab Toolbar

This toolbar contains buttons related to the creation, viewing, and management of Discovery Scan Jobs and Agent Management Jobs.

Some functions on the ***Active*** tab toolbar are common to all ***Job Results*** page tabs.

Table 51: Active Tab Toolbar

Name	Function
Discover... (menu)	Opens the **Discover...** menu.
Assets... (**Discover ...** menu item)	Creates a custom Discovery Scan Job. For additional information, refer to Discovering Assets by Discovery Scan Job on page 91.
Assets and Install Agents... (**Discover...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 109.
Assets and Uninstall Agents... (**Discover...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.
Delete	Deletes the selected job from the list. For additional information, refer to Deleting Jobs on page 147.
Cancel	Cancels the selected job. For additional information, refer to Canceling Jobs on page 148.
Pause	Pauses the selected job. For additional information, refer to Pausing Jobs on page 151.
Resume	Continues the selected paused job. For additional information, refer to Resuming a Paused Job on page 151.
Copy...	Duplicates the selected job. For additional information, refer to Copying Jobs on page 145.
View...	Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to Viewing Job Configurations on page 146.
Log...	Opens the log for the selected job. For additional information, refer to Viewing a Job Log on page 149.

Name	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Active Tab List

This list contains configuration overviews of active jobs. The number of items in the list depends on how many jobs are active.

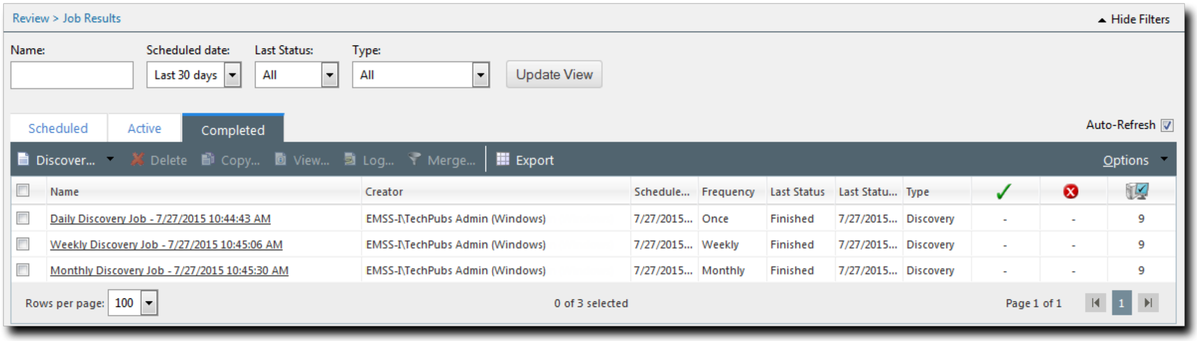
The following table describes each list column.

Table 52: Active Tab List

Column	Description
Name	The job name. The name is a link to the job's ***Results*** page.
Creator	The user account used to create the job.
Scheduled Time	The scheduled date and time for the job.
Frequency	The schedule type the job uses (`Once`, `Weekly`, `Monthly`).
Last Status	The last known status of a job.
Type	The job type (`Discovery` or `Agent Management`).
Targets Found	The number of assets discovered during job activity.

The Completed Tab

This tab lists Discovery Scan Jobs and Agent Management Jobs that are completed or canceled, as well as their configuration details.



Name:
Scheduled date: Last 30 days
Last Status: All
Type: All

□	Name	Creator	Schedule...	Frequency	Last Status	Last Statu...	Type	✓	✗	
□	Daily Discovery Job - 7/27/2015 10:44:43 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015...	Once	Finished	7/27/2015...	Discovery	-	-	9
□	Weekly Discovery Job - 7/27/2015 10:45:06 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015...	Weekly	Finished	7/27/2015...	Discovery	-	-	9
□	Monthly Discovery Job - 7/27/2015 10:45:30 AM	EMSS-I\TechPubs Admin (Windows)	7/27/2015...	Monthly	Finished	7/27/2015...	Discovery	-	-	9

Rows per page: 100 0 of 3 selected Page 1 of 1 1

Figure 46: Completed Tab

Completed and canceled jobs remain on this page until you delete them. Additionally, the job name links associated with each completed job take you to that job's ***Results*** page.

The Completed Tab Toolbar

This toolbar contains buttons related to the creation, viewing, and management of Discovery Scan Jobs and Agent Management Jobs.

Some functions on the ***Completed*** tab toolbar are common to all ***Job Results*** page tabs.

Table 53: Completed Tab Toolbar

Button	Function
Discover... (menu)	Opens the **Discover...** menu.
Assets... (**Discover ...** menu item)	Creates a custom Discovery Scan Job. For additional information, refer to Discovering Assets by Discovery Scan Job on page 91.
Assets and Install Agents... (**Discover...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 109.
Assets and Uninstall Agents... (**Discover...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.
Delete	Deletes the selected job from the list. For additional information, refer to Deleting Jobs on page 147.

Button	Function
Copy...	Duplicates the selected job. For additional information, refer to Copying Jobs on page 145.
View...	Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to Viewing Job Configurations on page 146.
Log...	Opens the log for the selected job. For additional information, refer to Viewing a Job Log on page 149.
Merge	Merges two jobs in to one. For additional information, refer to Merging Jobs on page 152.
Export	Exports the page data to a comma-separated value (.csv) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Completed Tab List

This list contains configuration overviews of finished and canceled jobs. The number of items in the list depends on how many jobs are finished and canceled.

The following table describes each list column.

Table 54: Completed Tab Table

Column	Icon	Description
Name		The job name. The name is a link to the job's ***Results*** page.
Creator		The user account used to create the job.
Scheduled Time		The scheduled date and time for the job.
Frequency		The schedule type the job uses (Once, Weekly, Monthly).
Last Status		The last known status of a job.
Last Status Time		The date and time of the last status update.

Column	Icon	Description
Type		The job type (`Discovery` or `Agent Management`).
Total Successful	✓	The total number of agents successfully managed (Agent Management Jobs only).
Total Failed	❌	The total number of agents that failed to install or uninstall (Agent Management Jobs only).
Total Complete	🖥	The total number or assets discovered during the scan.

Working with Jobs

You can perform a number of tasks related to Discovery Scan Jobs and Agent Management Jobs from the ***Job Results*** page. You can perform most of these tasks regardless of the tab selected. However, certain tasks are specific to certain tabs.

To perform tasks associated with jobs, click a toolbar button. Some buttons are unavailable until one or multiple jobs are selected from the page list.

The following list displays the task that you can perform from the ***Job Results*** page.

- Discovering Assets on page 144
- Installing Agents by Agent Management Job on page 145
- Uninstalling Agents by Agent Management Job on page 145
- Copying Jobs on page 145
- Viewing Job Configurations on page 146
- Deleting Jobs on page 147
- Exporting Job Result Data on page 148
- Canceling Jobs on page 148
- Viewing a Job Log on page 149
- Viewing Job Results on page 150
- Pausing Jobs on page 151
- Resuming a Paused Job on page 151
- Merging Jobs on page 152

Discovering Assets

Discover Assets jobs are Discovery Scan Jobs that let you customize scheduling, discovery methods, and discovery options.

To schedule a discover assets job from any tab on the ***Job Results*** page, select **Discover** > **Assets** from the toolbar.

For additional information, refer to Discovering Assets by Discovery Scan Job on page 91.

Installing Agents by Agent Management Job

Within Ivanti Endpoint Security, there are various pages in which you can install agents on endpoints using an Agent Management Job. To create an Agent Management Job on the ***Job Results*** page, select **Discover** > **Assets and Install Agents** from the toolbar.

For additional information, refer to Installing Agents by Agent Management Job on page 109.

Uninstalling Agents by Agent Management Job

Within Ivanti Endpoint Security, there are various pages in which you can uninstall agents on endpoints using an Agent Management Job. To create an Agent Management Job that uninstalls agents from the ***Job Results*** page, select **Discover** > **Assets and Uninstall Agents** from the toolbar. You can perform this task from any tab.

For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.

Copying Jobs

On occasion, you may want to create a job (Discovery Scan Job or Agent Management Job) that is identical to a preexisting completed job. Rather than creating a new job and recreating its configuration, you can copy that preexisting job with the desired configuration values already in place.

Copy jobs from any tab on the **Job Results** page.

1. Based on the type of job you want to copy, select an item from the navigation menu.

   Use one of the following methods to select jobs for copying.

Method	Step
To copy Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To copy Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the tab that lists the job you want to copy:
   - **Scheduled**
   - **Active**
   - **Completed**
3. Select the job you want to copy.

   Step Result: The **Copy** button becomes active.

   > **Tip:** When the **Name** check box is selected, all items become checked. However, you may only copy one item at a time.

4. Click **Copy**.

   Step Result: Depending on which job you selected, one of the following dialogs opens:

   - ***Copy Discover Assets Job***
   - ***Copy Install Agents Job***
   - ***Copy Uninstall Agents Job***

   The copied job is configured identically to the selected job.

5. If copying an Agent Management Job, dismiss the security credential acknowledgement by clicking **OK**.
6. [Optional] Edit the job configuration.

   If the job you are copying requires credentials (for either agent management or credential validation), you will have to re-enter the credentials for security purposes.

   > **Note:** When editing the ***Copy Discover Assets Wizard***, you can select or clear the **Use existing credential set** check box, which is available on the ***Credentials*** page. This option, which is unavailable during regular discover assets job configuration, lets you retain or discard the credential set entered during source job configuration. If you discard the credential set, you can enter a new credentials set or use no credentials.

7. Click **Save**.

Result: The copied job is saved and moved to the applicable ***Job Results*** page tab.

Viewing Job Configurations

Ivanti Endpoint Security can display a job's configuration details in a read-only dialog. View this dialog when you want to see a job's configuration without changing it.

View job configurations from any tab on the ***Job Results*** page.

1. Based on the type of job you want to view, select an item from the navigation menu.

   Use one of the following methods to select jobs for viewing.

Method	Step
To view Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To view Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the tab that lists the job configuration you want to view:

   - **Scheduled**
   - **Active**
   - **Completed**

3. Select the job you want to view.

   Step Result: The **View** button becomes active.

   > **Tip:** When the **Name** check box is selected, all items become checked. However, you may only view one item at a time.

4. Click **View**.

Result: Depending on the type of job you are viewing, one of the following dialogs opens in a read-only format:

- ***View Discover Assets Job***
- ***View Install Agents Job***
- ***View Uninstall Agents Job***

Use the dialog buttons to scroll through wizard pages.

Deleting Jobs

When a Discovery Scan Job or an Agent Management Job is no longer necessary, delete that job to completely remove its record from Ivanti Endpoint Security. Deleting jobs differs from canceling jobs. Deleted jobs are removed from the ***Job Results*** page altogether; canceled jobs are moved to the ***Completed*** tab.

Delete jobs from any tab on the ***Job Results*** page.

1. Based on the type of job you want to delete, select an item from the navigation menu.

   Use one of the following methods to select jobs for deleting.

Method	Step
To delete Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To delete Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the tab that lists the job you want to delete.

   - **Scheduled**
   - **Active**
   - **Completed**

3. Select the job(s) you want to delete.

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

   > **Tip:** When the **Name** check box is selected, all items become checked in the list and the **Delete** button becomes active.

4. Click **Delete**.

   Step Result: A dialog appears, asking you acknowledge the deletion.

5. Acknowledge the deletion by clicking **OK**.

Result: The job is deleted from the list.

Exporting Job Result Data

To export the list of Discovery Scan Jobs and Agent Management Jobs that are listed on any ***Job Results*** page tab to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 39.

Canceling Jobs

Cancel a Discovery Scan Job or an Agent Management Job that you do not want to complete but still want to keep a record of. Canceling jobs differs from deleting jobs. Canceled jobs move to the ***Completed*** tab; deleted jobs are removed from the ***Job Results*** page altogether. You can cancel jobs with a status of scheduled, paused, or running.

Cancel jobs from the ***Scheduled*** and ***Active*** tabs.

1. Based on the type of job you want to cancel, select an item from the navigation menu.

   Use one of the following methods to select jobs for canceling.

Method	Step
To cancel Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To cancel Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the tab that lists the job(s) you want to cancel:
   - The ***Scheduled*** tab
   - The ***Active*** tab

3. Select the job(s) you want to cancel.

   Step Result: The **Cancel** button becomes active.

   > **Tip:** When the **Name** check box is selected, all items become checked within the list and the **Cancel** button becomes active.

4. Click **Cancel**.

5. Click **OK** to confirm the cancellation.

Result: The selected job is canceled and moved to the ***Completed*** tab.

Viewing a Job Log

During activity, jobs record any substantial events or errors that occur. These logs are helpful when troubleshooting network, server, or agent issues. Not all jobs record logs.

View job logs from the ***Active*** or ***Completed*** tabs. Active job logs may not be complete because scanning or agent installation is not finished.

1. Based on the type of job log you want to view, select an item from the navigation menu.

   Use one of the following methods to select job logs for viewing.

Method	Step
To view Discovery Scan Job job logs:	Select **Review** > **Asset Discovery Job Results**.
To view Agent Management Job logs:	Select **Review** > **Agent Management Job Results**.

2. Select the tab that lists the job containing the log you want to view:
   - the ***Active*** tab
   - the ***Completed*** tab
3. Select the job containing the log you want to view.

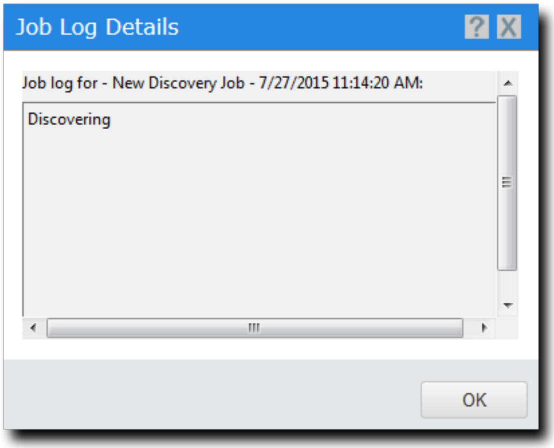
   Step Result: If a log is available, the **Log** button becomes active.

   > **Tip:** When the **Name** check box is selected, all items become checked. However, you may only view one log item at a time if it is available.

4. Click **Log**.

> **Note:** If more than one job is selected, or if the selected job does not have a log, then **Log** is unavailable.

Result: The ***Job Log Details*** dialog opens.



Job log for - New Discovery Job - 7/27/2015 11:14:20 AM:

Discovering

Figure 47: Job Log Details Dialog

Viewing Job Results

You can see the results for a job after it completes or while it runs. However, viewing the results for an active job will display only partially completed results. View results by clicking job name links, which open the applicable job's ***Results*** page.

Access job results from the ***Active*** and ***Completed*** tabs.

1. Based on the type of job results you want to view, select an item from the navigation menu.

   Use one of the following methods to select job results for viewing.

Method	Step
To view results for Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To view results for Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the tab that lists the job for which you want to view results:

   - **Active**
   - **Completed**

3. Click the job name link for the job results you want to view.

> **Note:** Scheduled jobs have no job name links.

Result: The ***Results*** page for the job you selected opens. The ***Results*** page for active jobs is partially complete because the job is still active. More job information appears as you refresh the page.

Pausing Jobs

While Discovery Scan Jobs or Agent Management Jobs are active, they can be temporarily paused. Only active jobs can be paused.

Pause jobs from the ***Active*** tab.

1. Based on the type of job you want to pause, select an item from the navigation menu.

   Use one of the following methods to select jobs for pausing.

Method	Step
To pause Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To pause Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the ***Active*** tab.
3. Select the job(s) you want to pause.

   Step Result: The **Pause** button becomes active.

   > **Tip:** When the **Name** check box is selected, all items become checked in the list and the **Pause** button becomes active.

4. Click **Pause**.

Result: The selected job is paused.

Resuming a Paused Job

Resume paused jobs to continue their activity. Only paused jobs can be resumed.

Prerequisites:

A pause job is present in the ***Active*** tab.

Resume paused jobs from the ***Active*** tab.

1. Based on the type of job you want to resume, select an item from the navigation menu.
   Use one of the following methods to select jobs for resuming.

Method	Step
To resume Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To resume Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

2. Select the ***Active*** tab.
3. Select the paused job(s) you want to resume.

   Step Result:

   Tip: The **Resume** button becomes active. When the **Name** check box is selected, all items become checked in the list and the **Pause** button becomes active.

4. Click **Resume**.

Result: The selected job resumes activity.

Merging Jobs

Merging completed jobs lets you view the results for two different jobs on one page. This feature is convenient for when you want to review multiple jobs' results without having to navigate between jobs.

You can only merge completed jobs that have a status of `Finished`. Merge completed jobs from the ***Completed*** tab. You can merge an unlimited number of completed jobs.

Note: Agent Management Jobs that install agents and Agent Management Jobs that uninstall agents cannot be merged.

1. Based on the type of jobs you want to merge, select an item from the navigation menu.
   Use one of the following methods to select jobs for merging.

Method	Step
To merge Discovery Scan Jobs:	Select **Review** > **Asset Discovery Job Results**.
To merge Agent Management Jobs:	Select **Review** > **Agent Management Job Results**.

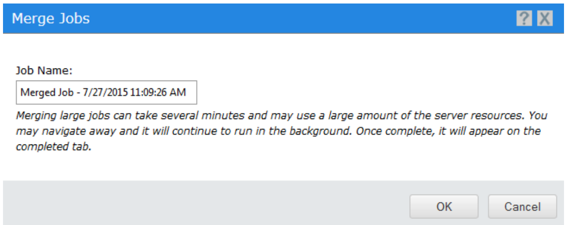
2. Select the ***Completed*** tab.

3. Select the job(s) you want to merge.

> **Note:** More than one job must be selected to merge jobs. When the **Name** check box is selected, all items become checked in the list and the **Merge** button becomes active.

4. Click **Merge**.

   Step Result: The ***Merge Jobs*** dialog opens.



Merge Jobs

Job Name:

Merged Job - 7/27/2015 11:09:26 AM

Merging large jobs can take several minutes and may use a large amount of the server resources. You may navigate away and it will continue to run in the background. Once complete, it will appear on the completed tab.

Figure 48: Merge Jobs Dialog

5. [Optional] Type a new name for the job in the **Job Name** field.

> **Note:** By default, new merged jobs are named `Merged Job`, followed by the server-side date and time, formatted according to the server's locale setting.

6. Click **OK**.

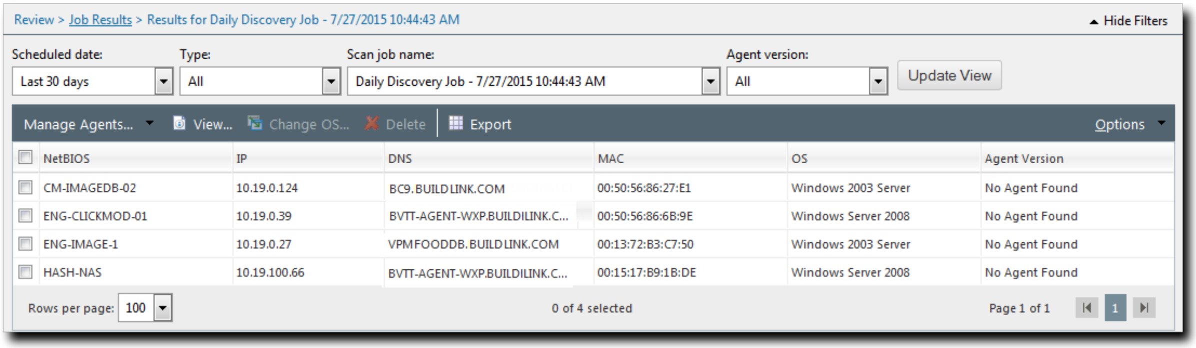
Result: The merged job appears in the list.

The Results Page

This page lists the results for a selected Discovery Scan Job or Agent Management Job. It lists each endpoint found during scanning, the endpoints' operating systems, and their address information. When the viewed ***Results*** page is associated with an Agent Management Job, additional information about agent information is displayed. Use this page to determine candidates for agent installation or to verify that an Agent Management Job ran smoothly.

You can access a job's ***Results*** page by clicking the links listed on the ***Job Results*** page ***Active*** and ***Completed*** tabs.

Note: If you access a ***Results*** page while a job is still active, the results will be incomplete.



Review > Job Results > Results for Daily Discovery Job - 7/27/2015 10:44:43 AM

Scheduled date: Last 30 days

Type: All

Scan job name: Daily Discovery Job - 7/27/2015 10:44:43 AM

Agent version: All

□	NetBIOS	IP	DNS	MAC	OS	Agent Version
□	CM-IMAGEDB-02	10.19.0.124	BC9.BUILDLINK.COM	00:50:56:86:27:E1	Windows 2003 Server	No Agent Found
□	ENG-CLICKMOD-01	10.19.0.39	BVTT-AGENT-WXP.BUILDILINK.C...	00:50:56:86:6B:9E	Windows Server 2008	No Agent Found
□	ENG-IMAGE-1	10.19.0.27	VPMFOODDB.BUILDLINK.COM	00:13:72:B3:C7:50	Windows 2003 Server	No Agent Found
□	HASH-NAS	10.19.100.66	BVTT-AGENT-WXP.BUILDILINK.C...	00:15:17:B9:1B:DE	Windows Server 2008	No Agent Found

Rows per page: 100

0 of 4 selected

Page 1 of 1

Figure 49: Results Page

Note: The ***Results*** page *is not* the ***Job Results*** page. The ***Results*** page contains endpoint details, while the ***Job Results*** page contains job configuration details. For additional information about the ***Job Results*** page, refer to The Job Results Page on page 136.

Viewing the Results Page

After running a Discovery Scan Job or Agent Management Job, you can view detailed results for individual jobs.

View the ***Results*** page by clicking a job link from the ***Job Result***s page.

1. Depending on the job results you want to view, select one of the following menu items:

- **Review** > **Asset Discovery Job Results**
- **Review** > **Agent Management Job Results**

2. Select the tab containing the job you want to review results for.

- The ***Active*** tab
- The ***Completed*** tab

3. Click the job link for the results you want to review.

Result: The ***Results*** page for the selected job opens.

The Results Page Toolbar

This toolbar contains buttons for features related to job results for endpoints.

The following table describes ***Results*** page toolbar button functions.

Table 55: Results Page Toolbar

Button	Function
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 109.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 173.
View...	Displays the configuration of the selected job. This dialog is read-only. For additional information, refer to Viewing Job Configurations on page 146.
Change OS	Changes the operating system result for the selected endpoint. For additional information, refer to Changing Endpoint Operating System Results on page 159.
Delete	Deletes the selected endpoint result from the list. For additional information, refer to Deleting Job Endpoint Results on page 160.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

Button	Function
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Results Page List

This list itemizes all endpoints discovered during the selected job. It also displays endpoint agent, address, and operating system information. Endpoints with agents installed offer links to their ***Details*** page.

The following table displays the information found on the ***Results*** page list.

Table 56: Results Page List

Column	Description
Access Level	The access level that the credentials entered during job configuration achieved on the endpoint (`None`, `Read`, `Full`, `Agent Installed`). For addition information refer to Access Levels on page 157. **Note:** This column only appears for Agent Management Jobs or Discovery Scan Jobs that had the **Validate credential access level** option selected.
NetBIOS	The NetBIOS name of the endpoint. The name serves as a link to the ***Details*** page for endpoints that have agents installed.
IP	The IP address of the endpoint.
DNS	The DNS name of the endpoint.
MAC	The MAC address of the endpoint.
OS	The operating system of the endpoint.
Install Status	The status of an agent installation. **Note:** This column only appears if the ***Results*** page pertains to an Agent Management Job or a merged job containing an Agent Management Job.
Status Message	The explanation of the **Install Status**. **Note:** This column only appears if the ***Results*** page pertains to an Agent Management Job or a merged job containing an Agent Management Job.

Column	Description
Agent Version	The agent version installed on the endpoint. A `No Agent Found` value indicates either no agent is present or the agent could not be detected.

Note: Endpoint results are collected during job activity. Therefore, older jobs may contain obsolete information. Additionally, if Agent Management Jobs are failing, their target endpoints may not be properly configured. For additional information of configuring endpoints for Agent Management Jobs, refer to Configuring Endpoints for Agent Management Jobs on page 380

Access Levels

The ***Results*** page also displays the **Access Level** column for agent management jobs and discovery jobs that have had the **Validate credential access level** option selected. This column displays the access levels that job credentials permit for job targets. Access levels provide feedback as to whether credentials entered during job configuration can provide agent management permission.

The following table describes each access level.

Table 57: Access Levels

Access Level	Description
`None`	Indicates the endpoint was discovered, but the credentials entered during job configuration are invalid on the applicable endpoint.
`Read`	Indicates the credentials entered during job configuration provide read access to the applicable endpoint's share drives. These credentials provide the access rights needed to run Agent Management Jobs.
`Full`	Indicates the credentials entered during job configuration have read and write access to the applicable endpoint's share drives. These credentials provide the access rights needed to run Agent Management Jobs.
`Agent Installed`	Indicates that the endpoint has an agent installed.

Working with Results

To perform tasks associated with job results, click a toolbar button. To perform some tasks, selecting one or multiple jobs from the ***Results*** page may be necessary.

- Viewing Endpoint Details on page 158
- Installing Agents by Agent Management Job on page 158
- Uninstalling Agents by Agent Management Job on page 159
- Downloading the Agent Installer on page 159
- Changing Endpoint Operating System Results on page 159
- Deleting Job Endpoint Results on page 160
- Exporting Discovery Scan Result Data on page 161

Viewing Endpoint Details

The ***Results*** page features links to the ***Details*** page for endpoints that have agents installed. View endpoint ***Details*** pages when you want to view agent-collected data about an endpoint. Links are not available for endpoints without agents installed.

You can also access endpoint details from the ***Endpoints*** page.

1. Depending on the job results you want to view, select one of the following menu items:
   - **Review** > **Asset Discovery Job Results**
   - **Review** > **Agent Management Job Results**
2. Ensure the **Active** or the ***Completed*** tab is selected.
3. Click the desired job name link.

   Step Result: The ***Results*** page for the selected job opens.
4. Click the desired NetBIOS link.

   Note: NetBIOS links are only available for endpoints with agents installed.

Result: The ***Details*** page for the selected endpoint opens.

Installing Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of installing agents on endpoints using agent management jobs. To create an Agent Management Job that installs agents from the ***Results*** page, select **Manage Agents** > **Install Agents** from the toolbar.

For additional information, refer to Installing Agents by Agent Management Job on page 109.

Uninstalling Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of uninstalling agents from endpoints using an Agent Management Job. To create an Agent Management Job that uninstalls agents from the ***Results*** page, select **Manage Agents** > **Uninstall Agents** from the toolbar.

For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.

Downloading the Agent Installer

From the ***Results*** page, you can download an agent installer to the endpoint that you are using.

To download an agent installer from the ***Results*** page, select **Manage Agents** > **Download Agent Installer** from the toolbar. For additional information, refer to Downloading the Agent Installer on page 173.

Changing Endpoint Operating System Results

When a job does not have the scan options selected necessary to identify an endpoint's operating system, Ivanti Endpoint Security identifies the endpoint's operating system as generic or unknown. When this event occurs, you can correct an endpoint's operating system scan result manually.

Change the operating system result of an endpoint from the ***Results*** page.

1. Select one of the following items from the navigation menu.
   - **Review** > **Asset Discovery Job Results**
   - **Review** > **Agent Management Job Results**

   These menu items filter the ***Job Results*** page for the selected job type.
2. Ensure the ***Completed*** tab is selected.
3. Click the desired job name link.

   Step Result: The ***Results*** page for the selected job opens.
4. Select the operating system result(s) you want to change.

5. Click **Change OS**.

   Step Result: The ***Change OS*** dialog opens.

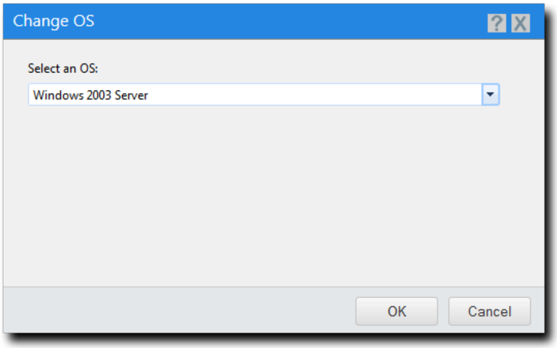


Figure 50: Change OS Dialog

6. Select the desired operating system from the list.
7. Click **OK**.

Result: The selected operating system result is changed.

Deleting Job Endpoint Results

While viewing results for a selected Discovery Scan Job or Agent Management Job, you can delete the entry for any endpoint scanned during the job. Delete entries when you no longer need them; for example, when an endpoint is removed from the network.

Delete endpoint entries from a job's ***Results*** page.

1. Select one of the following items from the navigation menu.
   - **Review** > **Asset Discovery Job Results**
   - **Review** > **Agent Management Job Results**

   These menu items filter the ***Job Results*** page for the selected job type.
2. Select the ***Completed*** tab.
3. Click a job name link.

   Step Result: The job’s ***Results*** page opens.
4. Select the check box(es) associated with the results you want to delete.
5. Click **Delete**.

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

Result: The selected discovery scan results are deleted from the list.

Exporting Discovery Scan Result Data

To export the list of endpoints that are listed on the ***Results*** page to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analysis purposes.

For additional information, refer to Exporting Data on page 39.

Chapter 9

Using Endpoints

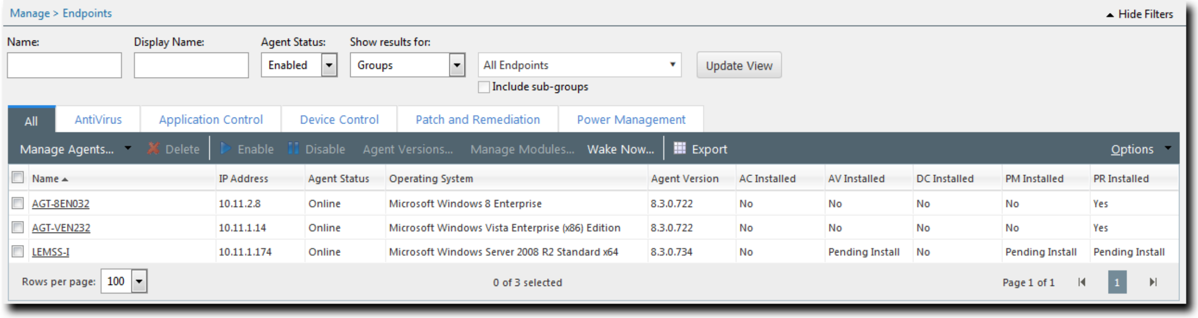
In this chapter:

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

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

About Endpoints

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



Name:

Display Name:

Agent Status: Enabled

Show results for: Groups

All Endpoints

□ Include sub-groups

□	Name ▲	IP Address	Agent Status	Operating System	Agent Version	AC Installed	AV Installed	DC Installed	PM Installed	PR Installed
□	AGT-8EN032	10.11.2.8	Online	Microsoft Windows 8 Enterprise	8.3.0.722	No	No	No	No	Yes
□	AGT-VEN232	10.11.1.14	Online	Microsoft Windows Vista Enterprise (x86) Edition	8.3.0.722	No	No	No	No	Yes
□	LEMSS-I	10.11.1.174	Online	Microsoft Windows Server 2008 R2 Standard x64	8.3.0.734	No	Pending Install	No	Pending Install	Pending Install

Rows per page: 100

0 of 3 selected

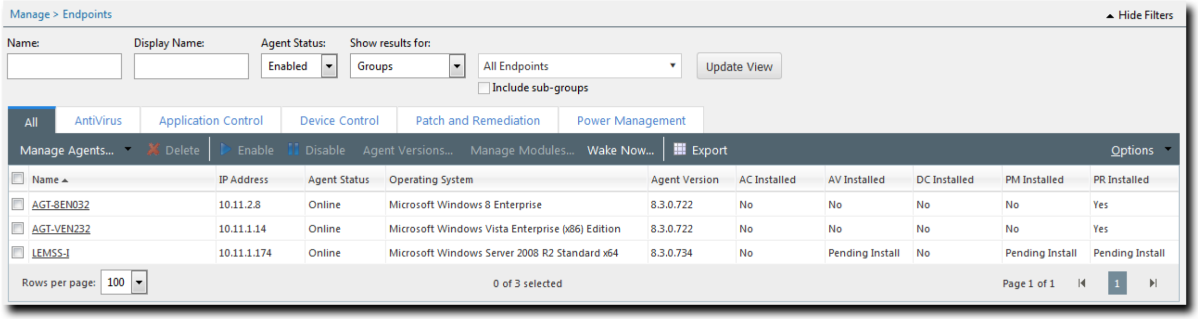
Page 1 of 1

Figure 51: Endpoints Page

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

The Endpoints Page

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



Name:

Display Name:

Agent Status: Enabled

Show results for: Groups — All Endpoints

☐ Include sub-groups

☐	Name	IP Address	Agent Status	Operating System	Agent Version	AC Installed	AV Installed	DC Installed	PM Installed	PR Installed
☐	AGT-8EN032	10.11.2.8	Online	Microsoft Windows 8 Enterprise	8.3.0.722	No	No	No	No	Yes
☐	AGT-VEN232	10.11.1.14	Online	Microsoft Windows Vista Enterprise (x86) Edition	8.3.0.722	No	No	No	No	Yes
☐	LEMSS-I	10.11.1.174	Online	Microsoft Windows Server 2008 R2 Standard x64	8.3.0.734	No	Pending Install	No	Pending Install	Pending Install

Rows per page: 100

0 of 3 selected

Page 1 of 1

Figure 52: Endpoints Page

The All Tab Toolbar

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

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

Table 58: All Tab Toolbar Functions

Button	Function
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Install agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 109.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 173.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 174.

Button	Function
Enable	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 175. **Note:** This button is only available when an endpoint is disabled.
Disable	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 176.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 173.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Installing Endpoint Modules on page 177.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The All Tab List

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

The following table describes the columns within the ***All*** tab list and the comma separated value (`.csv`) file you can export from it (refer to Exporting Data on page 39).

Table 59: All Tab List Columns

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

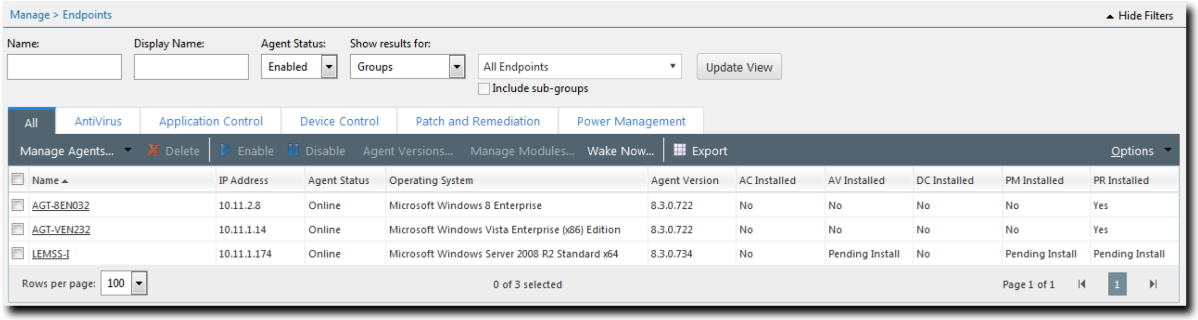
<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td><b>Agent Status</b></td><td>The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:
<table>
<tr><td><b>Online</b></td><td>The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 60 for more information on configuring default agent behavior.</td></tr>
<tr><td><b>Offline</b></td><td>The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an <code>Offline</code> status, the agent still enforces all policies.
<b>Note:</b> A <b>Warning</b> (⚠) icon next to an <code>Offline</code> status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.</td></tr>
<tr><td><b>Disabled</b></td><td>The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.</td></tr>
</table></td></tr>
<tr><td><b>Last Connected Date (Server)</b></td><td>Exported comma separated value (<code>.csv</code>) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.</td></tr>
</table>

Column	Description	
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values:	
	Started	EDS server has started and is in an operational state accepting workloads.
	Starting	EDS server is in the process of starting its service.
	Stopped	EDS server has stopped and is not accepting workloads.
	Stopping	EDS server is in the process of stopping so as to not accept workloads.
	Offline	EDS server is offline as it has not contacted the database in the configured amount of time.
Operating System	The operating system that the endpoint uses.	
Agent Version	The version of the Ivanti Endpoint Security Agent installed. **Note:** A ⚙ icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.	
***Module* Installed**	Indicates whether a module is installed on the endpoint. A new ***Module* Installed** column is added for each module installed on your Ivanti Endpoint Security Server. The following list defines column entry values:	
	Yes	The module is installed.
	No	The module is not installed.
	Pending Install	The module is in the process of installing.
	Pending Uninstall	The module is in the process of uninstalling.
	Error	There was an error while installing or uninstalling the module. Click the for additional information about the error.
	Expired	The module license has expired.

The All Tab

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

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



Name:

Display Name:

Agent Status: Enabled

Show results for: Groups

All Endpoints

□ Include sub-groups

□	Name	IP Address	Agent Status	Operating System	Agent Version	AC Installed	AV Installed	DC Installed	PM Installed	PR Installed
□	AGT-8EN032	10.11.2.8	Online	Microsoft Windows 8 Enterprise	8.3.0.722	No	No	No	No	Yes
□	AGT-VEN232	10.11.1.14	Online	Microsoft Windows Vista Enterprise (x86) Edition	8.3.0.722	No	No	No	No	Yes
□	LEMSS-I	10.11.1.174	Online	Microsoft Windows Server 2008 R2 Standard x64	8.3.0.734	No	Pending Install	No	Pending Install	Pending Install

Rows per page: 100

0 of 3 selected

Page 1 of 1

1

Figure 53: All Tab

The All Tab Toolbar

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

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

Table 60: All Tab Toolbar Functions

Button	Function
Manage Agents... (menu)	Opens the **Manage Agents** menu.
Install Agents... (**Manage Agents...** menu item)	Install agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 109.
Uninstall Agents... (**Manage Agents...** menu item)	Uninstalls agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 173.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting an Endpoint on page 174.
Enable	Enables a disabled endpoint. For additional information, refer to Enabling the Ivanti Endpoint Security Agent on page 175. **Note:** This button is only available when an endpoint is disabled.

Button	Function
Disable	Disables an enabled endpoint. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 176.
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading Endpoints on page 173.
Manage Modules...	Opens the **Add/Remove Modules** dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Installing Endpoint Modules on page 177.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The All Tab List

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

The following table describes the columns within the ***All*** tab list and the comma separated value (`.csv`) file you can export from it (refer to Exporting Data on page 39).

Table 61: All Tab List Columns

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

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td><b>Agent Status</b></td><td>The status of the Ivanti Endpoint Security Agent on the endpoint. Values include:
<table>
<tr><td><b>Online</b></td><td>The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 60 for more information on configuring default agent behavior.</td></tr>
<tr><td><b>Offline</b></td><td>The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an <code>Offline</code> status, the agent still enforces all policies.
<b>Note:</b> A <b>Warning</b> (⚠) icon next to an <code>Offline</code> status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details.</td></tr>
<tr><td><b>Disabled</b></td><td>The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.</td></tr>
</table></td></tr>
<tr><td><b>Last Connected Date (Server)</b></td><td>Exported comma separated value (<code>.csv</code>) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.</td></tr>
</table>

Column	Description
EDS Status	Exported comma separated value (`.csv`) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values: **Started** EDS server has started and is in an operational state accepting workloads. **Starting** EDS server is in the process of starting its service. **Stopped** EDS server has stopped and is not accepting workloads. **Stopping** EDS server is in the process of stopping so as to not accept workloads. **Offline** EDS server is offline as it has not contacted the database in the configured amount of time.
Operating System	The operating system that the endpoint uses.
Agent Version	The version of the Ivanti Endpoint Security Agent installed. **Note:** A ⚙ icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.
***Module* Installed**	Indicates whether a module is installed on the endpoint. A new ***Module* Installed** column is added for each module installed on your Ivanti Endpoint Security Server. The following list defines column entry values: **Yes** The module is installed. **No** The module is not installed. **Pending Install** The module is in the process of installing. **Pending Uninstall** The module is in the process of uninstalling. **Error** There was an error while installing or uninstalling the module. Click the for additional information about the error. **Expired** The module license has expired.

Viewing the Endpoints Page

The ***Endpoints*** page has filters that allow you to customize your view of the computers and other devices that are managed on your network.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. [Optional] Complete a task listed in Working with the Endpoints Page on page 172.

Working with the Endpoints Page

You can perform a number of tasks related to endpoints using toolbar buttons on the ***Endpoints*** page.

Click a button to perform a task. Some buttons are not available until one or more list item is selected.

The following list displays the tasks that you can perform from the ***Endpoints*** page.

- Installing an Agent on page 172
- Installing Agents by Agent Management Job on page 172
- Uninstalling Agents by Agent Management Job on page 173
- Downloading the Agent Installer on page 173
- Deleting an Endpoint on page 174
- Enabling the Ivanti Endpoint Security Agent on page 175
- Disabling the Ivanti Endpoint Security Agent on page 176
- Upgrading Endpoints on page 173
- Installing Endpoint Modules on page 177

Installing an Agent

Before you can manage a network endpoint, you must install an agent. You can install an agent manually or using a wizard.

There are two ways in which you can install an agent on an endpoint:

- Install an agent remotely by creating an Agent Management Job. For additional information, refer to Installing Agents by Agent Management Job on page 109.
- Install an agent locally by browsing to the Ivanti Endpoint Security server from the endpoint that you want to manage and downloading the agent installer. For additional information, refer to Downloading the Agent Installer on page 173.

Installing Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of installing agents using an Agent Management Job. To create an Agent Management Job that installs agents from the ***Endpoints*** page, select **Manage Agents** > **Install Agents** from the toolbar.

Tip: You can predefine job targets by selecting endpoints from the page list.

For additional information, refer to Installing Agents by Agent Management Job on page 109.

Uninstalling Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of uninstalling agents using an Agent Management Job. To create an Agent Management Job that uninstalls agents from the ***Endpoints*** page, select **Manage Agents** > **Uninstall Agents** from the toolbar.

Tip: You can predefine job targets by selecting endpoints from the page list.

For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.

Upgrading Endpoints

From the ***Endpoints*** page, you can upgrade your endpoints to the latest version of the Ivanti Endpoint Security Agent. You can update all the endpoints at once, but, as a test, you should upgrade just a few endpoints.

Upgrade your agents using the ***Manage Agent Versions*** dialog, which can be opened from any tab on the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the endpoints you want to upgrade.
3. Click **Agent Versions**.

   Step Result: The ***Manage Agent Versions*** dialog opens.

4. Select the latest agent version from the **Select One** menu and click **Apply to All Agents**.

   Tip:

   - You can also select an agent version for each endpoint by using the **Agent Version** column menu.
   - The agent versions available for upgrading can be selected from the ***Agents*** tab on the ***Options*** page.

5. Click **OK**.

Result: Your endpoints begin upgrading.

- Endpoint upgrade progress displays on the **Manage** > **Endpoints** page.
- Endpoints in the process of upgrading display the icon ⚙ in the **Agent Version** column.
- When the icons stops displaying, and the agent version updates, the upgrade is complete.

Downloading the Agent Installer

You can install an agent locally by connecting to the Ivanti Endpoint Security, downloading the agent installer, and running the installer on the endpoint that you want to manage.

The following procedure describes the steps required to download the agent installer to the endpoint that you want to manage using Ivanti Endpoint Security. The agent system requirements and installation procedure varies by operating system. For complete instructions regarding the installation of agents on supported operating systems, refer to the Ivanti Endpoint Security: Agent Installation Guide (http://help.ivanti.com) .

1. Log in to the target computer as the local administrator (or a member of the **Local Administrators** group).
2. Log into your Ivanti Endpoint Security.

   For additional information, refer to Logging In on page 20.
3. From the **Navigation Menu**, select **Tools** > **Download Agent Installer**.
4. Select the endpoint operating system from the **Operating System** drop-down list.
5. Select the agent version that you want to install on the endpoint from the **Agent Version** drop-down list.

   Note: The agent versions available for selection are defined by the **Agent Version Options**, which you can edit from the ***Options*** page ***Agents*** tab. For additional information, refer to Agent Versions on page 56.
6. Click **Download**.

Result: A ***Download File*** dialog opens, prompting you to save or open the installer.

Deleting an Endpoint

Deleting an endpoint removes its record from the Ivanti Endpoint Security.

Prerequisites:

The endpoints you want to delete must be disabled. For additional information, refer to Disabling the Ivanti Endpoint Security Agent on page 176.

Delete endpoints from the ***Endpoints*** page ***All*** tab.

Note: Deleting an endpoint removes its record from the Ivanti Endpoint Security database, but it does not remove the agent on the endpoint.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Ensure the page is filtered to display disabled agents.

   For additional information, refer to Using Filters on page 35.
3. Select one or multiple endpoints with disabled agents.
4. In the toolbar, click **Delete**.

   Step Result: A ***delete confirmation*** dialog displays.
5. Click **OK** to confirm the deletion.

Result: The endpoint is deleted from the list.

Enabling Modules on an Endpoint

Enabling a module's endpoint component activates the functions an agent's installed module after it has been disabled.

Prerequisites:

Endpoints must have the applicable agent module installed, and the endpoint must be licensed for the agent module. For additional information, refer to Installing Endpoint Modules on page 177.

Enable a module from the applicable ***Endpoints*** page tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the tab for the module that you want to enable for an endpoint.

   Note: The tabs available will vary based on the module(s) you have installed.

3. Select one or more endpoint that does not have the module enabled.
4. From the toolbar, select **Enable** > **Enable Module**.

Result: The module for the selected endpoints is enabled.

Enabling the Ivanti Endpoint Security Agent

Disabled Ivanti Endpoint Security Agents can be reenabled at any time. Enabling a Ivanti Endpoint Security Agent allows it to be included in the security management activities of the Ivanti Endpoint Security.

Enable endpoints from the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the disabled endpoint(s) you want to enable.
3. Click **Enable**.

Result: The agent and all modules are enabled.

Disabling Modules on an Endpoint

Disabling a module's endpoint components deactivates the module functions for the endpoint's agent.

Prerequisites:

The module you want to disable must currently be enabled.

Disable a module from the applicable ***Endpoints*** page tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.

2. Select the tab for the module that you want to disable for an endpoint.

   > **Note:** The tabs available will vary with which module(s) you have installed.

3. Select one or more endpoints with the agent module enabled.
4. From the toolbar, select **Disable** > **Disable Module**.

   Step Result: A notification displays, informing you that disabling the module stops module-related functions.

   > **Note:** Disabling a module does not release applicable agent license. To release an agent license, you must completely uninstall the agent module on the endpoints. For additional information, refer to Installing Endpoint Modules on page 177

5. Click **OK** to dismiss the notification.

Result: The module for the selected endpoints is disabled.

Disabling the Ivanti Endpoint Security Agent

Once the Ivanti Endpoint Security Agent on an endpoint is disabled, the installed modules no longer function. Disabled Ivanti Endpoint Security Agents remain listed and can be re-enabled at any time.

Disable endpoints from the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the enabled endpoint(s) you want to disable.
3. Click **Disable**.

Result: The endpoint is displayed in the list of endpoints identified with the disabled icon in the **Status** column. After disabling an agent, the endpoint can be deleted from Ivanti Endpoint Security.

> **Note:** Once disabled, the endpoint may not appear in the list based on the **Status** filter settings. To include disabled endpoints in the list, ensure you select **Disabled** or **All** in the **Status** filter.

The Add/Remove Modules Dialog

This dialog lists information about each module license you have purchased. You can also use it to install or remove module endpoint components to or from individual endpoints within your network.

Open this dialog from the ***Endpoints*** page by selecting one endpoint or more and clicking **Manage Modules**.

The following describes each item in the dialog table.

Table 62: Add/Remove Dialog Table

Item	Description
Licenses	The modules you are currently licensed for. A column appears for each module you are licensed for.
Purchased	The number of licenses purchased for the applicable module.
In Use	The number of licenses in use for the applicable module.
Pending	The number of licenses pending installation or removal for the applicable module.
Available	The number of module licenses available for assignment.

The following table describes each column in the dialog list.

Table 63: Add/Remove Dialog List

Column	Description
Endpoint Name	Indicates the name of managed endpoint.
IP Address	Indicates the IP address of the managed endpoint.
Agent Version	Indicates the agent version number defined for the endpoint.
Module Name	Indicates if the module endpoint component for the applicable module is installed on the endpoint. A selected check box indicates the component is installed on the endpoint. A cleared check box indicates the module is not installed on the endpoint.

Note: There is a ***Module Name*** column for each module you have purchased.

Installing Endpoint Modules

Before you can use a module's functions on your Ivanti Endpoint Security network endpoints, you must first install the module's endpoint component on the applicable endpoints. After installing a module endpoint, you can remove it any time.

Prerequisites:

If installing a module's endpoint components, the module's server component must be installed.

Manage module endpoint components for individual endpoints from the ***Add/Remove Modules*** dialog.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Select the checkbox(es) associated with the endpoints for which you want to manage modules.
3. Click **Manage Modules**.

   Step Result: The ***Add/Remove Modules*** dialog opens.

4. Manage modules for each endpoint.
   - To add a module for a particular endpoint, select the module checkbox for the applicable endpoint.
   - To remove a module for a particular endpoint, clear the module checkbox for the applicable endpoint.
5. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes. The begins installing or uninstalling the selected modules. As module management occurs, the endpoint ***Module* Installed** status changes in the ***Endpoint*** page list.

> **Note:** When installing the Device Control endpoint module, target endpoints must be rebooted to complete installation.

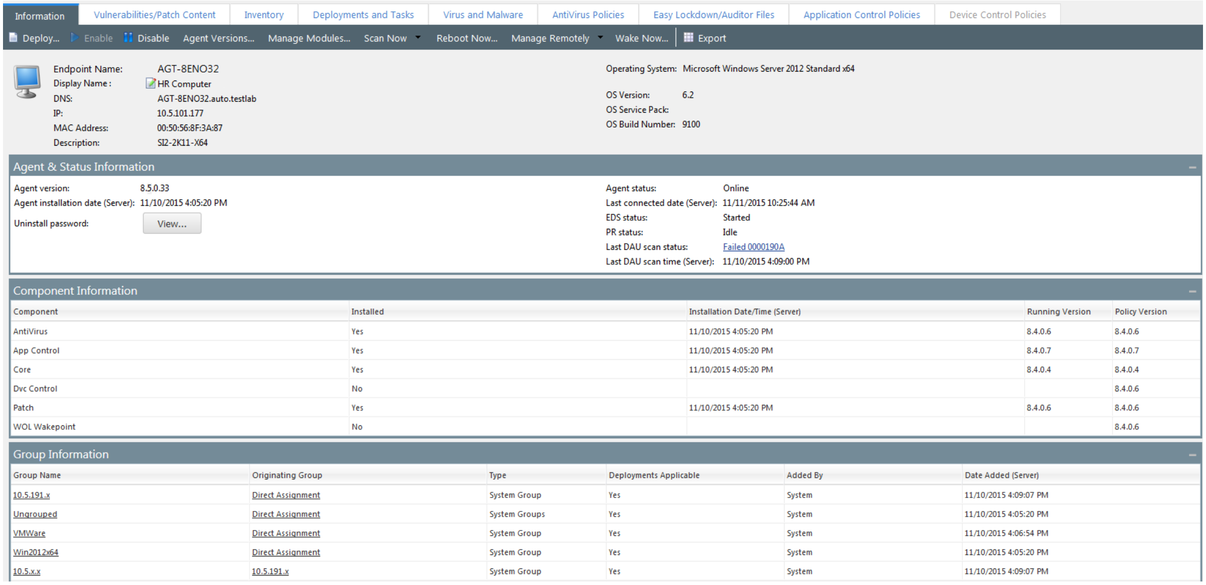
Exporting Endpoint Information

You can export the endpoint information generated in the Ivanti Endpoint Security so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.csv`) file format. For additional information, refer to Exporting Data on page 39.

The Endpoint Details Page

The ***Endpoint Details*** page lists general endpoint information, agent information, the modules installed on the endpoints, the groups the endpoint is included in, and the group policies applied to it. This page also includes a tab for each module installed.



Endpoint Name: AGT-8ENO32
Display Name : HR Computer
DNS: AGT-8ENO32.auto.testlab
IP: 10.5.101.177
MAC Address: 00:50:56:8F:3A:87
Description: SI2-2K11-X64

Operating System: Microsoft Windows Server 2012 Standard x64
OS Version: 6.2
OS Service Pack:
OS Build Number: 9100

Agent & Status Information

Agent version: 8.5.0.33
Agent installation date (Server): 11/10/2015 4:05:20 PM
Uninstall password:

Agent status: Online
Last connected date (Server): 11/11/2015 10:25:44 AM
EDS status: Started
PR status: Idle
Last DAU scan status: Failed 0000190A
Last DAU scan time (Server): 11/10/2015 4:09:00 PM

Component Information

Component	Installed	Installation Date/Time (Server)	Running Version	Policy Version
AntiVirus	Yes	11/10/2015 4:05:20 PM	8.4.0.6	8.4.0.6
App Control	Yes	11/10/2015 4:05:20 PM	8.4.0.7	8.4.0.7
Core	Yes	11/10/2015 4:05:20 PM	8.4.0.4	8.4.0.4
Dvc Control	No			8.4.0.6
Patch	Yes	11/10/2015 4:05:20 PM	8.4.0.6	8.4.0.6
WOL Wakepoint	No			8.4.0.6

Group Information

Group Name	Originating Group	Type	Deployments Applicable	Added By	Date Added (Server)
10.5.191.x	Direct Assignment	System Group	Yes	System	11/10/2015 4:09:07 PM
Ungrouped	Direct Assignment	System Groups	Yes	System	11/10/2015 4:05:20 PM
VMWare	Direct Assignment	System Group	Yes	System	11/10/2015 4:06:54 PM
Win2012x64	Direct Assignment	System Group	Yes	System	11/10/2015 4:05:20 PM
10.5.x.x	10.5.191.x	System Group	Yes	System	11/10/2015 4:09:07 PM

Figure 54: Endpoint Details Page

Viewing the Endpoint Details Page

The ***Endpoint Details*** page contains comprehensive details for an endpoint and its activity within the Ivanti Endpoint Security system.

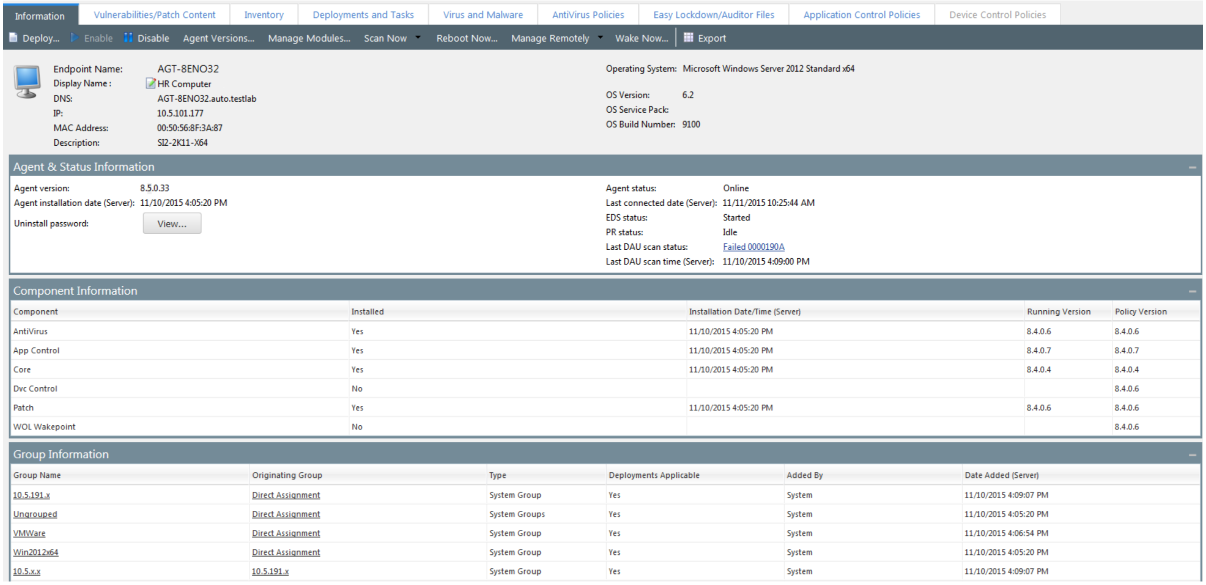
View the ***Endpoint Details*** page for an endpoint by clicking an endpoint name link from the ***Endpoints*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the **Name** link associated with the endpoint details you want to review.

   Step Result: The ***Endpoint Details*** page opens to the ***Information*** tab.
3. [Optional] Complete a task listed in Working with the Endpoint Details Page on page 186.

The Information Tab

The ***Information*** tab displays information about a selected endpoint. The page displays general information organized into endpoint, agent, status, component, group, and policy sections.



Endpoint Name: AGT-8ENO32
Display Name : HR Computer
DNS: AGT-8ENO32.auto.testlab
IP: 10.5.101.177
MAC Address: 00:50:56:8F:3A:87
Description: SI2-2K11-X64

Operating System: Microsoft Windows Server 2012 Standard x64

OS Version: 6.2
OS Service Pack:
OS Build Number: 9100

Agent & Status Information

Agent version: 8.5.0.33
Agent installation date (Server): 11/10/2015 4:05:20 PM
Uninstall password:

Agent status: Online
Last connected date (Server): 11/11/2015 10:25:44 AM
EDS status: Started
PR status: Idle
Last DAU scan status: Failed 0000190A
Last DAU scan time (Server): 11/10/2015 4:09:00 PM

Component Information

Component	Installed	Installation Date/Time (Server)	Running Version	Policy Version
AntiVirus	Yes	11/10/2015 4:05:20 PM	8.4.0.6	8.4.0.6
App Control	Yes	11/10/2015 4:05:20 PM	8.4.0.7	8.4.0.7
Core	Yes	11/10/2015 4:05:20 PM	8.4.0.4	8.4.0.4
Dvc Control	No			8.4.0.6
Patch	Yes	11/10/2015 4:05:20 PM	8.4.0.6	8.4.0.6
WOL Wakepoint	No			8.4.0.6

Group Information

Group Name	Originating Group	Type	Deployments Applicable	Added By	Date Added (Server)
10.5.191.x	Direct Assignment	System Group	Yes	System	11/10/2015 4:09:07 PM
Ungrouped	Direct Assignment	System Groups	Yes	System	11/10/2015 4:05:20 PM
VMWare	Direct Assignment	System Group	Yes	System	11/10/2015 4:06:54 PM
Win2012x64	Direct Assignment	System Group	Yes	System	11/10/2015 4:05:20 PM
10.5.x.x	10.5.191.x	System Group	Yes	System	11/10/2015 4:09:07 PM

Figure 55: The Information Tab

Tip:

- Each ***Information*** tab section can be collapsed and expanded.
- Each section can also be dragged higher or lower on the page. Place more frequently used information high on the page.

The Information Tab Toolbar

The ***Information*** tab toolbar contains the endpoint assessment tasks and functions that are available for you to perform on managed endpoints.

The following table describes the buttons available in the ***Information*** tab toolbar.

Table 64: Information Tab Toolbar Buttons

Toolbar Button	Description
Enable	Enables the endpoint (if it is disabled). For additional information, refer to Enabling an Endpoint on page 187.
Disable	Disables the endpoint (if it is enabled). For additional information, refer to Disabling an Endpoint on page 188.

Toolbar Button	Description
Agent Versions...	Defines the agent version(s) that can be installed on an endpoint. For additional information, refer to Upgrading the Agent on a Single Endpoint on page 187.
Manage Modules...	Opens the ***Add/Remove Modules*** dialog, which lets you manage agent features for modules install on Ivanti Endpoint Security. For additional information, refer to Managing Endpoint Modules on page 188.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **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.

Endpoint Information

The fields that appear in this section of the ***Information*** tab contain identifier and operating system details, such as the IP address and the operating system.

The **Endpoint Information** section displays the following endpoint data:

Table 65: Endpoint Information Field Descriptions

Field	Description
Endpoint Name	The name of the endpoint.
DNS	The DNS name of the endpoint.
Display Name	Alternate name or phrase (up to 50 characters) for the endpoint to help you identify and distinguish it. Endpoint decision-making information you can provide here includes what system it belongs to, where it is located, and what it is used for. The Display Name will appear as a tool-tip when you hover over the Endpoint Name in the on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view).
IP	The IP Address of the endpoint.
MAC Address	The MAC address of the endpoints.
Description	The description of the endpoint, if available.
Operating System	The abbreviated name of the operating system detected on the endpoint.

Field	Description
OS Version	The version number of the operating system running on the endpoint.
OS Service Pack	The service pack level of the endpoint.
OS Build Number	The build number of the operating system running on the endpoint.

Agent Information

The fields that appear in the **Agent Information** section of the ***Information*** tab contain agent status, version, and connectivity details for the agent installed on the endpoint.

The **Agent Information** section displays the following agent data.

Table 66: Agent Information Field Descriptions

Field	Description
Agent version	The version of the agent that the endpoint is currently running. **Note:** A ⚙ icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.
Agent installation date (Server)	The date and time on the server when the agent registered with Ivanti Endpoint Security. This is typically the date the agent was installed on the endpoint.
Uninstall password (button)	Click **View** to view the uninstall password assigned to the endpoint. See Viewing the Agent Uninstall Password on page 186 for more information.

Status Information

The fields that appear in the **Status Information** section of the ***Information*** tab contain status and connectivity details for the agent installed on the endpoint.

Table 67: Status Information Field Descriptions

Field	Description
Agent status	Indicates the status of the endpoint. The following list defines column values: **Online** The agent is able to communicate with the Ivanti Endpoint Security server in the predefined time period. Refer to Configuring the Agents Tab on page 60 for additional information on configuring agent default behavior. **Offline** The agent is unable to communicate with the Ivanti Endpoint Security server in the predefined time period. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** () icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) the endpoint connects to is offline. Click the icon to find out additional status details. **Disabled** The agent will no longer enforce any module policies or complete tasks. All endpoints must show a `Disabled` status in order to delete the endpoint. Refer to Disabling the Ivanti Endpoint Security Agent on page 176.
Last connected date (Server)	The date and time on the server that the agent last communicated with Ivanti Endpoint Security.
EDS Status	The status of the Endpoint Distribution Service on the server. Service statuses include **Started** and **Stopped**.

Component Information

This table lists which module components are installed on the endpoint. It also lists additional information about each module.

The following table describes each **Component Information** table column.

Table 68: Component Information Table

<table>
<tr><th>Column</th><th colspan="2">Description</th></tr>
<tr><td><b>Component</b></td><td colspan="2">Indicates the name of the applicable module.</td></tr>
<tr><td rowspan="7"><b>Installed</b></td><td colspan="2">Indicates whether the module is installed on the endpoint. Values include:</td></tr>
<tr><td><b>Yes</b></td><td>The module is installed.</td></tr>
<tr><td><b>No</b></td><td>The module is not installed.</td></tr>
<tr><td><b>Pending Install</b></td><td>The module is in the process of installing.</td></tr>
<tr><td><b>Pending Uninstall</b></td><td>The module is in the process of uninstalling.</td></tr>
<tr><td><b>Error</b></td><td>There was an error while installing or uninstalling the module. Click the for additional information about the error.</td></tr>
<tr><td><b>Expired</b></td><td>The module license has expired.</td></tr>
<tr><td><b>Installation Date/Time (Server)</b></td><td colspan="2">Indicates the date and time on the server that the user initiated a module install.</td></tr>
<tr><td><b>Running Version</b></td><td colspan="2">Indicates the version of the module installed on the agent.</td></tr>
<tr><td><b>Policy Version</b></td><td colspan="2">Indicates the version of the module that is should be installed based on the agent version defined in the applicable agent policy set.</td></tr>
</table>

Group Information

The columns that appear in the **Group Information** section of the ***Information*** tab contain group membership details for the endpoint.

The **Group Information** section displays the following group data for an endpoints.

Table 69: Group Information Column Descriptions

Column	Description
Group Name	The group that the endpoint holds membership in, either through direct assignment or inheritance. Click the group name to open ***Group Information*** page.

Column	Description
Originating Group	The name of the group in the parent hierarchy from which the the endpoint inherits membership. If the endpoint is directly assiged to a group, the value displayed is **Direct Assignment**. Click the value to go to the ***Group Information*** page.
Type	The group type, which can include: • **System Group**: a group created by Ivanti Endpoint Security • **Custom Group**: a group created by a user • **My Groups**: an indication that the group is within the group hieracrchy
Deployments Applicable	Indicates that there are applicable deployments available for this endpoint.
Added By	The Ivanti Endpoint Security user who added the endpoint to the group. If the endpoint was added Ivanti Endpoint Security, the column contains a value of `System`.
Date Added (Server)	The date and time that the endpoint was added to the group.

Note:

- If the values in the **Group Name** and the **Originating Group** columns are identical, then the endpoint is directly assigned to that group and is not inherited..
- Groups listed in gray indicate that the endpoint holds group membership through inheritance.

Policy Information

The fields that appear in the **Policy Information** section of the ***Information*** tab contain details about the policies used by the endpoint during a deployment.

These policies are the results of applying each of the policies defined by the endpoint's group membership and filling in any undefined policies from the Global Policy. Conflict resolution rules are applied when applicable.

Table 70: Policy Information Column Descriptions

Column	Description
Name	The name of the policy applied to the endpoint.
Value	The value of the policy applied to the endpoint.

Column	Description
Description	The description of the policy.

Tip: For a description of all agent policies, including agent policies not applied to the endpoint, refer to The Agent Policy Sets Page List on page 242.

Working with the Endpoint Details Page

You can perform a number of tasks related to endpoints from the ***Endpoint Details*** page. You perform most of these tasks regardless of the tab selected. However, certain tasks are specific to certain tabs.

To perform most tasks associated with endpoints, click a toolbar button. To perform some tasks, selecting one or multiple endpoints from the page list may be necessary.

The following list displays the tasks you can perform from the ***Endpoint Details*** page.

- Viewing the Agent Uninstall Password on page 186
- Upgrading the Agent on a Single Endpoint on page 187
- Enabling an Endpoint on page 187
- Disabling an Endpoint on page 188
- Managing Endpoint Modules on page 188
- Exporting Endpoint Information on page 189

Viewing the Agent Uninstall Password

If you need to uninstall the agent from an endpoint, you will be prompted to enter a password during the uninstall. You can view this uninstall password from the ***Endpoint Details*** page for the endpoint.

View the agent uninstall password from the endpoint's ***Endpoint Details*** page ***Information*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the ***Name*** link for the relevant endpoint.

   Step Result: The ***Endpoints Details*** page opens to the ***Information*** tab.
3. From the toolbar, click **View**.

Result: The ***Agent Uninstall Password*** dialog opens, displaying the password. Record the password if necessary. Close the dialog when you are done.

The Agent Uninstall Password Dialog

The ***Agent Uninstall Password*** dialog contains the endpoint's name and the password that is required to uninstall the agent locally from an endpoint.

The following table describes the fields that appear on the ***Agent Uninstall Password*** dialog.

Table 71: Agent Uninstall Password Dialog Fields

Field	Description
Endpoint name	The endpoint's name.
Agent uninstall password	The password required to uninstall the agent from the endpoint locally.

Upgrading the Agent on a Single Endpoint

From the ***Endpoint Details*** page, you can upgrade the Ivanti Endpoint Security Agent installed on the endpoint to a newer version.

Define the agent version for the endpoint from the ***Information*** tab.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link associated with endpoint you want to define agent version(s) for.

   Step Result: The ***Endpoint Details*** page for the endpoint opens to the ***Information*** tab.

3. Click **Agent Versions**.

   Step Result: The ***Manage Agent Versions*** dialog opens.

4. Select an agent version from the **Agent Version** list.

   Note: The agent versions available for selections are defined from the ***Options*** page. For additional information, refer to Configuring the Agents Tab on page 60.

5. Click **OK**

Result: The ***Manage Agent Versions*** dialog closes. If an agent version other than the defined version is installed on the endpoints, the defined version is installed over the previous version.

Enabling an Endpoint

Enabling an endpoint includes the endpoint in the content management activities of the Ivanti Endpoint Security.

You can enable an endpoint from the ***Endpoint Details*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.

2. Click the link in the **Name** column that corresponds to the endpoint that you want to enable.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Click **Enable**.

Result: The endpoint is enabled.

Disabling an Endpoint

Disabling an endpoint stops agent functions on an endpoint. Disabled endpoints are not included in security management activity.

You can disable an endpoint from the ***Endpoint Details*** page.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds with the endpoint you want to disable.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Click **Disable**.

   Step Result: A ***disable confirmation*** dialog displays.

4. In the ***confirmation*** dialog box, click **OK**.

Result: The endpoint is disabled. After disabling an agent, the endpoint can be deleted from Ivanti Endpoint Security.

> **Note:** Once disabled, the endpoint may not appear in the ***Endpoints*** page list based on the **Status** filter settings. To include disabled devices in the list, ensure you select **Disabled** or **All** in the **Status** filter.

Managing Endpoint Modules

You may select which module license an endpoint's agent uses. Using this feature allows you control which modules apply to a particular endpoint.

Manage modules for individual endpoints from the ***Add/Remove Modules*** dialog.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link for the endpoint you want to work with.

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

3. Click **Manage Modules**.

   Step Result: The ***Add/Remove Modules*** dialog opens.

4. Manage modules for each endpoint.
   - Select an empty checkbox to add a module.
   - Clear selected checkboxes to remove a module.
5. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes and modules are either installed or uninstalled according to your changes.

Exporting Endpoint Information

You can export the endpoint information generated in the Ivanti Endpoint Security so that it can be used in other applications.

The export utility lets you export endpoint information to a comma-separated value (`.csv`) file format. For additional information, refer to Exporting Data on page 39.

Adding a Display Name to an Endpoint

You can associate an alternate name (50 characters maximum) with an endpoint to help you identify and distinguish it.

Use the Display Name to provide endpoint decision-making information like what system it belongs to, where it is located, and what it is used for.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to add a Display Name to.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Beside the **Display Name**, click the **Edit** icon.

   Step Result: An editable field appears.
4. Enter a word or phrase up to 50 characters in length. If you leave the field blank the **Endpoint Name** will be used.

5. Click the **Save** icon (✓) .

Note: The **Cancel** icon (☒) cancels your changes and anything you enter is not saved.

Result: A Display Name is added to the Endpoint information. It will appear on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view):

- Tool-tip when you hover over the Endpoint Name.
- Display Name column of Endpoint lists (the tool-tip when you hover over a Display Name is the Endpoint Name).
- Display Name column of the comma separated list (CSV) file you export.

Tip: You can filter endpoints by Display Name using the **Display Name** filter.

Editing the Display Name of an Endpoint

You can edit the alternate name associated with an endpoint on the **Manage** > **Endpoints** Information tab.

The Display Name is used to provide endpoint decision-making information like what system it belongs to, where it is located, and what it is used for.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to add a Display Name to.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.
3. Beside the **Display Name**, click the **Edit** icon.

   Step Result: An editable field appears.
4. Enter a word or phrase up to 50 characters in length. If you leave the field blank the **Endpoint Name** will be used.
5. Click the **Save** icon (✓).

Note: The **Cancel** icon (☒) cancels your changes and anything you enter is not saved.

Result: The Display Name is changed. It will appear on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view):

- Tool-tip when you hover over the Endpoint Name.
- Display Name column of Endpoint lists (the tool-tip when you hover over a Display Name is the Endpoint Name).
- Display Name column of the comma separated list (CSV) file you export.

Tip: You can filter endpoints by Display Name using the **Display Name** filter.

Removing the Display Name of an Endpoint

You can remove the alternate name associated with an endpoint on the **Manage** > **Endpoints** Information tab.

The Display Name is used to provide endpoint decision-making information like what system it belongs to, where it is located, and what it is used for.

1. From the **Navigation Menu**, select **Manage** > **Endpoints**.
2. Click the link in the **Name** column that corresponds to the endpoint that you want to add a Display Name to.

   Step Result: The ***Endpoints Details*** page opens with the ***Information*** tab selected by default.

3. Beside the **Display Name**, click the **Edit** icon.

   Step Result: An editable field appears.

4. Remove the name from the field.
5. Click the **Save** icon (💾).

   Note: The **Cancel** icon (☒) cancels your changes and anything you enter is not saved.

Result: The custom Display Name is removed and the Endpoint Name is used instead. It will appear on the **Manage** > **Endpoints** page and **Manage** > **Groups** page (Endpoint Membership view):

- Tool-tip when you hover over the Endpoint Name.
- Display Name column of Endpoint lists.
- Display Name column of the comma separated list (CSV) file you export.

Chapter 10

Using Groups

In this chapter:

Within Ivanti Endpoint Security, you can organize endpoints into groups, which are collections of endpoints. Organizing endpoints into a group lets you manage them as a single object.

About Groups

A *group* is a collection of endpoints that you can manage collectively. Within Ivanti Endpoint Security you can create custom groups to administer all endpoints as a single object.

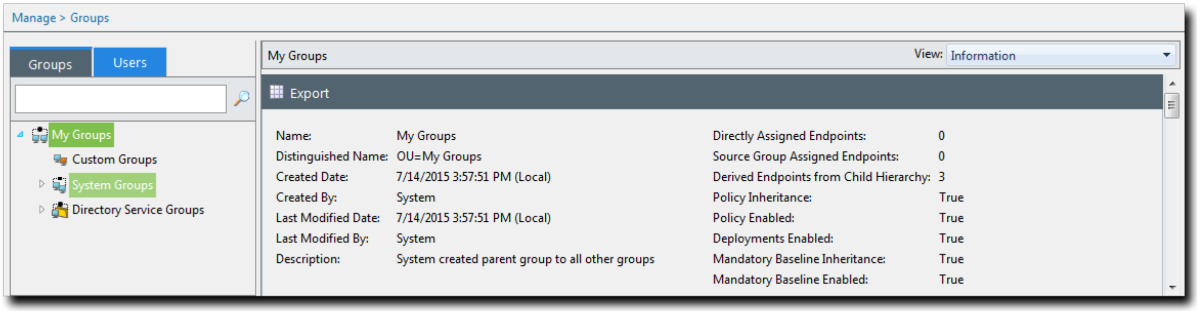
Groups are organized into a tree hierarchy in which groups are nested; groups can contain other groups. This structure allows for inheritence of group members and policies, helping to minimize endpoint maintenance.

- For more information about the controls used to managed groups, see The Groups Page Browser on page 195.
- For more information about how you can use groups and their hierarchy to simplify Ivanti Endpoint Security administration, see Group Hierarchy on page 196.
- For more information about the different types of groups in Ivanti Endpoint Security, see Defining Groups on page 197.

The Groups Page

Use this page to control groups. The functions from many other Ivanti Endpoint Security pages are available from this page (the ***Endpoints*** page, the ***Users and Roles*** page, and so on). However, the functions performed on the ***Groups*** page pertain primarily to the selected group's endpoints.

Groups are selected from the **Browser**, a ***Groups*** page pane. The browser displays an expandable tree that lists parent and child groups. From this browser, you can access group information by clicking a group. Information for the selected group displays in the main pane.



My Groups

View: Information

Name:	My Groups	Directly Assigned Endpoints:	0
Distinguished Name:	OU=My Groups	Source Group Assigned Endpoints:	0
Created Date:	7/14/2015 3:57:51 PM (Local)	Derived Endpoints from Child Hierarchy:	3
Created By:	System	Policy Inheritance:	True
Last Modified Date:	7/14/2015 3:57:51 PM (Local)	Policy Enabled:	True
Last Modified By:	System	Deployments Enabled:	True
Description:	System created parent group to all other groups	Mandatory Baseline Inheritance:	True
		Mandatory Baseline Enabled:	True

Figure 56: Groups Page

Unlike most other Ivanti Endpoint Security pages, which are organized by tabs, the ***Groups*** page is organized by views, which are selectable from the **View** list. The information displayed for a selected group changes according to view.

The views are:

- The Information View on page 198
- The Group Membership View on page 202
- The Endpoint Membership View on page 207
- The Agent Policy Sets View on page 219
- The Roles View on page 225
- The Dashboard View on page 230
- The Settings View on page 231

The Groups Page Browser

Interact with all groups in Ivanti Endpoint Security by using the ***Groups*** page **Browser**, which organizes your groups into a tree hierarchy.

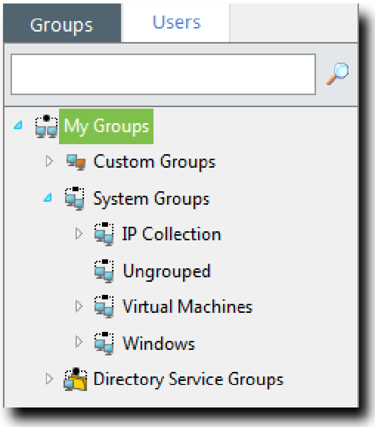


Figure 57: Browser

You can interact with the **Browser** in a variety of ways:

- You can expand the group hierarchy by clicking the **triangle**.
- You can collapose the group hierarchy by clicking click the **triangle** again.
- You can interact with a group by selecting it and using the ***Groups*** page features.
- You can create a new group, add endpoints to the selected group, or change views for the selected group by right-clicking it and making a selection from the menu.
- You can drag and drop custom groups by dragging the custom groups *icon* (not the group name) into another group.

Note: Remember a couple of thing when you are dragging and dropping groups:

- You can't drag a group down within its own child hierarchy. Groups can be moved to other group hierarchys however.
- If you drag a group with a child hierarchy into another group, the child hierachy gets moved as well.
- If the group you are moving is inheriting Agent Policy Sets, moving that group will change the policies it inherits. Before moving the group, check what Agent Policy Sets the group is inheriting, because moving a group without understanding its inherited policies can result in *big* changes to endpoint behavior!

Group Hierarchy

Within the ***Groups*** page **Browser**, groups are organized into a tree hierarchy. This hierarchy creates a structure similar to a family tree. This structure allows you to aggregate group membership and settings through inheritance. Familiarize yourself with examples of group hierarchy in this topic to understand how groups impact endpoint group membership and settings.

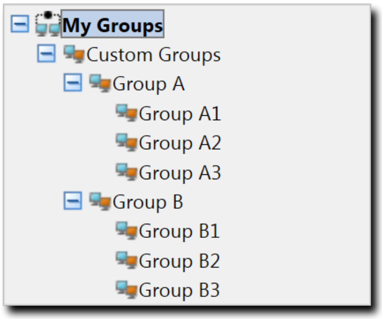


Figure 58: Group Tree Example

Root Group	In the Ivanti Endpoint Security group tree structure, the root group is the group of origin, which has no parents or ancestors. Within Ivanti Endpoint Security, **My Groups** is the root group, and all other groups are its descendent.
Parent Group	A parent group is a group that is one branch higher in the tree than the groups below it. In the figure above, **Group A** is parent of **Group A1**, **Group A2**, and **Group A3**. A parent group can have multiple child groups, and these children inherit the parent group settings.
Child Group	A child group is a group that is one branch lower in the tree than its parent. In the figure above, **Group A1** is the child of **Group A**. Each child group can only have one parent, and the child group inherits its parent settings by default.
Sibling Groups	Sibling groups are groups that share a parent group. In the figure above, **Group A** and **Group B** are siblings. Any group can have zero, one, or more siblings.
Ancestor Groups	Ancestors groups are all the groups above a group in the tree hierarchy for a single lineage. In the figure above, **Group A1** has ancestor groups of **Group A**, **Custom Groups**, and **My Groups**. **Group B** *is not* an ancestor group for **Group A1**.
Descendent Groups	Descendent groups are all the groups below a group in the tree hierarchy. In the figure above, **Customs Groups** has descendants in **Group A** (and all its child groups) and **Group B** (and all its child groups).

Leaf Group	A leaf group is a group that has no children. In the figure above, **Group A1** is a leaf group.
Inheritance	Inheritance is the mechanism that allows groups to aggregate endpoint membership and settings. • Endpoint membership is inherited *up* the tree. For example, endpoints added to **Group A3** are aggregated to with the endpoints directly assigned to **Group A**. • Settings (such as mandatory baselines and agent policies) are inherited *down* the tree. For example, an Agent Policy Set assigned to **Custom Group**s is also assigned to **Group A**, as well as groups **A1**, **A2**, and **A3**. Setting inheritance is enabled by default, but you can also disable it. Each group has its own inheritance settings. See Editing Group Settings on page 232.

Note: Within the **Browser**, `System Groups` and `Directory Service Groups` hierarchies cannot be modified. For additional information on group types, refer to Defining Groups on page 197.

Defining Groups

Within Ivanti Endpoint Security, there are several types of groups. Some groups are created by users, while others are created by the Ivanti Endpoint Security system. When working with groups, only user-created groups can be deleted.

Groups are categorized into the following classifications.

Table 72: Group Definitions

Groups	Group Type	Icon	Description
My Groups	Custom Groups	(Parent) and (Child)	Custom groups are created and managed by the user.
	System Groups[1]	(Parent) and (Child)	These groups are system created groups.
	Directory Service Groups	(Parent) and (Child)	These groups are created when an agent submits a directory service hierarchy that does not already exist in Ivanti Endpoint Security. You cannot modify **Directory Service Groups** or their hierarchies.

Groups	Group Type	Icon	Description
(1) Endpoints identified in your network are automatically assigned a group membership based on IP address, Active Directory (AD) membership, or operating system. Not all IP ranges, AD groups, or operating systems may be shown. This omission is because Ivanti Endpoint Security creates system groups based on only the endpoints present in your network.			
Note: An **Ungrouped** group is a group of endpoints that have not yet been added to a custom group. A **Virtual Machines** group is a group that is created for endpoints that are in a virtual machine environment (VMware, Citrix, etc). You cannot modify **System Groups** or their hierarchies.			

Viewing Groups

Navigate to the ***Groups*** page to work with groups. After navigating to the page, select a group and a view.

You can select this page from the navigation menu at any time.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. Expand the **Browser** tree to the desired group.
3. Select the group you want to view.

   Step Result: The selected group’s information displays.

4. Select the desired view from the **View** list.

   Tip: You may right-click within the **Browser** tree and select either the **Create Group** option, **Add Endpoints to Groups** option, or a specific view. You must be on **Custom Groups** to utilize the **Create Group** or **Add Endpoints to Groups** option.

Result: The selected group’s information displays on the main pane. Select a different view from the **View** list to change the information displayed.

The Information View

This view includes basic information about the selected group's membership, hierarchy, agent policy sets, roles, and so on. Select this view for a comprehensive listing of group settings.

Group settings and information appear in sections. Each section displays information for each type of group settings. Empty sections indicate undefined settings.

The ***Information*** view features the following sections:

- Group Information on page 199
- Email Notification Addresses on page 200
- Child Groups on page 200
- Agent Policy Sets on page 201
- Resultant Agent Policy Set Information on page 201
- Roles on page 202

The following table describes the ***Information*** view buttons.

Table 73: Information View Button

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

Group Information

The first section in the ***Information*** view displays general information about the selected group's settings. These settings are controlled within the various ***Groups*** page views. Select this view when you want to see a group's settings from a single source.

The following table describes the first fields within the first section of the **Information** view.

Table 74: Group Information

Field	Description
Name	Indicates the name of the group.
Distinguished Name	Indicates the system-created name based upon the group’s parent hierarchy.
Created Date	Indicates the date and time the group was created.
Created By	Indicates the user who created the group.
Last Modified Date	Indicates the date and time the group was last modified.
Last Modified By	Indicates the user who last modified the group.
Description	Indicates the description of the group.
Directly Assigned Endpoints	Indicates the number of endpoints assigned to the group. Inherited endpoints are not included.

Field	Description
Source Group Assigned Endpoints	Indicates the number of endpoints assigned to the source group.
Derived Endpoints from Child Hierarchy	Indicates the number of endpoints inherited from child groups.
Policy Inheritance	Indicates if agent policy sets are inherited from the group's parent (`True` or `False`).
Policy Enabled	Indicates if agent policy sets can be assigned to the group (`True` or `False`).

Email Notification Addresses

After a group is created, it can be assigned an email address. This email is intended to be attributed to the group.

Email addresses are not assigned from the ***Information*** view; this view merely displays the assigned addresses. For additional information on assigning an email address to a group, refer to Editing Group Settings on page 232.

The following reference describes the **Email Notification Addresses** table.

Table 75: Email Notification Addresses Table

Column	Description
Notification Address	The email addresses of the group owner.

Child Groups

This section lists the direct Child Groups. Only direct children are listed; deeper descendants such as grandchild groups are not listed.

Tip: This section only lists direct Child Groups; to assign direct Child Groups to a group use the ***Group Membership*** view.

Table 76: Child Groups Table

Column	Description
Type	The group type (`Custom Group`, `System Group`, or `Directory Service Group`).
Group Name	The name of the child group.
Distinguished Name	The system-created name of the group, which is based upon the group's parent hierarchy.
Description	The description of the group.

Agent Policy Sets

This section lists the Agent Policy Sets assigned to the selected group, and whether or not that policy set is directly assigned or assigned via inheritance.

Tip: This section only lists group Assigned Policy Sets; to Assign Policy Sets to the selected group use the ***Policies*** view.

Table 77: Agent Policy Sets Table

Field	Description
Policy Set Name	Indicates the name of the Agent Policy Set.
Assigned	Indicates if the Agent Policy Set is directly assigned to the group or inherited. A value of `True` indicates the Agent Policy Set is directly assigned.

Note: When a group **Policy Enabled** setting is enabled, the group will use the Global System Policy set to define undefined policies. For additional information, refer to Defining Agent Policy Inheritance Rules on page 240.

Resultant Agent Policy Set Information

When a group is assigned two or more Agent Policy Sets, some of the policies may conflict. When conflicts occur, the system applies the agent policy conflict resolution rules to determine which policy to apply. This section lists the resultant policies used when there is Agent Policy Sets conflict.

The following table describes the ***Resultant Agent Policy Set Information*** information.

Table 78: Resultant Agent Policy Set Information

Field	Description
Name	The name of the agent policy.
Value	The agent policy value. When determining the policy value, directly assigned policies supersede inherited policies. Additionally, directly assigned policies that conflict are resolved by the conflict resolution rules.
Description	The description of the agent policy.

Note: Only agent policies inherited or directly assigned to the group are displayed in **Resultant Agent Policy Set Information**. To see a complete listing of all policies assigned to a managed endpoint, refer to The Information Tab on page 180.

Roles

You can restrict user access to specific groups based on roles. This section lists the user roles that can access the selected group.

> **Tip:** This section only lists the Roles that can access the group; to assign Roles to a group, use the ***Roles*** view.

Table 79: Roles Table

Field	Description
Role Name	Indicates the name of the user role that can access the group.
Role Source	Indicates the name of the group that the assigned role is inherited from. If the role source contains no value, the role is directly assigned to the selected group.
Assigned	Indicates if the role is inherited or directly assigned to the group. A value of `True` indicates the role is directly assigned to the group.

Exporting Information View Data

To export the information displayed within the ***Information*** view to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 39.

The Group Membership View

This view lets you view the selected group's direct child groups. If the selected group is a custom group, you can also create new custom child groups that you can populate with the desired endpoints. Custom groups also let you edit or delete any listed preexisting child groups.

This view only lists direct child groups; you cannot manage grandchild groups or further descendants.

The Group Membership View Toolbar

This toolbar contains buttons related to the creation and management of groups.

The following table describes the toolbar functions. Some functions are common to all the ***Groups*** page views.

Table 80: Group Membership Toolbar

Button	Function
Create	Creates a new group. For additional information, refer to Creating a Group on page 204.

Button	Function
Delete	Deletes a group. For additional information, refer to Deleting Groups on page 205.
Move...	Assigns a group to a new parent group. For additional information, refer to Moving a Group on page 206.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Group Membership View List

This list displays the selected group's direct child groups. Each listing contains group identification information and icons used to edit identification information or delete the group altogether.

The following table displays the ***Group Membership*** view list details.

Table 81: Group Membership View

Column	Icon	Description
Action	N/A	Contains **Edit** and **Delete** icons. Use these icons to edit or delete the associated group.
Groups	🖥	Contains an icon that indicates the type of the group: • `System` (🖥) • `Custom` (🖥) • `Directory Service` (📁)
Name	N/A	Indicates the name of the child group.
Description	N/A	Indicates the description of the group.
Distinguished Name	N/A	Indicates the system-created name based upon the group’s parent hierarchy.

Column	Icon	Description
Endpoints	N/A	Indicates the number of endpoints assigned to the group.

Note: ***System*** and ***Directory Service*** groups cannot have their child group or endpoint memberships edited. However, their assigned agent policy sets can be edited.

Creating a Group

Ivanti Endpoint Security provides preconfigured groups. However, you can also create custom groups. Populate custom groups with desired endpoints. You can only create custom groups within the **Browser** custom group hierarchy.

Create groups from the ***Group Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. Select the ***Custom Group*** from the directory tree that you want to create a child group for.
4. Click **Create**.

   Step Result: A new row appears on the page.
5. In the **Name** field, type a name for the group.
6. [Optional] Type a brief description about the group in the **Description** field.
7. Click the **Save** icon associated with the new group.

Result: The group is saved to the list and is added to the directory tree. A ***Distinguished Name*** is generated for the group.

After Completing This Task:
Add endpoints to the group. For additional information, refer to Adding Endpoints to a Group on page 212.

Editing Groups

You can edit the names and descriptions for custom groups.

You may edit the name and description for groups within the **Custom Groups** hierarchy. Edit groups from the ***Group Membership*** view.

Note: For **System Groups** and **Directory Service Groups** only the **Description** field can be edited, not the **Name** field.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the **Group Browser**, select a group within the **Custom Groups** hierarchy you want to edit.

4. Click the **Edit** icon (📝).

   Step Result: The **Name** and **Description** field displays.

5. [Optional] Edit the **Name** field associated with the group.
6. [Optional] Edit the **Description** field associated with the group.
7. Click the **Save** icon associated with the new group.

Result: The group changes are saved.

> **Note:** Within the ***Group Membership*** view, you can only edit the group name and description. To edit group behavior, use the ***Groups*** page views.

Deleting Groups

Delete a group when you no longer need to manage its endpoints collectively. Only custom groups can be deleted. After deleting a group, you cannot recover it; you must recreate the group.

Delete custom groups from the ***Groups Membership*** view.

> **Note:** Deleting a group does not prevent an endpoint within that group from rebooting or scanning; these tasks occur at the endpoint level.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the directory tree, select the parent group of the group(s) you want to delete.

   > **Note:** Only groups within the **Custom Groups** hierarchy can be deleted.

4. Delete the desired group(s).

   Use one of the following methods.

   > **Note:** If the group you want to delete has a child hierarchy, the group cannot be deleted until the child groups have been deleted or moved.

Method	Steps
To delete a single group:	Click the **Delete** icon associated with the group you want to delete.
To delete multiple groups:	**1.** Select the check boxes associated with the groups you want to delete. **2.** From the toolbar, click **Delete**.

   Step Result: A dialog appears asking you to acknowledge the deletion.

5. Click **OK**.

Result: The selected group(s) are deleted.

Moving a Group

After creating a group, you can change its position within the **Browser** tree.

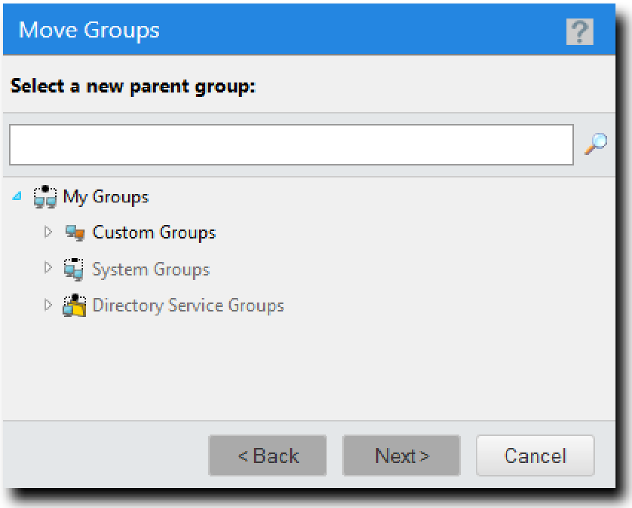
Move groups from the ***Group Membership*** view on the ***Groups*** page.

Note: When moving a group, if the group is configured to inherit agent policies, roles, or any other settings, the group inherits those values from its new parent.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Group Membership**.
3. From the **Browser**, select the parent group of the group you want to move.
4. Select the group you want to move.
5. Click **Move**.

   Note: You cannot move groups in **System Groups** or **Directory Service Groups**.

   Step Result: The ***Move Groups*** dialog opens.



Move Groups

Select a new parent group:

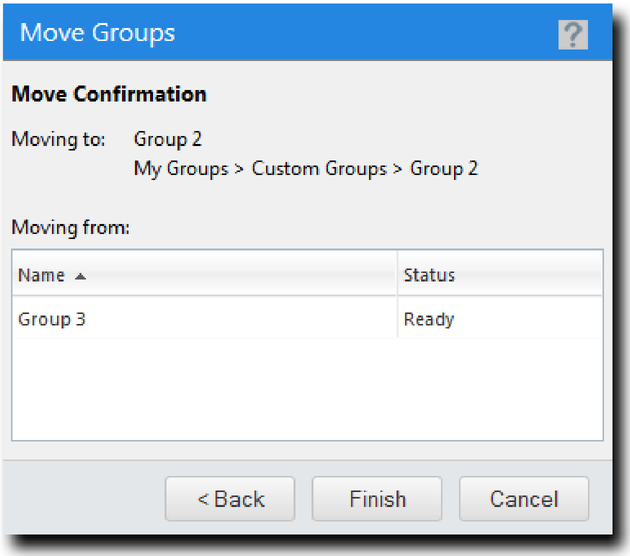
Figure 59: Move Groups Dialogs

6. Select a new parent group.

7. Click **Next**.

   Step Result: The group is moved to the new parent group.

   > **Note:** If the group you are moving contains a child hierarchy, those groups are moved as well.



Move Groups

Move Confirmation

Moving to: Group 2
My Groups > Custom Groups > Group 2

Moving from:

Name ▲	Status
Group 3	Ready

Figure 60: Move Confirmation

8. Click **Finish**.
9. Click **Close**.

Result: The select group is moved to its new place in the group hierarchy.

Exporting Group Membership View Data

To export information displayed in the ***Group Membership*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 39.

The Endpoint Membership View

This view lists the endpoints that hold membership in the selected group. If the group selected is a custom group, you can also use this view to add endpoints. Use this view to manage endpoints assigned to the selected group. This view contains features similar to those available from the ***Endpoints*** page.

For additional information about this view, refer to The All Tab (Groups Page) on page 208.

The All Tab (Groups Page)

Use the ***All*** tab to perform tasks related to group endpoints.

The All Tab Toolbar (Groups Page)

The ***All*** tab toolbar contains buttons for you to perform tasks and functions for managed endpoints.

The following table describes the toolbar functions used in the ***All*** tab, available on the ***Groups*** page ***Endpoint Membership*** view.

Table 82: All Tab Toolbar (Groups Page)

Button	Description
Membership	Adds or removes managed endpoints to or from the selected group. For additional information, refer to Adding Endpoints to a Group on page 212.
Manage Agents... (menu)	Opens the Manage Agents menu.
Install Agents... (**Manage Agents...** menu item)	Installs agents on selected endpoints. For additional information, refer to Installing Agents by Agent Management Job on page 214.
Uninstall Agents... (**Manage Agents...** menu item)	Deletes agents from selected endpoints. For additional information, refer to Uninstalling Agents by Agent Management Job on page 215.
Download Agent Installer... (**Manage Agents...** menu item)	Downloads an agent installer to the endpoint used to access Ivanti Endpoint Security. For additional information, refer to Downloading the Agent Installer on page 215.
Delete	Deletes a disabled endpoint. For additional information, refer to Deleting Endpoints (Groups Page) on page 216.
Enable	Enables a disabled endpoint. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 217.
Disable	Disables an enabled endpoint. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 217.
Agent Versions...	Defines the endpoint agent version. For additional information, refer to Defining the Endpoint Agent Version (Groups Page) on page 215.
Manage Modules...	Opens the ***Add/Remove Modules*** dialog. Use this dialog to toggle module-specific agent functions. For additional information, refer to Managing Endpoint Modules (Groups Page) on page 218.

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The All Tab List (Groups Page)

The ***All*** tab lists the operating system, identification, agent, and module information for group endpoints.

The following table describes the columns within the ***All*** tab list.

Table 83: All Tab List Columns

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

Column	Description
Agent Status	The status of the Ivanti Endpoint Security Agent on the endpoint. Values include: **Online** — The agent is communicating with the Ivanti Endpoint Security Server regularly. See Configuring the Agents Tab on page 60 for more information on configuring default agent behavior. **Offline** — The agent has not communicated with Ivanti Endpoint Security Server within the check in interval. In an `Offline` status, the agent still enforces all policies. **Note:** A **Warning** (⚠) icon next to an `Offline` status indicates that the Endpoint Distribution Service (EDS) server the endpoint connects to is offline. Click the icon to find out additional status details. **Disabled** — The agent is disabled by a Ivanti Endpoint Security administrator. It doesn't enforce module policies nor complete tasks.
Last Connected Date (Server)	Exported comma separated value (`.csv`) file only. Last date and time (in server local time) when the endpoint communicated with the Endpoint Distribution Service (EDS) server.

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td><b>EDS Status</b></td><td>Exported comma separated value (<code>.csv</code>) file only. Status of the Endpoint Distribution Service (EDS) server. The following list defines column values:
<table>
<tr><td><b>Started</b></td><td>EDS server has started and is in an operational state accepting workloads.</td></tr>
<tr><td><b>Starting</b></td><td>EDS server is in the process of starting its service.</td></tr>
<tr><td><b>Stopped</b></td><td>EDS server has stopped and is not accepting workloads.</td></tr>
<tr><td><b>Stopping</b></td><td>EDS server is in the process of stopping so as to not accept workloads.</td></tr>
<tr><td><b>Offline</b></td><td>EDS server is offline as it has not contacted the database in the configured amount of time.</td></tr>
</table></td></tr>
<tr><td><b>Operating System</b></td><td>The operating system that the endpoint uses.</td></tr>
<tr><td><b>Agent Version</b></td><td>The version of the Ivanti Endpoint Security Agent installed.
<b>Note:</b> A ⚙ icon next to an agent version indicates that an upgrade of the agent was requested. Click the icon to display additional agent version details.</td></tr>
<tr><td><b><i>Module</i> Installed</b></td><td>Indicates whether a module is installed on the endpoint. A new <b><i>Module</i> Installed</b> column is added for each module installed on your Ivanti Endpoint Security Server. The following list defines column entry values:
<table>
<tr><td><b>Yes</b></td><td>The module is installed.</td></tr>
<tr><td><b>No</b></td><td>The module is not installed.</td></tr>
<tr><td><b>Pending Install</b></td><td>The module is in the process of installing.</td></tr>
<tr><td><b>Pending Uninstall</b></td><td>The module is in the process of uninstalling.</td></tr>
<tr><td><b>Error</b></td><td>There was an error while installing or uninstalling the module. Click the for additional information about the error.</td></tr>
<tr><td><b>Expired</b></td><td>The module license has expired.</td></tr>
</table></td></tr>
</table>

Adding Endpoints to a Group

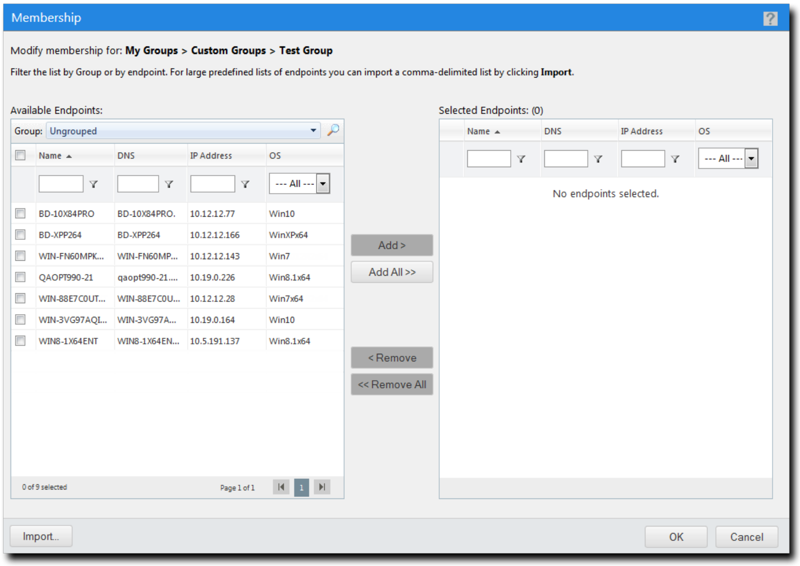
You can manage endpoints collectively by adding them to custom groups.

Add endpoints to a group from the ***Groups*** page.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **Groups** tree, right-click a group in the **Custom Groups** hierarchy and select **Add endpoints to group**.

    Remember: Endpoints can only be added to custom groups.

    Step Result: The ***Membership*** dialog opens.



Membership

Modify membership for: **My Groups** > **Custom Groups** > **Test Group**

Filter the list by Group or by endpoint. For large predefined lists of endpoints you can import a comma-delimited list by clicking **Import**.

Available Endpoints:

Group: Ungrouped

□	Name	DNS	IP Address	OS
				--- All ---
□	BD-10X84PRO	BD-10X84PRO.	10.12.12.77	Win10
□	BD-XPP264	BD-XPP264	10.12.12.166	WinXPx64
□	WIN-FN60MPK...	WIN-FN60MP...	10.12.12.143	Win7
□	QAOPT990-21	qaopt990-21....	10.19.0.226	Win8.1x64
□	WIN-88E7C0UT...	WIN-88E7C0U...	10.12.12.28	Win7x64
□	WIN-3VG97AQI...	WIN-3VG97A...	10.19.0.164	Win10
□	WIN8-1X64ENT	WIN8-1X64EN...	10.5.191.137	Win8.1x64

0 of 9 selected

Page 1 of 1

Selected Endpoints: (0)

Name	DNS	IP Address	OS
			--- All ---

No endpoints selected.

Figure 61: Membership Dialog

3. Add endpoints to the group.
    a) [Optional] To filter the endpoints that are listed down to a pre-existing group, select a **Group** from the drop-down list and click 🔍.
    b) [Optional] To filter the endpoints that are listed, type filter criteria in the table fields and click ▽ to select an operator.

c) Select endpoints and click **Add**.

Tip:

- Click **Add All** to include the entire list.
- You can add endpoints to the group by importing them from a list. Click **Import** to use this feature.
- Use the **Remove** and **Remove All** buttons to remove endpoints from the list.

d) Review the list of endpoints to confirm it is correct.

4. Click **OK**.

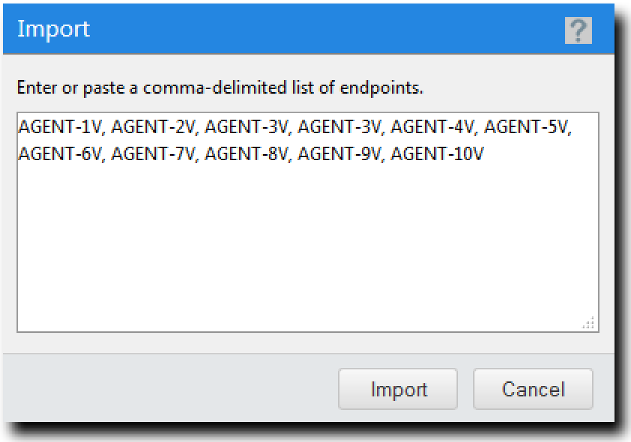
Result: The selected endpoints are added to the group. Select **Endpoint Membership** from the **View** list to confirm they are added.

Importing Endpoints into Groups

If you are adding a large number of endpoints to a group, importing a list of endpoints can be faster than than selecting them individually within the ***Membership*** dialog.

Import Rules

- You can only import endpoints using their host names. IP Addresses cannot be imported.
- You must separate each endpoint with a comma.



Enter or paste a comma-delimited list of endpoints.

AGENT-1V, AGENT-2V, AGENT-3V, AGENT-3V, AGENT-4V, AGENT-5V, AGENT-6V, AGENT-7V, AGENT-8V, AGENT-9V, AGENT-10V

Figure 62: Import List Example

Tip: You can use Ivanti Endpoint Security to easily obtain a list of endpoints to import. To create a list:

1. Open the ***Endpoints*** page (**Manage** > **Endpoints**).
2. Using the page filters to display the endpoints you want to add to your group.
3. Click **Export**.
4. Open the exported .csv file and copy and paste the endpoint names into the **Import** dialog. Add a comma between each name.

Installing Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of installing an agent on endpoints using an Agent Management Job. To create an Agent Management Job that installs agents from the ***Endpoint Membership*** view, select **Manage Agents** > **Install Agents** from the toolbar.

For additional information, refer to Installing Agents by Agent Management Job on page 109.

Uninstalling Agents by Agent Management Job

Within Ivanti Endpoint Security, there are multiple methods of uninstalling an agent from endpoints using an Agent Management Job. To create an Agent Management Job that uninstalls agents from the ***Endpoint Membership*** view, select **Manage Agents** > **Uninstall Agents** from the toolbar.

To pre-populate the ***Schedule Agent Management Job - Uninstall Wizard*** **target** list, first select the desired group from the **Browser**, and then select the check box associated with the desired endpoints.

For additional information, refer to Uninstalling Agents by Agent Management Job on page 122.

Downloading the Agent Installer

You can install an agent on a local endpoint from the ***Endpoint Membership*** view.

To download an agent installer from the ***Endpoint Membership*** view, select **Manage Agents** > **Download Agent Installer** from the toolbar. For additional information, refer to Downloading the Agent Installer on page 173.

Defining the Endpoint Agent Version (Groups Page)

From the ***Groups*** page, you can upgrade your endpoints to a newer version of the agent.

Define agent version(s) for group endpoints from the ***Groups*** page ***Endpoint Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Select the endpoints on which you want to define agent version(s).
5. Click **Agent Versions**.

   Step Result: The ***Manage Agent Versions*** dialog opens.

6. Define the agent version(s).

   Use one of the following methods:

Method	Steps
To define a standard agent version for all listed endpoints:	- From the **Select One** list, select an agent version. - Click **Apply to All Agents**.
To define an agent version for each endpoint:	Select an agent version from the **Agent Version** list for each endpoint.

> **Note:** The agent versions available for selections are defined from the ***Options*** page. For additional information, refer to Configuring the Agents Tab on page 60.

7. Click **OK**.

Result: The ***Manage Agent Versions*** dialog closes. If an agent version other than the defined version is installed on the endpoints, the defined version is installed over the previous version.

Deleting Endpoints (Groups Page)

From the ***Groups*** page, you can delete an endpoint from the Ivanti Endpoint Security database.

Prerequisites:

The endpoints you want to delete must be disabled. For additional information, refer to Enabling or Disabling Ivanti Endpoint Security Agents within a Group on page 217.

Delete endpoints from the ***Endpoint Membership*** view.

> **Note:** Deleting an endpoint removes its record from the Ivanti Endpoint Security database, but it does not remove the agent on the endpoint.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.

   > **Note:** You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy that is disabled.

4. Select the endpoint listings you want to delete.
5. Click **Delete**.

   Step Result: A confirmation dialog opens.

6. Click **OK** to confirm the deletion.

Result: The selected endpoints are deleted.

Enabling or Disabling Ivanti Endpoint Security Agents within a Group

Disabling an agent deactivates its functionality. Disabled agents do not contact the Ivanti Endpoint Security server, use Ivanti Endpoint Security features, or occupy Ivanti Endpoint Security licenses. Disable an agent if it will be unused for a prolonged period. You can re-enable an agent at any time.

Enable or disbale an agent within a group from the ***Endpoint Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. From the **Browser**, select a group within either the **Custom Groups** or **Systems Groups** hierarchy.
4. If necessary, define filter criteria and click **Update View**.
5. Select the endpoints on which you want to enable or disable the agent:

   Use one of the following methods.

Method	Steps
To enable a disabled endpoint:	Click **Enable**.
To disable an enabled endpoint:	1. Click **Disable**. 2. Acknowledge the disablement by clicking **OK**.

Result: The applicable agents are enabled or disabled. The ***Endpoint Membership*** view and ***Endpoints*** page reflect your changes.

> **Note:** Disabling an agent within a group is not limited to the group; the agent is completely disabled within the Ivanti Endpoint Security.

Enabling or Disabling Endpoint Modules within a Group

From the groups page, you can disable an agent's individual modules. Disable an endpoint's module component if it will be unused for a prolonged period. You can re-enable the endpoint module at any time.

Prerequisites:

Endpoints must have the applicable agent module installed, and the endpoint must be licensed for the agent module. For additional information, refer to Installing Endpoint Modules on page 177.

Enable or disable a module within a group from the ***Endpoint Membership*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.

2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Select the tab for the module you want to enable or disable.

   Tip: The tabs available depend on which modules you have purchased and installed.

5. [Optional] Define filter criteria and click **Update View**.
6. Select the check box(es) for endpoint(s) with module components you want to enable or disable.
7. Enable or disable the selected endpoint module(s):

   Use one of the following methods.

Method	Steps
To enable a disabled module component:	Select **Enable** > **Enable Module**.
To disable an enabled endpoint:	**1.** Select **Enable** > **Enable Module**. **2.** Acknowledge the disablement by clicking **OK**.

Result: The applicable endpoint module components are enabled or disabled. The ***Endpoint Membership*** view and ***Endpoints*** page reflect your changes.

Note: Disabling an endpoint module within a group is not limited to the group; the endpoint module is completely disabled within the Ivanti Endpoint Security system.

Managing Endpoint Modules (Groups Page)

You can manage endpoint module licences from the ***Groups*** page. Using this feature allows you control which modules apply to a particular endpoint.

Manage modules for individual endpoints from the ***Groups*** page ***Endpoint Membership*** view.

1. Select **Manage** > **Groups**.
2. From the **View** list, select **Endpoint Membership**.
3. Select a group from the directory tree.

   Note: You may select a group that is in either the **Custom Groups** or **Systems Groups** hierarchy.

4. Select the checkbox(es) associated with the endpoints for which you want to manage modules.
5. Click **Manage Modules**.

   Step Result: The ***Add/Remove Modules*** dialog opens.

6. Manage modules for each endpoint.
    - To activate a module for a particular endpoint, select the module check box for the applicable endpoint.
    - To deactivate a module for a particular endpoint, clear the module check box for the applicable endpoint.

    Tip: Select or clear the **Select All** check boxes associated with a module to globally toggle a module for all endpoints.

7. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes. The agent features for each edit are updated during the next Discover Applicable Updates task.

Exporting Endpoint Membership View Data

To export information displayed in the ***Endpoint Membership*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 39.

The Agent Policy Sets View

After creating agent policy sets, you can apply them to a group using the ***Agent Policy Sets*** view. From this view you can add or remove existing agent policy sets to or from the selected group. Additionally, you can create policy sets from this view. However, this view, unlike the ***Agent Policy Sets*** page, does not let you edit policy sets or view their details. This view is only applicable to agent policy sets.

For additional information about agent policy sets, refer to About Agent Policies and Agent Policy Sets on page 237.

The Agent Policy Sets View Toolbar

This toolbar allows you to manage Agent Policy Sets for groups.

Table 84: Agent Policy Sets View Toolbar

Button	Function
Assign	Assigns an Agent Policy Set to the selected group and its child groups. For additional information, refer to Assigning an Agent Policy Set to a Group on page 220.
Unassign	Unassigns an Agent Policy Set to the selected group and its child groups. For additional information, refer to Unassigning an Agent Policy Set from a Group on page 221.
Create...	Creates an Agent Policy Set. For additional information, refer to Creating an Agent Policy Set (Groups Page) on page 222.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Agent Policy Sets View List

This list itemizes all agent policy sets and policy details assigned to the selected group.

View the ***Agent Policy Sets View*** list from the ***Groups*** page. The following table describes ***Agent Policy Sets View*** list.

Column	Description
Action	The **Unassign** icon indicates the Agent Policy Set may be unassigned. **Note:** You may use the **Unassign** icon to remove a policy set from the selected group. For additional information, refer to Unassigning an Agent Policy Set from a Group on page 221. The **Unassign Disabled** icon indicates the Agent Policy Set cannot be unassigned. **Note:** The **Unassign Disabled** icon indicates the policy is inherited. An inherited Agent Policy Set can not be unassigned from the group.
Name	The name of the Agent Policy Set. **Note:** You may select the **Name** column to sort the Agent Policy Set list.

Assigning an Agent Policy Set to a Group

Assigning an Agent Policy Set to a group defines functional rules for the group.

Prerequisites:

Create an Agent Policy Set. Refer to Creating an Agent Policy Set (Groups Page) on page 222 for details.

Assign Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 237 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Assign**.

   Step Result: The **Select a Policy Set** list becomes active.

5. Select an agent policy set from the **Select a Policy Set** list.
6. Click the **Save** icon (💾) to save your changes.

   Step Result: The **Select a Policy Set** list closes and your policy is assigned.

   Note: The **Cancel** icon (☒) cancels your changes and any edits are not saved.

Result: The policy set is saved and associated with the group.

Unassigning an Agent Policy Set from a Group

When desired, you can unassign an Agent Policy Set from a group.

Prerequisites:

An Agent Policy Set is assigned. Refer to Assigning an Agent Policy Set to a Group on page 220 for details.

Unassign the Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 237 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Remove the desired policy sets.

   Use one of the following methods.

Method	Steps
To remove one Agent Policy Set:	Click the **Unassign** icon (⟲) associated with the Agent Policy Set you want to remove.
To remove multiple Agent Policy Sets:	**1.** Select the check boxes associated with the Agent Policy Sets you want to remove. **2.** From the toolbar, click the **Unassign** button.

   Note: An **Unassign Disabled** icon indicates you cannot remove an inherited Agent Policy Set. Instead, you must change the group policy inheritance setting or remove the inherited policy set from the parent group. Refer to *Policy Inheritance* in Editing Group Settings on page 232 for additional information.

   Step Result: A dialog appears, prompting you to acknowledge the removal.

5. Click **OK**.

   Step Result: The selected policy set(s) are removed and the dialog closes.

Result: The Agent Policy Set(s) are no longer associated with the group.

Creating an Agent Policy Set (Groups Page)

You can create agent policy sets from the ***Agent Policy Set*** view. Agent policy sets are collections of values that can be assigned to groups to regulate how agents behave.

Note: When creating an agent policy set from the ***Agent Policy Set*** view, the created policy set will be immediately applied to the group selected in the directory tree.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Set**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Create**.

   Step Result: The ***Create Agent Policy Set*** dialog opens.

5. Type the applicable information in the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.

Field Name	Type
Policy Set Description	A description of the Agent Policy Set (optional).

6. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 239.

Option	Description
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.

7. Define the **Agent Logging** options.

   The following table describes each option.

Option	Step
Logging level (button)	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 252.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

8. Define the **Ivanti Endpoint Security Agent Communication** options.

   The following table describes each option.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *True*.
Send interval (list)	Select the amount of time that the agent should wait before sending an event to the Ivanti Endpoint Security server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval (field and list)	Type and select the amount of time that the agent should delay before reattaching events from the Ivanti Endpoint Security Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.

Options	Step
Timeout interval **(field and list)**	Type and select the amount of time the agent should stay attached to the Ivanti Endpoint Security server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval **(field and list)**	Type and select the amount of time between agent check-ins with the Ivanti Endpoint Security server (1 minute-1 day). A value of *15 minutes* is the default setting.

9. Define the **Ivanti Endpoint Security Agent Notification Defaults** options.

   The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the ***Agent Control Panel*** (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**). **Note:** • This policy will not take effect until the agent is restarted. • This policy can hide only the Ivanti Endpoint Security Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***. • This policy cannot hide the Patch Agent or the Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the ***Agent Control Panel*** are hidden or accessible to an endpoint user after logging on (**True** or **False**).

10. Define the **Reboot Behavior Defaults** option.

    An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

    a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.

Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

11. Click **Save**.

Result: Your agent policy set is saved and assigned to the selected group. You can also assign the agent policy set to other endpoint groups or edit the set.

Exporting Agent Policy Sets View Data

To export information displayed in the ***Agent Policy Sets*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 39.

The Roles View

This view lists the user roles that can access the selected group. This view is similar to the ***Roles*** page, but applies only to the selected group rather than the entire system. From this view, you can manage which roles have access to the selected group.

The Roles View Toolbar

This toolbar contains buttons that let you add (or remove) roles that can access the selected group. You can also use it to create new user roles.

The following table describes the functionality of each **Roles** view toolbar button.

Table 85: Roles View Toolbar

Button	Function
Add	Adds a role to the group. For additional information, refer to Adding a Role to a Group on page 226.
Remove	Removes a role from the group. For additional information, refer to Removing a Role from a Group on page 227.
Create...	Creates a new user role. For additional information, refer to Creating User Roles (Roles View) on page 228.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Roles View List

This list displays the roles that can access the selected group. Use the **Action** column to remove user roles. Additionally, you can filter this table using the filter row.

The following table describes each **Roles** view list column.

Table 86: Roles View List

Column	Description
Action	Contains a **Remove** icon. Use this icon to remove a role from the associated group.
Status	Contains an icon that indicates the type of role. For additional information, refer to one of the following topics: • Predefined System Roles on page 274 • Custom Roles on page 275
Name	Indicates the name of the user role.
Source Group	Indicates the group from which the role was created.

Adding a Role to a Group

Add a user role to a group to grant it group access. If the selected group's **Policy inheritance** setting is set to **true**, the added user role will also be able to access the selected group's descendant groups.

Add roles to a group from the ***Roles*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.
4. Click **Add**.

5. Select a role from the **Select a Role** list.

   Select from the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

   Note: ***Custom Role(s)*** are only available if a custom role has been created.

6. Click the **Save** icon.

Result: The role is saved and associated with the group.

Removing a Role from a Group

Remove a user role from a group to deny its associated users group access. If the selected group has **policy inheritance** set to **true**, removing a role will remove the role from the selected group's descendant groups as well.

Remove user roles from a group using the ***Roles*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.
4. Remove roles from the group.

   Use one of the following methods.

Method	Steps
To remove a single role:	Click the **Remove** icon associated with the role you want to remove from the group.
To remove multiple roles:	**1.** Select the check boxes associated with the roles you want to remove from the group. **2.** From the toolbar, click **Remove**.

Note: Inherited roles cannot be removed. To remove inherited roles, either edit the group's inheritence policy or remove the roles from the applicable parent group. To understand group policy inheritance and its effects, refer to Defining Agent Policy Inheritance Rules on page 240.

Step Result: A dialog displays, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

Result: The role is removed and is no longer associated with the group.

Creating User Roles (Roles View)

Custom roles let you select individual access rights, accessible groups, and accessible endpoints for that role. Create a custom role when predefined system roles do not contain the access rights needed for a particular user. Creating a custom role is also useful when you require a role that can only access specific groups or endpoints.

You can create roles from the ***Roles*** view as well as the ***Roles*** tab.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Roles**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Create**.

   Step Result: The ***Create Role*** dialog appears with the ***Information*** tab selected by default.

5. Type a name in the **Name** field.
6. Type a description in the **Description** field.
7. Select a role template from the **Role Template** list.

   Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.

8. Select the ***Access Rights*** tab.
9. Select or clear the desired access rights.

   For additional information, refer to Predefined System Roles on page 274.

   Tip: Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

10. Select the ***Groups*** tab.
11. Assign the desired accessible endpoint groups to the role.

    Use one of the following methods to assign groups.

Method	Steps
To assign individual groups:	1. From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign. 2. Click **Assign**.

Method	Steps
To assign all groups:	Click **Assign All**.

Tip: Remove groups using **Remove** and **Remove All**.

12. Select the ***Endpoints*** tab.

13. Assign the desired accessible endpoints to the role.

Use one of the following methods to assign endpoints.

Method	Steps
To assign individual endpoints:	**1.** From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign. **2.** Click **Assign**.
To assign all endpoints:	Click **Assign All**.

Tip: Remove endpoints using **Remove** and **Remove All**.

14. Click **OK**.

Result: The new role is saved and assigned to the selected group.

> **Note:** A created role can be edited from the ***Users and Roles*** page ***Roles*** tab. Refer to Editing User Roles on page 284.
>
> In addition, a new role can be assigned to users. Refer to Editing Users on page 265.

Exporting Roles View Data

To export information displayed in the ***Roles*** view list to a comma separated value (`.csv`) file, click the toolbar **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 39.

The Dashboard View

Similar to the ***Home*** page dashboard, the ***Dashboard*** view displays widgets depicting Ivanti Endpoint Security activity. However, unlike the ***Home*** page dashboard, the ***Dashboard*** view widgets include only information about endpoints within the selected group and its child hierarchy.

Widgets graphs and information are generated based on the latest Ivanti Endpoint Security server and agent data available.

Note: The widgets displayed in the ***Dashboard*** view include data from the selected group's child hierarchy. Configuration changes made to the dashboard settings apply to all groups; not just the selected group.

Group Dashboard Widgets

Most widgets available on the ***Home*** page dashboard are also available from the ***Dashboard*** view. The data depicted on each dashboard changes according to which group is selected.

The following table describes the available widgets.

Table 87: Group Dashboard Widgets

Widget	Description
Agent Module Installation Status	Displays the installation and licensing statistic of each agent module.
Agent Status	Displays all agents grouped by status.
Discovery Scan Results: Agents	Displays the total number of agent-supported endpoints discovered in the last-run Discovery Scan Job and identifies how many have an agent installed.

Tip: For information about how to edit the group dashboard, refer to Editing the Dashboard on page 44.

Widget Setting and Behavior Icons

Setting and behavior icons are user interface controls that let you manage widgets and the dashboard within the ***Groups*** view. Click these controls to maximize, minimize, hide, and refresh widgets.

The following table describes each icon action.

Table 88: Widget Setting and Behavior Icons

Icon	Action
🔧	Opens the ***Dashboard Settings*** dialog.

Icon	Action
🖨	Opens the dashboard in print preview mode.
⊟	Collapses the associated widget.
▣	Expands the associated collapsed widget.
☒	Hides the associated widget.
🔄	Refreshes the associated widget (or the entire dashboard).

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

Previewing and Printing the Dashboard

As with the ***Home*** page dashboard, you can preview and print the ***Group*** page ***Dashboard*** view. ***Dashboard*** view widgets display data that applies only to the selected group.

To preview the ***Dashboard*** view, select the applicable group from the **Browser** and click the print icon.

For additional information, refer to Previewing and Printing the Dashboard on page 44.

Editing the Dashboard

Just as with the ***Home*** page dashboard, you can edit the widgets displayed on the ***Group*** page ***Dashboard*** view. ***Dashboard*** view widgets display data that only applies to the selected group.

To edit the widgets displayed within the ***Dashboard*** view, select the applicable group from the **Browser** and click the edit icon.

For additional information, refer to Editing the Dashboard on page 44.

The Settings View

This view lets you edit various basic settings for the selected group. The settings in this view are miscellaneous settings that cannot be grouped with other settings.

The following table describes ***Settings*** view button functions.

Table 89: Settings View Toolbar

Button	Function
Save	Saves the settings defined in the page.

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

Editing Group Settings

If different settings are required, you can edit the default settings for a group. Modifying group settings not only modifies settings for the selected group, but also potentially determines settings for descendant groups.

Modify group settings from the ***Settings*** view.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Settings**.
3. Select the desired group from the directory tree.
4. [Optional] Under **General**, edit the following as necessary.

Option	Description
Group Name (field)	The group name. **Note:** Only `Custom` group names can be edited.
Distinguished Name	A system-created group name that represents the group's parent hierarchy. **Note:** The **Distinguished Name** cannot be edited.
Group Description (field)	The group description.

5. Under **Policy**, edit the following lists as necessary.

List	Description
Policy Inheritance	Defines whether the group inherits the agent policies assigned to the group's parent hierarchy. A `True` value sets the group to inherit its parent hierarchy's agent policy settings. **Note:** To understand agent policy inheritance and its effects, refer to Defining Agent Policy Inheritance Rules on page 240.
Policies Enabled	Defines whether agent policies may be assigned to the group. A `True` value allows users to assign agent policies directly to the group.

6. Under **Other**, edit the following fields as necessary.

Field	Description
Group Owners	User-defined email addresses indicating the owners of the group.
Source Groups (button)	User-defined group or groups whose agents are dynamically assigned to the group. For additional information, refer to Assigning a Source Group to a Custom Group on page 235.

7. Click **Save**.

Result: The new settings are saved and applied to the group.

Defining Source Groups

Source groups are groups that automatically assign managed endpoints to a associated custom group. Use a source group to maintain multiple endpoint memberships by editing only a single group. This feature simplifies maintenance of endpoint membership among groups.

When working within the ***Groups*** page ***Settings*** view, you can assign the selected view a source group. By assigning the selected group a source group, the selected group will be modified when the source group has endpoints added or removed. Source groups only affect endpoint membership, not group agent policies and settings.

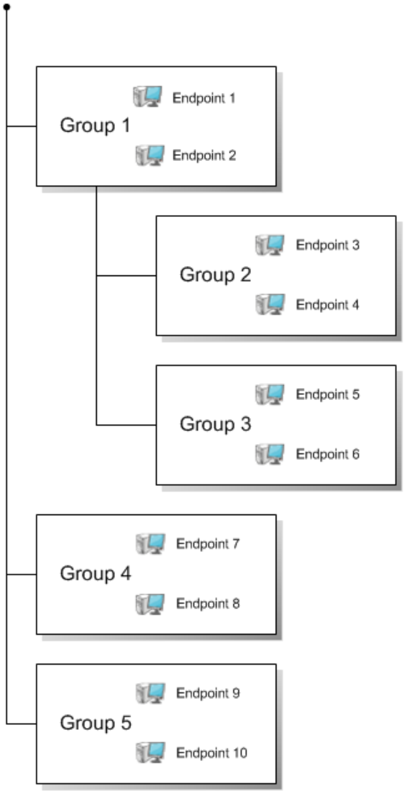


Figure 63: Source Group Diagram

When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. Source groups can only be assigned to custom groups.

The preceding diagram and the following bullets clarify how group sources operates.

- If group 3 uses group 5 as a source group, then group 3 would include endpoints 9 and 10, as well as endpoints 5 and 6.
- Because group 3 is in group 1's hierarchy, group 1 also includes endpoints 9 and 10.
- If group 4 uses group 1 as a source group, group 4 would include endpoints 7 and 8 (through direct assignment), endpoints 1 and 2 (through a directly assigned source group), endpoints 3, 4, 5, and 6 (through group 1's hierarchy), and endpoints 9 and 10 (through an indirectly assigned source group for [group 5 is a source group for group 3]).

Assigning a Source Group to a Custom Group

When a custom group is created, you can assign it a *source group*, which is a group that automatically assigns managed endpoints to associated groups. For example, if you assign *Group 1* as a source group to *Group 2*, any agents assigned to *Group 1* are automatically assigned to *Group 2*.

Assign a group a source group from the ***Settings*** view.

Note: Source groups can only be assigned to custom groups.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Settings**.
3. Select a custom group from the directory tree.
4. Under **Other**, click **Modify**.

   If necessary, scroll to the button.

   Step Result: The ***Edit Source Groups*** dialog opens.

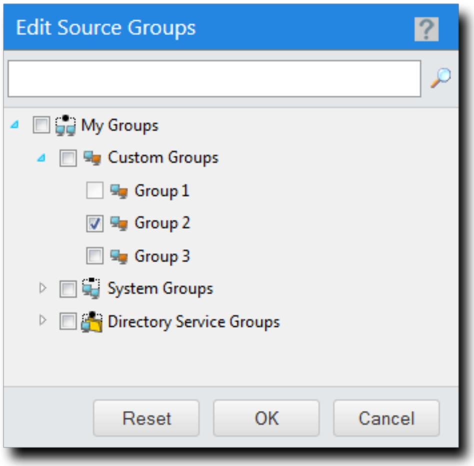


Figure 64: Edit Source Groups Dialog

5. Expand the directory tree or use the search field to locate the group you want to use as a source.
6. Select the groups you want to use as sources.

   Note: When selecting a source group, all endpoints within the source group's child hierarchy are included, regardless of whether the child groups are selected. Additionally, if the source group (or any of its child groups) has a source group, those endpoints are also included. For additional information, refer to Defining Source Groups on page 233.

7. Click **OK**.

Result: The custom group now uses the selected groups as sources. As new agents are added to (or removed from) the source group, they are also added to (or removed from) the custom group.

Exporting Settings View Data

To export information displayed in the ***Settings*** view to a comma separated value (`.csv`) file, click **Export**. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 39.

Chapter 11

Managing Agent Policy Sets

In this chapter:

- The Agent Policy Sets Page
- Working with Agent Policy Sets

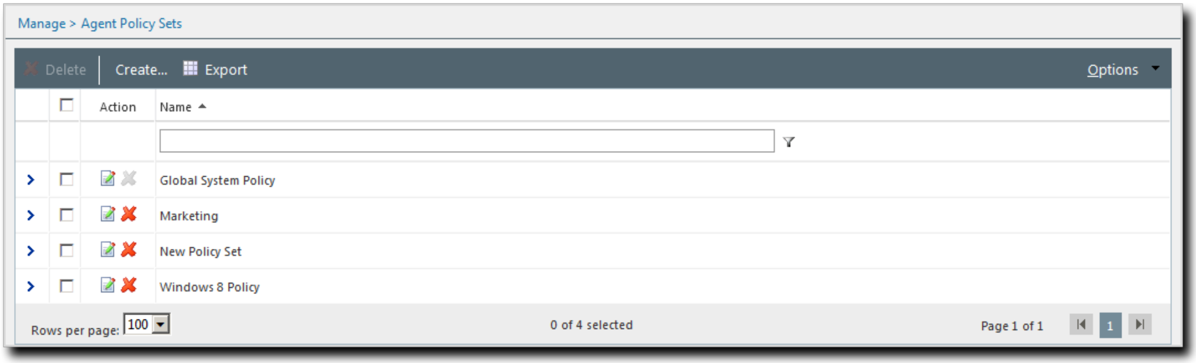
Use *Agent Policy Sets* to control agent behavior. Agent Policy Sets are basic rules which define how agents behave.

Apply the *Agent Policy Sets* to groups to implement your policies to groups. There is a policy for every agent function.

The Agent Policy Sets Page

You can control agent behavior by creating and assigning Agent Policy Sets. Use the ***Agent Policy Sets*** page to define agent rules of behavior.

You can access this page at any time from the navigation menu.



Manage > Agent Policy Sets

	☐	Action	Name ▲
›	☐		Global System Policy
›	☐		Marketing
›	☐		New Policy Set
›	☐		Windows 8 Policy

Rows per page: 100

0 of 4 selected

Page 1 of 1

Figure 65: Agent Policy Sets Page

About Agent Policies and Agent Policy Sets

Agent Policies are rules that govern agent behavior. Agent Policy Sets are a collections of agent policy values.

Assign agent policies to groups using the *Agent Policy Sets* view. Based on group membership, agents operate according to the values in assigned Agent Policy Sets. Assignment of Agent Policy Sets is optional.

Groups without assigned Agent Policy Sets have their behavior defined by the **Global System Policy**. The **Global System Policy** does the following:

- Defines behavior for groups with no assigned policy set.
- Defines policy values for incomplete agent policy sets.

When agents holding multiple group memberships are assigned conflicting agent policy values, they are resolved with conflict resolution rules. These rules are a set of protocols that determine which policy value an agent uses when conflicts occur. For additional information, refer to Defining Agent Policy Conflict Resolution on page 240.

About Agent Hardening

Agent Policy Sets include **Agent Hardening** policies, which are policies used to prevent unauthorized Ivanti Endpoint Security Agent removal.

Agent Hardening (when set to On)

- It prevents the Ivanti Endpoint Security Agent installation location (`C:\Program Files\HEAT\EMSSAgent` by default) from being renamed, edited, or deleted.
- The Agent is *hardened*, meaning the agent cannot be intentionally or unintentionally modified.
- When hardening is in place, you can still upgrade or uninstall the agent after entering the **agent uninstall password** or the **global uninstall password**, which is only necessary when modifying the agent locally from the endpoint.

  For additional information about defining **Agent Hardening** policies, refer to the following topics:

  - Creating an Agent Policy Set on page 244
  - Editing an Agent Policy Set on page 247

Global uninstall password

Important: The **Global uninstall password** option is only available when editing the **Global System Policy** agent policy set. Refer to Changing the Global Uninstall Password on page 250 for additional information.

The **Global uninstall password** is a universal password that temporarily disables agent uninstall protection. This password works on all network endpoints. You are prompted for this password when manually upgrading or uninstalling hardened agents.

Note:

- Ivanti *does not* recommend providing end users with the global uninstall password in uninstall scenarios. The **Global uninstall password** should be used by the Ivanti Endpoint Security Administrator only.
- In the event an end user needs to uninstall the Ivanti Endpoint Security Agent, provide them with the **Agent uninstall password**, a password that works only for their endpoint. For additional information, refer to Viewing the Agent Uninstall Password on page 186.

Viewing the Agent Policy Sets Page

Navigate to this page to view Agent Policy Sets and their policy settings. Expand policy sets to view the individual policy settings.

You can access this page any time using the navigation menu.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. [Optional] Complete a task listed in Working with Agent Policy Sets on page 244.

Defining Agent Policy Inheritance Rules

You can configure a group to inherit policies from its parent hierarchy using the **Policy inheritance** setting.

Because a group can inherit policies and have them directly assigned, policy conflicts may arise. The following rules apply when a group has **Policy Inheritance** set to `True`:

1. Any conflicting policies are assigned to the parent, but not the child. Conflicting policies are resolved at the parent level using the conflict policy resolution rules.
2. Agent Policy Set values directly assigned to a group supersede inherited Agent Policy Set values.
3. Any conflicting policies that are assigned directly to the child group are resolved by conflict resolution rules.
4. Any Agent Policy Set values that are undefined by the group's directly assigned policy are defined by the parent's group policy.
5. Policy values still undefined are defined by the **Global System Policy** set.

For more information on how to enable a group's *Policy Inheritance* setting, refer to Editing Group Settings on page 232.

For more information on *Conflict Policy Resolution* rules, refer to Defining Agent Policy Conflict Resolution on page 240.

Defining Agent Policy Conflict Resolution

On occasion, a group or endpoint may be assigned two different Agent Policy Sets that have conflicting policies. When this occurs, the system determines which policy to use based on the *Agent Policy Conflict Resolution* rules.

Conflicting policies are resolved in the following order.

1. **Group Policies** - Conflicting policy sets assigned to a group are resolved before conflicting policy sets assigned to an agent are resolved.

   The following rules apply if a group has **Policy Inheritance** set to `False`:

   a. The group does not inherit its parent policy set. Therefore, only policy sets assigned directly to the group require resolution.
   b. Conflicting policies are resolved according to the agent policy conflict resolution rules.

   The following rules apply if a group has **Policy Inheritance** set to `True`:

  a. The group inherits its parent policy set. Any conflicting policy sets that are resolved at the parent level prior to assignment to the child level.
  b. Conflicting policies are assigned directly to the group are resolved using the agent policy conflict resolution rules. Any policy set values assigned directly to a group supersede inherited policy set values.
  c. Finally, any policies that are undefined by direct assignment are defined by inheritance.
2. **Agent Policies** - After resolving the group policies, the conflicting policies assigned to an endpoint (using its group membership) are resolved. The following rules apply:
  a. The resultant policies of all groups the endpoint is a member are resolved according to the agent policy conflict resolution rules.
  b. Any policy values that have not been defined using the agent group membership are populated based on the policy settings defined in the **Global System Policy**.

Note: Conflict resolution rules do not apply to the **Global System Policy**.

The following table defines the rules used when resolving conflicting policy settings:

Table 90: Agent Policy Conflict Resolution Rules

Policy Setting	Resolution
Hide Agent Control Panel	The agent uses true (`Y`).
Core: Download file via HTTP	The agent uses true (`Y`).
Maximum Log File Size	The agent uses the largest log file size value.
Logging Level	The agent uses the most comprehensive logging level value (Trace [`4`] > Diagnostic [`3`] > Normal [`2`] > Error [`1`] > Critical [`0`]).
Agent uninstall protection	The agent uses `On`.
Show alerts on endpoints	The agent uses false (`N`).
Reboot behavior	The agent uses a combination of the most secure value, while still giving the user the best chance to save their work. The items are listed in the following order: • Notify user, user response required before reboot = `0` • Don't notify user, wait for next user-initiated reboot = `2` • Notify user, automatically reboot with 5 minute timer = `1`
Core: Heartbeat Interval	The agent uses the largest heartbeat interval frequency value.
Core: Receive Interval	The agent uses the largest receive interval frequency value.
Core: Timeout Interval	The agent uses the largest timeout interval frequency value.
Core: Send Interval	The agent uses the largest send interval frequency value.

The Agent Policy Sets Page Toolbar

This toolbar contains buttons that allow you to create and edit Agent Policy Sets.

The following table describes each toolbar button.

Table 91: Agent Policy Sets Page Toolbar

Button	Function
Delete	Deletes the selected Agent Policy Set(s). For additional information, refer to Deleting an Agent Policy Set on page 250.
Create...	Creates a new Agent Policy Set. For additional information, refer to Creating an Agent Policy Set on page 244.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Agent Policy Sets Page List

For each agent policy set that you create, an item for that set appears in the ***Agent Policy Sets*** page list. This list names each existing agent policy set and provides access to editing functionality.

Table 92: Agent Policy Sets Page List

Column	Description
Action	Contains **Edit** and **Delete** icons. Use these icons to edit and delete the associated agent policy set. For additional information, refer to the following topics: • Editing an Agent Policy Set on page 247 • Deleting an Agent Policy Set on page 250 **Note:** The **Global System Policy** cannot be deleted.
Name	The name of the agent policy set.

Each item listed on the ***Agent Policy Sets*** page can be expanded to list its individual policy settings. To view agent policy set details from the page list, click the **Rotating Chevron** (>) for the agent policy set, which opens a table containing additional details.

Table 93: Agent Policy Set Details Table

Name	Description
Policy Name	Indicates the unique name of the agent policy set.
Type	Indicates the type of agent policy set (`System` or `User Defined`).
Description	Indicates the description of the agent policy set.
Created By	Indicates the name of the user that created the agent policy set.
Created Date	Indicates the date and time that the agent policy set was created.
Modified By	Indicates the name of the user that last modified the agent policy set.
Modified Date	Indicates the date and time that the agent policy set was last modified.
Agent uninstall protection	Indicates whether agent uninstall protection is on.
Hide agent control panel	Indicates whether the Agent Control Panel is hidden from an endpoint user when they log on to their system. Any dialog or notification launched by the Ivanti Endpoint Security agent will also be hidden until the ***Agent Control Panel*** is started manually using ***Windows Control Panel***.
Reboot behavior	Indicates the reboot behavior. The following values indicate each reboot behavior setting: • Notify user, user response required before reboot = `0` • Notify user, automatically reboot with 5 minute timer = `1` • Don't notify user, wait for next user-initiated reboot = `2`
Download files via HTTP	Indicates whether the Ivanti Endpoint Security Agent downloads files via HTTP rather than HTTPS. All other communication occurs over HTTPS.
Maximum Log File Size	Specifies the maximum size of the Ivanti Endpoint Security agent log before it is deleted.
Logging Level	Indicates the level of detail recorded in the Ivanti Endpoint Security Agent. The following values indicate each logging level: Critical = `0`, Error = `1`, Normal = `2`, Diagnostic = `3`, Trace = `4`.

Name	Description
Show alerts on endpoints	Indicates whether alerts and notifications are shown to endpoint users.
Core: Heartbeat Interval	Indicates the interval at which the Endpoint Service sends a heartbeat to the server (in minutes).
Core: Receive Interval	Indicates the interval at which the Endpoint Service communication receive delay intervals (in seconds).
Core: Timeout Interval	Indicates the interval at which the Endpoint Service communication receive time intervals (in seconds)
Core: Send Interval	Indicates the interval at which the Endpoint Service communication send delay intervals.
Note: This reference table does not list the **Value** contained in the agent policy set details. This column (which appears in the user interface) contains values that agent policies are set to.	

Working with Agent Policy Sets

There are many tasks that you can perform from the ***Agent Policy Sets*** page related to agent policy sets. Some tasks are performed by clicking toolbar buttons, while others are performed by interacting with list items.

- Creating an Agent Policy Set on page 244
- Editing an Agent Policy Set on page 247
- Deleting an Agent Policy Set on page 250
- Changing the Global Uninstall Password on page 250
- Defining Agent Policy Logging Levels on page 252
- Exporting Data for Agent Policy Sets on page 254

Creating an Agent Policy Set

You can create an unlimited number of Agent Policy Sets to define how endpoints behave. Following creation, associate an Agent Policy Set with a group or endpoint to apply policy settings. After installing new modules, additional options are available when creating an Agent Policy Set.

Create an Agent Policy Sets from the ***Create Agent Policy Set*** dialog.

1. Select **Manage** > **Agent Policy Sets**.
2. Click **Create**.

   Step Result: The ***Create Agent Policy Set*** dialog opens.

3. Type the applicable information in the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

4. Define the **Agent Hardening** option.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 239.

Option	Description
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.

5. Define the **Agent Logging** options.

   The following table describes each option.

Option	Step
Logging level **(button)**	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 252.
Maximum log file size **(field)**	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

6. Define the **Ivanti Endpoint Security Agent Communication** options.

   The following table describes each option.

Options	Step
Use HTTP for file download **(list)**	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *True*.
Send interval **(list)**	Select the amount of time that the agent should wait before sending an event to the Ivanti Endpoint Security server (0-5 seconds). A value of *2 seconds* is the default setting.

Options	Step
Receive interval **(field and list)**	Type and select the amount of time that the agent should delay before reattaching events from the Ivanti Endpoint Security Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.
Timeout interval **(field and list)**	Type and select the amount of time the agent should stay attached to the Ivanti Endpoint Security server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval **(field and list)**	Type and select the amount of time between agent check-ins with the Ivanti Endpoint Security server (1 minute-1 day). A value of *15 minutes* is the default setting.

7. Define the **Ivanti Endpoint Security Agent Notification Defaults** options.

   The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the ***Agent Control Panel*** (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**). **Note:** • This policy will not take effect until the agent is restarted. • This policy can hide only the Ivanti Endpoint Security Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***. • This policy cannot hide the Patch Agent or the Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the ***Agent Control Panel*** are hidden or accessible to an endpoint user after logging on (**True** or **False**).

8. Define the **Reboot Behavior Defaults** option.

   An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

   a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.
Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

9. Click **Save**.

Result: Your Agent Policy Set is saved. You can now assign the Agent Policy Set to endpoint groups or edit the set.

After Completing This Task:
To assign an Agent Policy Set to a group, complete Assigning an Agent Policy Set to a Group on page 220.

Editing an Agent Policy Set

Following the creation of an Agent Policy Set, you can modify it to accommodate network environment changes.

The ***Edit A Policy Set*** dialog allows you to modify an agent policy set.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Click the **Edit** icon associated with the policy set you want to edit.

   Step Result: The ***Edit a Policy Set*** dialog opens.

3. [Optional] Edit the **Policy Set Details** fields.

Field Name	Type
Policy Set Name	The name of the Agent Policy Set.
Policy Set Description	A description of the Agent Policy Set (optional).

4. [Optional] Edit the **Agent Hardening** options.

   These options define the steps required to delete an agent. For additional information, refer to About Agent Hardening on page 239.

Option	Step
Agent uninstall protection (list)	Select from the list to define whether the agent requires a password to be uninstalled. The default value is **On**.
Global Uninstall Password (button)	Click **Modify** to open the ***Global Uninstall Password*** dialog. Use this dialog to define a password for manually uninstalling the agent. For additional information, refer to Changing the Global Uninstall Password on page 250. **Note:** This option only available when editing the Global System Policy agent policy set. Only users assigned to the built-in Administrator role may view or modify the global uninstall password.

5. [Optional] Edit the **Agent Logging** options.

Option	Step
Logging level (button)	Click to open the ***Logging Level*** dialog. Use this dialog to select the agent logging level. For additional information, refer to Defining Agent Policy Logging Levels on page 252.
Maximum log file size (field)	Type the amount of disk space that triggers the agent to delete its log (1-500 MB). A value of *10* is the default setting.

6. [Optional] Edit the **Ivanti Endpoint Security Agent Communication** options.

Options	Step
Use HTTP for file download (list)	Select whether packages are downloaded using HTTP, regardless of whether HTTPS is used for communication between the agent and Ivanti Endpoint Security (*True* or *False*). The default value is *True*.
Send interval (list)	Select the amount of time that the agent should wait before sending an event to the Ivanti Endpoint Security server (0-5 seconds). A value of *2 seconds* is the default setting.
Receive interval (field and list)	Type and select the amount of time that the agent should delay before reattaching events from the Ivanti Endpoint Security Server. This value cannot exceed seven days. A value of *0 seconds* is the default setting.

Options	Step
Timeout interval **(field and list)**	Type and select the amount of time the agent should stay attached to the Ivanti Endpoint Security server before disconnecting (1 minute-7 days). A value of *12 hours* is the default setting.
Heartbeat interval **(field and list)**	Type and select the amount of time between agent check-ins with the Ivanti Endpoint Security server (1 minute-1 day). A value of *15 minutes* is the default setting.

7. [Optional] Define the **Ivanti Endpoint Security Agent Notification Defaults** options.

   The following table describes each option.

Option	Description
Hide Agent Control Panel	This option controls whether the ***Agent Control Panel*** (and all associated dialogs and notifications) are hidden or accessible to an endpoint user after logging on (**True** or **False**). **Note:** • This policy will not take effect until the agent is restarted. • This policy can hide only the Ivanti Endpoint Security Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden. • When set to **True**, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***. • This policy cannot hide the Patch Agent or the Agent.
Show Alerts on Endpoint	This option control whether the associated dialogs and notifications for the ***Agent Control Panel*** are hidden or accessible to an endpoint user after logging on (**True** or **False**).

8. [Optional] Edit the **Reboot Behavior Defaults**.

   An endpoint module installation or feature may require an endpoint to restart (such as the Device Control module). This option defines how the reboot is performed.

   a) From the **Reboot behavior** list, select a behavior.

Notify user, user response required before reboot	All logged-on endpoint users must agree unanimously to a restart. After the final user agrees to the reboot it will start immediately.
Notify user, automatically reboot within 5 minute timer	All users logged on to the endpoint are notified by a dialog that a restart will take place in five minutes.

Don't notify user, wait for next user-initiated reboot	No dialog notifies users that a reboot is required, and the policy does not take effect until the next time the endpoint is rebooted.

9. Click **Save**.

Result: Your edits are saved. The new policy values take effect the next time the applicable agents communicate with the Ivanti Endpoint Security server.

Deleting an Agent Policy Set

As your network environment changes, Agent Policy Sets may no longer be applicable. When this event occurs, you may delete the unnecessary Agent Policy Set.

You can delete Agent Policy Sets at any time from the ***Agent Policy Sets*** page.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Delete one or more Agent Policy Sets.

   Use one of the following methods.

Method	Steps
To delete one Agent Policy Set:	Click the **Delete** icon associated with an Agent Policy Set.
To delete multiple Agent Policy Sets:	**1.** Select the check boxes associated with the Agent Policy Sets you want to delete. **2.** From the toolbar, click the **Delete** button.

Note: Assigned agent policy sets and the **Global System Policy** cannot be deleted.

Step Result: A dialog displays, asking you to acknowledge the deletion.

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

Result: The Agent Policy Set(s) is deleted.

Changing the Global Uninstall Password

Change the Global Uninstall Password associated with the **Global System Policy** set. to uninstall any agent in your network.

Note: To uninstall an agent from its host endpoint, you must enter one of two passwords: *Endpoint Uninstall Password* or the *Global Uninstall Password*. The Global Uninstall Password feature ensures that endpoint users cannot uninstall the agent without the knowledge and permission of the administrator.

Define the Global Uninstall Password when editing the **Global System Policy**.

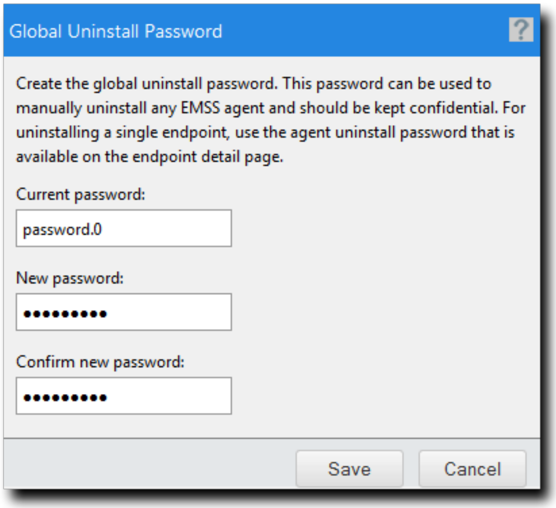
1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.

2. Click the edit icon (📝) for the **Global System Policy** set.

   Step Result: The ***Edit a Policy Set*** dialog opens.

3. Under the ***Agent Hardening*** section, click the **Modify** button adjacent to the **Global uninstall password** field.

   Step Result: The ***Global Uninstall Password*** dialog opens.



Global Uninstall Password

Create the global uninstall password. This password can be used to manually uninstall any EMSS agent and should be kept confidential. For uninstalling a single endpoint, use the agent uninstall password that is available on the endpoint detail page.

Current password: password.0

New password: •••••••••

Confirm new password: •••••••••

Figure 66: Global Uninstall Password Dialog

4. Type the desired password in the **New password** field.

   Tip: The password must be at least 8 characters in length.

5. Retype the password in the **Confirm new password** field.
6. Click **Save**.

   Note: Password edits are not saved until the agent policy set itself is saved.

7. Finish any desired edits to the **Global System Policy** set and click **Save**.

   Note: Password edits are not saved until the **Global System Policy** set is saved.

Result: The ***Global Uninstall Password*** dialog closes. Your edits take effect the next time Ivanti Endpoint Security and the applicable agents communicate.

Tip: The password required to uninstall the agent from the endpoint locally can be found. Refer to Viewing the Agent Uninstall Password on page 186 for additional information.

Defining Agent Policy Logging Levels

All Ivanti Endpoint Security Agents record a log of events that transpire on the endpoint. An Agent Policy Set logging level setting controls how much memory an agent's host endpoint allocates for event logs.

Note: A defined logging level can help troubleshoot agent policy behavior. Define logging levels carefully: a low logging level may not record enough information to be useful; however, a high logging level may record verbose information at the cost of higher disk space.

Define logging levels when creating or editing an Agent Policy Set.

1. From the **Navigation Menu**, select **Manage** > **Agent Policy Sets**.
2. Perform one of the following procedures based on your context.

Context	Procedure
If you are creating an agent policy set:	Click **Create**.
If you are editing an agent policy set:	Click the edit icon associated with the policy set containing the logging level setting you want to edit.

Step Result: Either the ***Create an Agent Policy Set*** or the ***Edit a Policy Set*** dialog opens.

3. Under the ***Agent Logging*** section perform one of the following procedures based on your context.

Context	Procedure
If you are defining the logging level for the first time:	Click the **Define** button adjacent to the **Logging level** field.

Context	Procedure
If you are modifying the logging level:	Click the **Modify** button adjacent to the **Logging level** field.

Step Result: The ***Logging Level*** dialog opens.

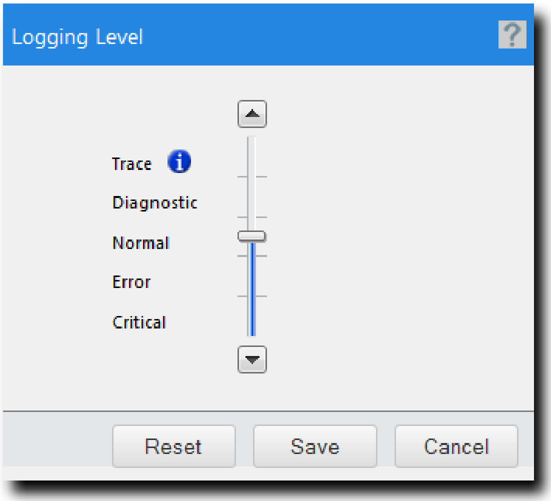


Figure 67: Logging Level Dialog

4. Move the slider to the desired logging level.

   The following table describes each logging level.

Logging Level	Description
Trace	Logs all errors and system actions. **Note:** This highest level logging level should be used only when necessary, as it will consume a large amount of resources on the endpoint.
Diagnostic	Logs all errors and major system actions.
Normal	Logs all errors and basic system action and usage information.
Error	Logs only errors.
Critical	Logs only critical events.

5. Click **Save**.

6. Finish any additional edits to the Agent Policy Set and click **Save**.

   > **Note:** Logging level edits are not saved until the Agent Policy Set is saved.

Result: The ***Logging Level*** dialog closes. Your edits take effect the next time the Ivanti Endpoint Security server and the applicable agents communicate.

Exporting Data for Agent Policy Sets

Click the toolbar **Export** button to export the list of Agent Policy Sets listed on the ***Agent Policy Sets*** page to a comma-separated value (`.csv`) file. Exporting data lets you work with data in other programs for reporting and analytical purposes.

Data for policy values are also exported. For additional information, refer to Exporting Data on page 39.

Assigning an Agent Policy Set to a Group

Assigning an Agent Policy Set to a group defines functional rules for the group.

Prerequisites:

Create an Agent Policy Set. Refer to Creating an Agent Policy Set (Groups Page) on page 222 for details.

Assign Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

> **Note:** Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 237 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.

   > **Note:** You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Click **Assign**.

   Step Result: The **Select a Policy Set** list becomes active.

5. Select an agent policy set from the **Select a Policy Set** list.
6. Click the **Save** icon (💾) to save your changes.

   Step Result: The **Select a Policy Set** list closes and your policy is assigned.

   > **Note:** The **Cancel** icon (☒) cancels your changes and any edits are not saved.

Result: The policy set is saved and associated with the group.

Unassigning an Agent Policy Set from a Group

When desired, you can unassign an Agent Policy Set from a group.

Prerequisites:

An Agent Policy Set is assigned. Refer to Assigning an Agent Policy Set to a Group on page 220 for details.

Unassign the Agent Policy Sets to groups from the ***Agent Policy Sets*** view.

Note: Groups that do not have an associated Agent Policy Set assigned, use the **Global System Policy**. Refer to About Agent Policies and Agent Policy Sets on page 237 for additional information.

1. From the **Navigation Menu**, select **Manage** > **Groups**.
2. From the **View** list, select **Agent Policy Sets**.
3. Select a group from the directory tree.

   Note: You may select a group that is either in the **Custom Groups** or **Systems Groups** hierarchy.

4. Remove the desired policy sets.

   Use one of the following methods.

Method	Steps
To remove one Agent Policy Set:	Click the **Unassign** icon (↻) associated with the Agent Policy Set you want to remove.
To remove multiple Agent Policy Sets:	**1.** Select the check boxes associated with the Agent Policy Sets you want to remove. **2.** From the toolbar, click the **Unassign** button.

   Note: An **Unassign Disabled** icon indicates you cannot remove an inherited Agent Policy Set. Instead, you must change the group policy inheritance setting or remove the inherited policy set from the parent group. Refer to *Policy Inheritance* in Editing Group Settings on page 232 for additional information.

   Step Result: A dialog appears, prompting you to acknowledge the removal.

5. Click **OK**.

   Step Result: The selected policy set(s) are removed and the dialog closes.

Result: The Agent Policy Set(s) are no longer associated with the group.

Chapter 12

Managing Ivanti Endpoint Security Users and Roles

In this chapter:

- The Users and Roles Page
- The Users Tab
- Working with Users
- The Roles Tab
- Working with Roles

User and role management features let you add, edit, and delete Ivanti Endpoint Security users, and also assign users access rights.

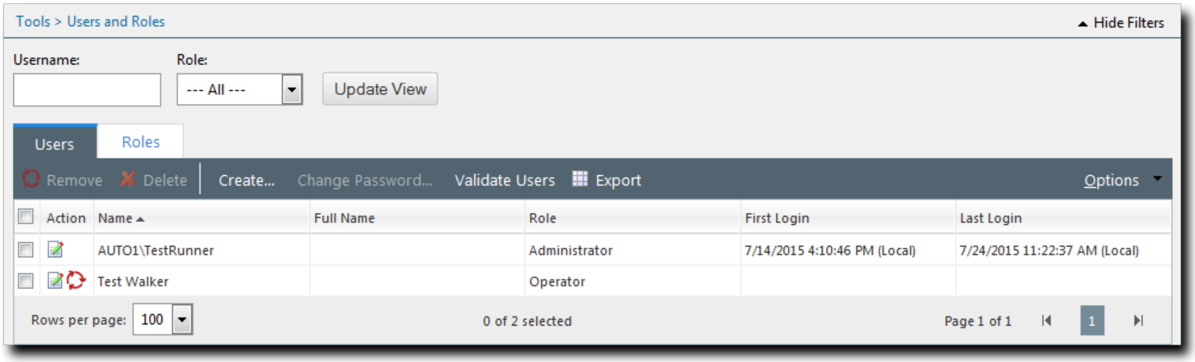
Create, configure, and manage users and roles from the ***Users and Roles*** page.

The Users and Roles Page

This page lets you view and manage *Users* and *Roles*. Users are a name or title used to log in to the Ivanti Endpoint Security Web console. Roles defines the functions and pages that are available to a user and includes access rights to groups and endpoints.

Existing users and user roles are listed on the ***Users*** and ***Roles*** tab:

- The Users Tab on page 259
- The Roles Tab on page 273



Username:

Role: --- All ---

☐	Action	Name ▲	Full Name	Role	First Login	Last Login
☐		AUTO1\TestRunner		Administrator	7/14/2015 4:10:46 PM (Local)	7/24/2015 11:22:37 AM (Local)
☐		Test Walker		Operator		

Rows per page: 100

0 of 2 selected

Page 1 of 1

Figure 68: Users and Roles Tabs

Viewing the Users and Roles Page

Navigate to this page to create and manage users and user roles.

You can access this page using the navigation menu.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Select a tab based on the task you want to accomplish:
   - To work with users, select the **Users** tab.
   - To work with roles, select the **Roles** tab.
3. [Optional] Complete a task.
   - To complete a user task, refer to Working with Users on page 261.
   - To complete a roles task, refer to Working with Roles on page 282.

User Access

Ivanti Endpoint Security supports the establishment of security policies that conform to your network needs. Two mechanisms determine security access: Windows-based authentication and Ivanti Endpoint Security access rights.

Windows Authentication

Access to Ivanti Endpoint Security (Ivanti Endpoint Security) is controlled by the Windows operating system authentication of local groups.

> **Note:** Users who have access to Ivanti Endpoint Security are members of the local Windows group, `PLUS Admins`. Members of this group have specific registry and file permissions to use the Ivanti Endpoint Security application.

Ivanti Endpoint Security Access Rights

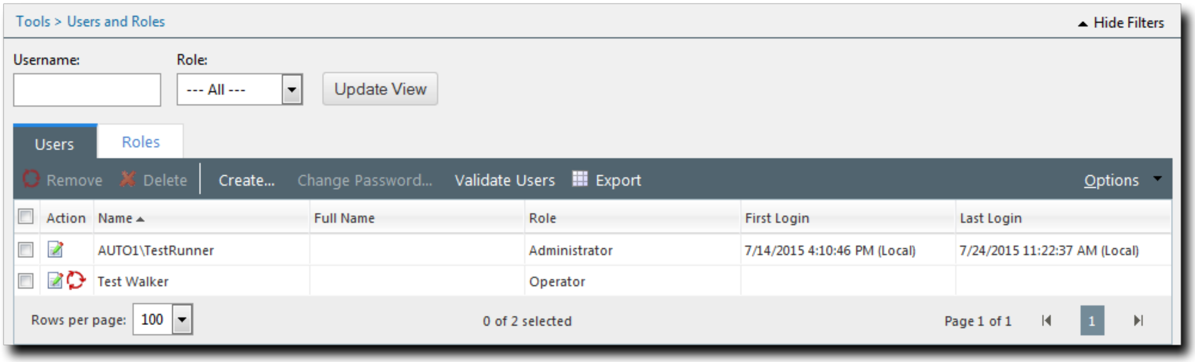
After a user logs in to Ivanti Endpoint Security, the system authenticates the user based on their assigned role. If a user does not have access to a given Ivanti Endpoint Security page or function, an access denied message displays, or the feature is simply unavailable.

On the ***Users and Roles*** page, the ***Users*** tab is where you create and manage users, and the ***Roles*** tab is where you create and manage Ivanti Endpoint Security roles.

The Users Tab

This tab lets you create and manage Ivanti Endpoint Security users.

The tab displays user details and allows you remove, delete, create, and modify a user. This includes changing an assigned user role.



Username:

Role: --- All ---

□	Action	Name ▴	Full Name	Role	First Login	Last Login
□		AUTO1\TestRunner		Administrator	7/14/2015 4:10:46 PM (Local)	7/24/2015 11:22:37 AM (Local)
□		Test Walker		Operator		

Rows per page: 100 — 0 of 2 selected — Page 1 of 1 — 1

Figure 69: Users Tab

About Users

Users are names or titles that are used to log in to the Ivanti Endpoint Security Web console. Users can be defined as individuals (John Smith) or conceptual users (Quality Assurance Manager).

A user profile includes access credentials (user name and password) and the role assigned to the user. A user can be assigned only one role at a time, but multiple users can share a user role which defines the functions and pages that are available to them.

There are two methods of introducing users to the system: creating users and adding users.

Creating New Users	When a user is created, that user is added to both Ivanti Endpoint Security (Ivanti Endpoint Security) database and Windows. Additionally, new users assigned the **Manage Users** access right are added to the Windows Administrators group; without addition to this group, the user would be unable to modify other users.
Adding Existing Windows Users	You can grant existing Windows users (both local users and domain users) access to Ivanti Endpoint Security. Using this method, you can search Windows for existing users and add them to Ivanti Endpoint Security. Additionally, added users assigned the **Manage Users** access right are added to the Windows Administrators group; without addition to this group, the user would be unable to modify other users.

Note: Microsoft IIS Web server software, used by Ivanti Endpoint Security, does not support user names or passwords in languages that require unicode characters (such as Korean or Kanji).

The Users Tab Toolbar

This toolbar contains buttons that let you create and manage users.

The following table describes the function of each toolbar button.

Table 94: Users Tab Toolbar

Button	Function
Remove	Removes the selected user. Removing a user removes it from Ivanti Endpoint Securitywithout deleting that user account within Windows. For additional information, refer to Removing Users on page 267.
Delete	Deletes the selected user. Deleting a user removes it from Ivanti Endpoint Security and Windows. For additional information, refer to Deleting Users on page 268.
Create...	Creates a new user. For additional information, refer to Creating New Users on page 262.
Change Password...	Changes the password for the selected user. For additional information, refer to Changing a User Password on page 269.
Validate Users	Removes Ivanti Endpoint Security users that cannot be found in: • Your domain (if the Ivanti Endpoint Security Server can contact it). • The Ivanti Endpoint Security Server local **PLUS Admins** user group. For additional information, refer to Validating Users on page 272.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Users Tab List

This list displays each user role within the system. Use the list icons to edit or remove users. Additionally, you can also filter the lists to display only specified roles.

The following table describes the ***Users*** tab list columns.

Table 95: Users Tab List

Column	Description
Action	Contains **Edit** and **Remove** icons. Use these icons to edit or remove the associated user. For additional information, refer to one of the following topics: • Editing Users on page 265 • Removing Users on page 267
Name	The name of user.
Full Name	The full name of the user.
Role	The role assigned to the user.
First Login	The date and time in which the user first logged in.
Last Login	The date and time in which the user last logged in.

Working with Users

To perform tasks associated with users, click a toolbar button or list icon. To perform some tasks, selecting one or multiple users from the list may be necessary.

- Creating New Users on page 262
- Adding Existing Windows Users on page 264
- Editing Users on page 265
- Removing Users on page 267
- Deleting Users on page 268
- Changing a User Password on page 269
- Changing Your Password on page 271
- Validating Users on page 272
- Exporting User Data on page 272

Creating New Users

You can create a new user when you need to allow a person within your organization access to Ivanti Endpoint Security Web console.

Create new users from the ***Users*** tab.

Note: New users are added to both Ivanti Endpoint Security (Ivanti Endpoint Security) and Windows. Refer to User Access on page 258 for additional information.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Click **Create**.

   Step Result: The ***Create User Wizard*** opens.
4. Ensure the **Creating a new local user** option is selected.
5. Click **Next**.

   Step Result: The ***New user information*** dialog opens.
6. Define the user credentials.

   Tip: The * indicates a required field.

   Type the applicable information in the following fields.

<table>
<tr><th>Field Name</th><th>Description</th></tr>
<tr><td><b>User name</b></td><td>The desired user name.
<b>Note:</b> The user name must be a unique name. It must be between 1-20 characters in length and cannot include any of the following characters:
• ′ \ ″ @ ^ % & { } ( ) [ ] ; < > ! # : ? / = |</td></tr>
<tr><td><b>Password</b></td><td>The desired password.
<b>Note:</b> The <b>Password Strength</b> indicator factors password effectiveness based on password length, complexity, character variety, and common word resemblance. Strong passwords contain eight characters or greater and combine symbols, numbers, uppercase letters, and lowercase letters. Also, they do not resemble common words or names, including words with numbers in place of letters.</td></tr>
<tr><td><b>Confirm Password</b></td><td>The password retyped.</td></tr>
</table>

7. From the **Select a Role** list, select the desired role.

   Select from the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

   Note: ***Custom Role(s)*** are only available if a custom role has been created. Refer to Custom Roles on page 275 for additional information.

8. [Optional] Define the user information.

   Type applicable information in the following fields.

Field Name	Description
Description	The description of the user.
Full name	The full name of the user.
Office phone	The office phone number of the user.
Cell phone	The cell phone number of the user.
Pager	The pager number of the user.
E-mail	The email address of the user.

9. Click **Finish**.

   Step Result: The ***Creation Summary*** dialog opens indicating you have successfully created a user.

   Note: In the event that user creation requirements are not met, you receive a notification message or in the event of password failure the ***Creation Summary*** dialog opens to display the error. You must resolve these errors to successfully create a user.

10. Click **Close**.

    Step Result: The ***Creation Summary*** dialog closes.

Result: The new user is created and is displayed on the ***User Tab*** list. The new user can now access all authorized features of Ivanti Endpoint Security.

You may edit the user from the ***Users*** tab. Refer to Editing Users on page 265.

Adding Existing Windows Users

You can create a user by adding a pre-existing Windows domain or local user. Add this type of user when they need to access to Ivanti Endpoint Security Web console.

Add existing Windows users from the ***Users*** tab.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Click **Create**.

   Step Result: The ***Create User Wizard*** opens.

3. Select the **Adding existing local or domain users** option.
4. Click **Next**.

   Step Result: The ***Existing user*** dialog opens.

5. In the **Search for the following users** field, type a user name, or the beginning characters of one or more user names.

   Use semicolons to separate user names. To search for users within a specific domain, prefix the user name with the domain. Example, (`DOMAINNAME\UserName`).

   > **Note:** There must be a secure connection between the domain and the Ivanti Endpoint Security's domain, or the user will be unable to access Ivanti Endpoint Security.

6. Click **Next.**

   Step Result: The ***User Roles*** dialog opens.

7. From the **Select a Role** list, select the desired role.

   Select from the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

   > **Note:** ***Custom Role(s)*** are only available if a custom role has been created. Refer to Custom Roles on page 275 for additional information.

8. Click **Finish**.

   Step Result: The ***Creation Summary*** dialog opens indicating you have successfully created a user.

   > **Note:** In the event that user creation requirements are not met, you receive a notification message or in the event of password failure the ***Creation Summary*** dialog opens to display the error. You must resolve these errors to successfully create a user.

9. Click **Close**.

   Step Result: The ***Creation Summary*** dialog closes.

Result: The new user is created and is displayed on the ***User Tab*** list. The new user can now access all authorized features of Ivanti Endpoint Security.

You may edit the user from the ***Users*** tab. Refer to Editing Users on page 265.

Editing Users

Edit existing Ivanti Endpoint Security users to change their assigned role or contact information.

Edit users from the ***Users*** tab.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Find the desired user(s).

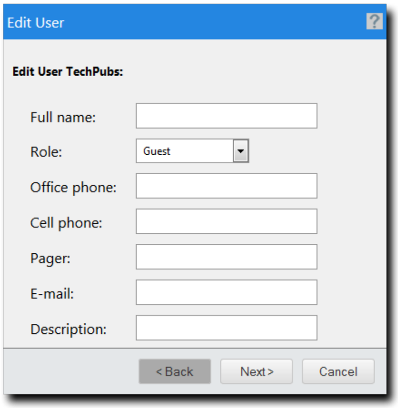
   Use one of the following methods.

Method	Steps
To search for user(s) by name:	1. Type an applicable name in the **Username** field. 2. Click **Update View**.
To search for user(s) by role:	1. Select the applicable role from the **Role** drop-down list. 2. Click **Update View**.

   Step Result: The user list updates based on your search.

4. Click the **Edit** icon associated with the user you want to edit.

   Step Result: The ***Edit User*** dialog opens.



Edit User TechPubs:

Full name:

Role: Guest

Office phone:

Cell phone:

Pager:

E-mail:

Description:

Figure 70: Edit User Dialog

5. [Optional] Edit the **Full name** field.
6. [Optional] Select a new role from the **Role** list.

   Select one of the following roles:

   - **Administrator**
   - **Manager**
   - **Operator**
   - **Guest**
   - ***Custom Role(s)***

   Note: *Custom Role(s)* are only available if a custom role has been created.

7. [Optional] Edit the following fields.

Field Name	Description
Office phone	The user’s office phone number.
Cell phone	The user’s cell phone number.
Pager	The user’s pager number.
E-mail	The user’s email address.
Description	The user’s description.

8. Click **Next**.

   Step Result: The ***Edit Confirmation*** dialog opens.

9. Click **Finish**.

   Step Result: The ***Edit Summary*** dialog opens.

10. Click **Close**.

    Step Result: The ***Edit Summary*** dialog closes.

Result: The user is updated according to your changes.

Removing Users

Removing a user account removes it from Ivanti Endpoint Security without deleting that user account within Windows or in Active Directory.

Remove users when you want to prevent a user from logging in to Ivanti Endpoint Security, (Ivanti Endpoint Security) but want the user to still to have a Windows (local) account. Once removed, the user is removed from the Ivanti Endpoint Security endpoint groups and the user list on the ***Users and Roles*** page.

Note: For additional information on deleting users (deleting removes them from both Ivanti Endpoint Security and Windows), refer to Deleting Users on page 268.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for user(s) by name:	**1.** Type an applicable name in the **Username** field. **2.** Click **Update View**.
To search for user(s) by role:	**1.** Select the applicable role from the **Role** drop-down list. **2.** Click **Update View**.

   Step Result: The user list updates based on your search.

4. Remove the desired user(s).

   Important: You cannot remove users assigned the **Administrator** role. You must first edit the user, change the role, then remove the user.

   Use one of the following methods.

Method	Steps
To remove a single user:	Click the **Remove** icon associated with the user you want to remove.
To remove multiple users:	1. Select the check boxes associated with the users you want to remove. 2. From the toolbar, click the **Remove** button.

   Step Result: A dialog displays, asking you to acknowledge the removal.

5. Acknowledge the removal by clicking **OK**.

Result: The user is removed from Ivanti Endpoint Security. You can re-add the removed user at any time if the user's Windows account still exists.

Deleting Users

Delete a user when you want to remove it from both Ivanti Endpoint Security and Windows.

Deleting users removes them from both Ivanti Endpoint Security and Windows (locally), whereas removing users only removes them from Ivanti Endpoint Security.

Note: Refer to Removing Users on page 267 for additional information on how to remove a user.

Delete users from the ***Users and Roles*** page ***Users*** tab.

Important: You cannot delete users assigned the **Administrator** role. You must first change the role type by editing the user, then you may remove the user.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for user(s) by name:	1. Type an applicable name in the **Username** field. 2. Click **Update View**.

Method	Steps
To search for user(s) by role:	**1.** Select the applicable role from the **Role** drop-down list. **2.** Click **Update View**.

Step Result: The user list updates based on your search.

4. Select the user(s) you want to delete.
5. Click **Delete**.

Caution: Deleting a user deletes them from both Ivanti Endpoint Security and Windows (locally).

Step Result: A dialog displays, asking you to acknowledge the deletion.

6. Acknowledge the deletion by clicking **OK**.

Result: The user is deleted from both Ivanti Endpoint Security and Windows (locally).

Note: Deleting a Ivanti Endpoint Security user that was added from your Active Directory will not delete the Windows user account within Active Directory. The account will only be removed from Ivanti Endpoint Security.

Changing a User Password

Change a password for security reasons or if a user has forgotten theirs.

Prerequisites:

You have the **Change Password** access right. Refer to Defining Access Rights on page 275 for additional information on this access right that allows you edit other user's passwords.

Change user passwords from the ***Users*** tab.

Note: Changing a user's password in Ivanti Endpoint Security also changes the user's Windows password on the Ivanti Endpoint Security server or in Active Directory.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Ensure the ***Users*** tab is selected.
3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for user(s) by name:	**1.** Type an applicable name in the **Username** field. **2.** Click **Update View**.

Method	Steps
To search for user(s) by role:	**1.** Select the applicable role from the **Role** drop-down list. **2.** Click **Update View**.

Step Result: The user list updates based on your search.

4. Select the user whose password you want to change.

Tip: You may only select a single user at a time to change passwords.

5. Click **Change Password**.

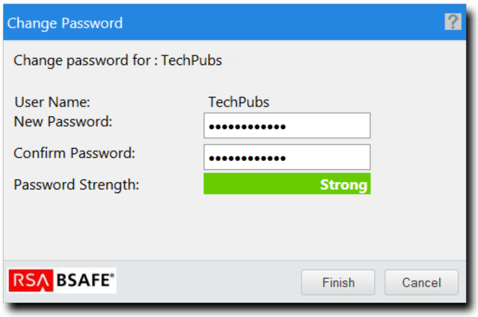
   Step Result: The ***Change password for*** dialog opens.

6. Type a new password in the **New Password** field.

   The **Password Strength** indicator factors your password security based on length, complexity, character variety, and common word resemblance.

   Strong passwords contain eight characters or greater and combine symbols, numbers, and letters (both upper and lowercase). Also, they do not resemble common words or names, including words with numbers in place of letters.

Attention: Passwords must adhere to Windows local and/or domain password policies.



Change Password

Change password for : TechPubs

User Name: TechPubs

New Password: ••••••••••••

Confirm Password: ••••••••••••

Password Strength: Strong

Figure 71: Change My Password Dialog

7. Retype the password in the **Confirm Password** field.
8. Click **Finish**.

Result: The password for the user is changed.

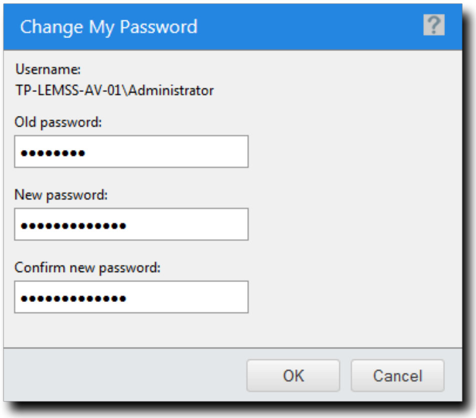
Changing Your Password

You can change your own password at any time. Changing your password in Ivanti Endpoint Security (Ivanti Endpoint Security) also changes your Windows password on the Ivanti Endpoint Security server or Active Directory.

Change your password from the navigation menu.

1. Select **Tools** > **Change My Password**.

   Step Result: The ***Change My Password*** dialog opens.



Change My Password

Username:
TP-LEMSS-AV-01\Administrator

Old password: ••••••••

New password: •••••••••••••

Confirm new password: •••••••••••••

Figure 72: Change My Password Dialog

2. Type your old password in the **Old password** field.

   The **Password Strength** indicator factors password effectiveness based on password length, complexity, character variety, and common word resemblance.

   Strong passwords contain eight characters or greater and combine symbols, numbers, uppercase letters, and lowercase letters. Also, they do not resemble common words or names, including words with numbers in place of letters.

   Attention: Passwords must adhere to Windows local and/or domain password policies.

3. Type your new password in the **New Password** field.
4. Retype your new password in the **Confirm New Password** field.
5. Click **OK**.

Result: Your password is changed. Use your new password the next time you log in to Ivanti Endpoint Security, Windows, or Active Directory.

Validating Users

Over time, staff who use Ivanti Endpoint Security move on from your enterprise. This attrition can create orphaned user accounts in the Ivanti Endpoint Security system. Instead of manually managing user and roles, you can use the **Validate Users** button to revoke access rights for orphaned accounts.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. From the toolbar, click **Validate Users**. Click **OK** to continue.

> **Note:** If Ivanti Endpoint Security can't contact the domain, domain users won't be validated. Retry validation when Ivanti Endpoint Security has domain connectivity.

Result:

- User validation synchronization begins. Depending on the number of users in your domain, this process may take up to two minutes.
- Users in Ivanti Endpoint Security that are deleted from either your domain or your Ivanti Endpoint Security Server PLUS Admin local user group are removed from the console.

> **Note:** Only user accounts that are deleted from the domain (or server) have their access rights revoked. Users accounts that are merely disabled remain in the Ivanti Endpoint Security system.

Exporting User Data

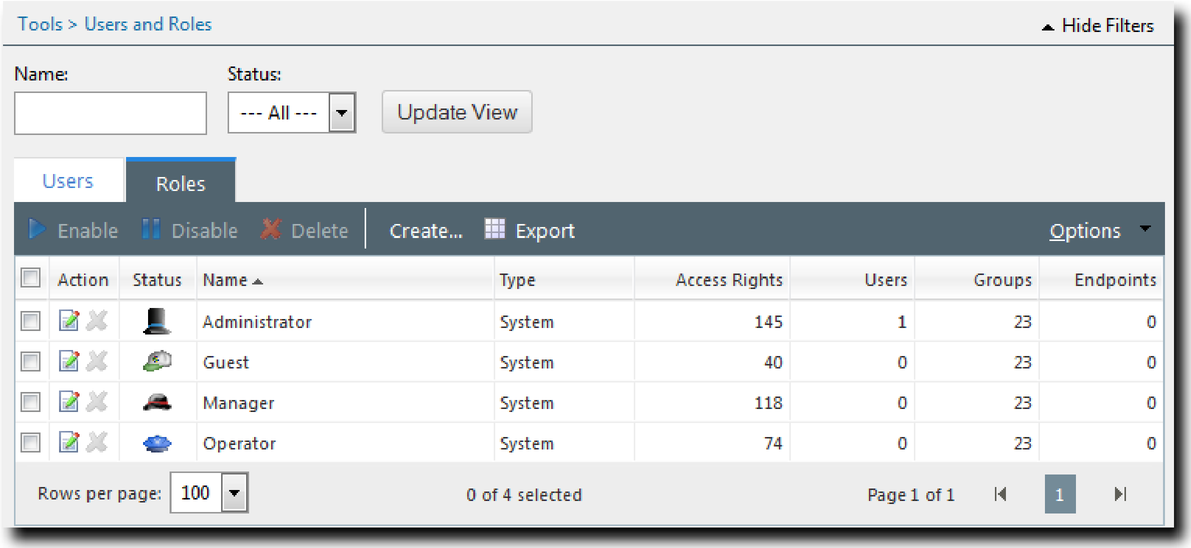
You can export the data displayed on the ***Users*** tab list so that it can be used in other applications. This data is exported to a comma separated value (`.csv`) file.

To export data, click the **Export** button. For additional information, refer to Exporting Data on page 39.

The Roles Tab

This tab lets you create new roles and manage existing roles. It also lists information about each existing role.

Additionally, you can use this tab to edit roles or remove roles.



Tools > Users and Roles

▲ Hide Filters

Name:

Status: --- All ---

Update View

Users | Roles

Enable | Disable | Delete | Create... | Export | Options

☐	Action	Status	Name ▲	Type	Access Rights	Users	Groups	Endpoints
☐	✎ ✖		Administrator	System	145	1	23	0
☐	✎ ✖		Guest	System	40	0	23	0
☐	✎ ✖		Manager	System	118	0	23	0
☐	✎ ✖		Operator	System	74	0	23	0

Rows per page: 100

0 of 4 selected

Page 1 of 1 | 1

Figure 73: Roles Tab

About Roles

Roles define the functions and pages that are available to a user and include general access rights, group access rights, and endpoint access rights within the Ivanti Endpoint Security. Roles can be customized and assigned to users.

The Ivanti Endpoint Security (Ivanti Endpoint Security) contains two types of roles:

System Roles	These roles are included with the default Ivanti Endpoint Security installation. These roles are predefined with access rights appropriate for various user types. System roles cannot be edited or disabled, and by default can access all system groups and endpoints.
Custom Roles	These roles are created after Ivanti Endpoint Security installation by users with the **Manage Users** access right. Custom roles let you grant users unique sets of access rights. Additionally, these roles let you define specific endpoints and groups that can be accessed and managed.

The following table describes role attributes.

Table 96: Role Attribute Descriptions

Role Attribute	Description
Access Rights	Define the pages and functions available to the user.
Accessible Groups	Define the specific endpoint groups accessible to the user.
Accessible Endpoints	Define the specific endpoints accessible to the user.

Predefined System Roles

Predefined system roles are the default roles offered by Ivanti Endpoint Security. The commonly used access rights selected for these roles are usually adequate for most networks and their users. Additionally, these roles can access and manage all groups and endpoints.

Predefined system roles have the following benefits:

- These roles types and their commonly used access rights are usually adequate for most networks and their users.
- A user assigned a predefined system role has access to all endpoints and groups.
- Users with the **Manage Users** access rights can assign predefined system roles to users.
- A predefined system role can be used as a template for creating a custom role.

The following table describes each predefined system role.

Table 97: Predefined System Role Descriptions

Role	Icon	Description
Administrator	🎩	Users with this role have full access to all Ivanti Endpoint Security pages and functions. The Administrators role allows you to assign endpoints to other roles. **Important:** At least one user must be assigned the administrator role at all times.
Guest	🧢	Users can access pages, but cannot use their functions; this role allows read-only access.
Manager	🎩	Users can access pages and functions.
Operator	🧢	Users can perform all routine functions (detect, export, and so on). Operators usually perform typical daily functions.
Note: A user assigned a system role has access to all endpoints and groups.		

Custom Roles

Custom roles are created after Ivanti Endpoint Security installation. Custom roles let you grant users unique sets of access rights. Additionally, this role lets you define specific endpoints and groups that can be accessed and managed.

Custom roles have the following benefits:

- You can configure a custom role to restrict access to endpoints and groups.
- You can configure a custom role to restrict access to Ivanti Endpoint Security pages and functions.
- Unlike system roles (which cannot be disabled or deleted), you can disable or delete a custom role at any time.
- When creating new custom roles you may use preexisting roles as templates to aid you.
- Custom roles are denoted by the **Wool Hat** icon.

Note: Custom roles are created by users with the **Manage Users** access right.

Defining Access Rights

Access rights are individual privileges that define whether a user can access a system feature. These rights control availability for every Ivanti Endpoint Security (Ivanti Endpoint Security) page, feature, function, and action. The pages and features available to users are based on the access rights associated with the role assigned to them. The system roles are assigned a default set of access rights. Users inherit the access rights of the role they are assigned.

Access rights begin with read-only access to system pages and permission to export data. At the administrative level, users can be assigned rights to fully manage the various system pages and functions.

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

Access Right	Description	Access
All		🎩
Dashboard		
View Dashboard	Access to view the home page dashboard.	🎩 👒 🧢 🧢
View Current Status	Access to view the status of the server.	🎩 👒 🧢 🧢
Jobs		
View Discovery Scan Jobs	Access to view discovery scan jobs.	🎩 👒
Create Discovery Scan Jobs	Access to create and copy discovery scan jobs	🎩 👒
View Agent Management Jobs	Access to view agent management jobs.	🎩 👒

Access Right	Description	Access
Create Agent Management Jobs	Access to create and copy agent management jobs.	🎩 🔴
Manage Modules via Jobs	Access to install or uninstall agent modules using agent management jobs.	🎩 🔴
Manage Jobs	Cancel, pause, resume, delete or merge all jobs the user has access to.	🎩 🔴
Export Jobs	Export the jobs list.	🎩 🔴
View AV Centralized Quarantine	Access to view AntiVirus Centralized Quarantine page	🎩 🔴 🔵
Manage AV Centralized Quarantine	Access to delete and restore files from Centralized Quarantine	🎩 🔴 🔵
Endpoints		
View Endpoints	Access the manage endpoints all tab.	🎩 🔴 🔵 🟢
Manage All Tab	Enable and disable agents, delete endpoints, manage agent modules, and wake endpoints.	🎩 🔴
Export All Tab	Export the all tab endpoints list.	🎩 🔴 🔵
Manage Remotely	Access the remote management options available.	🎩 🔴
Download Agent Installers	Access to the Download Agent Installers page.	🎩 🔴 🔵
Manage Agent Version	Access to the Manage Agent Version dialog.	🎩 🔴
Groups		
View Groups	Access the groups.	🎩 🔴 🔵 🟢
Manage Groups	Add, edit, enable, disable, and delete groups.	🎩 🔴
Export Groups	Export the groups list.	🎩 🔴 🔵
Users		
View Users	Access the user groups.	🎩 🔴 🔵 🟢
Manage Users	Add or remove users from individual user policies.	🎩 🔴
Export Users	Export the user groups list.	🎩 🔴 🔵

Access Right	Description	Access
Deployments and Tasks		
Create Deployments	Ability to create new deployments.	🎩 👒 🧢
View My Deployments and Tasks	Access the deployments and tasks that this user has created.	🎩 👒 🧢 ⛑️
View All Deployments	Access the deployments that all users have created.	🎩 👒 🧢
Manage Deployments and Tasks	Deploy, enable, disable, abort, and delete deployments and tasks that this user has access to.	🎩 👒 🧢
Export Deployments and Tasks	Export the deployments and tasks in the list that this user has access to.	🎩 👒 🧢
Agent Policy Sets		
View All Agent Policy Sets	Access the agent policy sets.	🎩 👒 🧢 ⛑️
Manage All Agent Policy Sets	Create, edit and delete agent policy sets.	🎩
Export All Agent Policy Sets	Export the agent policy sets list.	🎩 👒
Reports		
Reports Administer	Generate reports regardless of access rights for groups and endpoints.	🎩
View My Core Reports	Generate core reports only for those items this user has access to.	🎩 👒 🧢 ⛑️
Export Reports	Export the generated reports.	🎩 👒 🧢
Configure Enterprise Reporting (ER)	Configure settings to manage Configure Enterprise Reporting (ER)	🎩
Users/Roles		
View Users	Access the users and roles list view.	🎩 👒 🧢 ⛑️
Manage Users	Create, delete, enable, and disable users and roles.	🎩
Export Users	Export the users and roles list.	🎩 👒

Access Right	Description	Access
Change Password	Ability to change the password for users other than themselves.	🎩
Manage Server Modules		
Installation Manager	Access the Installation Manager to install, update and uninstall server modules.	🎩
Subscriptions		
View Subscription	Access the subscription service information.	🎩 👒 🧢 ⛑
Manage Subscription	Edit or update subscription service updates.	🎩
Export Subscription	Export the subscription service information.	🎩 👒
Directory/Computer Synchronization		
View Directory Sync Schedule	Access to view the active directory sync schedule page.	🎩 👒 🧢 ⛑
Manage Directory Sync Schedule	Create, edit, delete, enable, disable directory syncs.	🎩 👒
Export Directory Sync Schedule	Export the directory sync schedule lists.	🎩 👒 🧢
Email notifications		
View Email Notifications	Access the email notifications page.	🎩 👒 🧢 ⛑
Manage Email Notifications	Create and edit email notifications and settings for core feature. Note: All types of notifications may be deleted with this right.	🎩
Export Email Notifications	Export the emails notifications list.	🎩 👒
Options		
View Options	Access to general, agent and deployment default server options.	🎩 👒 🧢 ⛑
Manage Options	Set and edit general, agent and deployment default server options.	🎩
Export Options	Export the options list.	🎩 👒
Technical Support		

Access Right	Description	Access
View Technical Support	Access the technical product support information.	🎩 👒 🧢 🪖
Export Technical Support	Export the technical product support information.	🎩 👒 🧢
Licenses		
View Licenses	Access the product licenses.	🎩 👒 🧢 🪖
Manage Licenses	Update product licenses.	🎩
Export Licenses	Export the product license information.	🎩 👒

Defining Accessible Groups

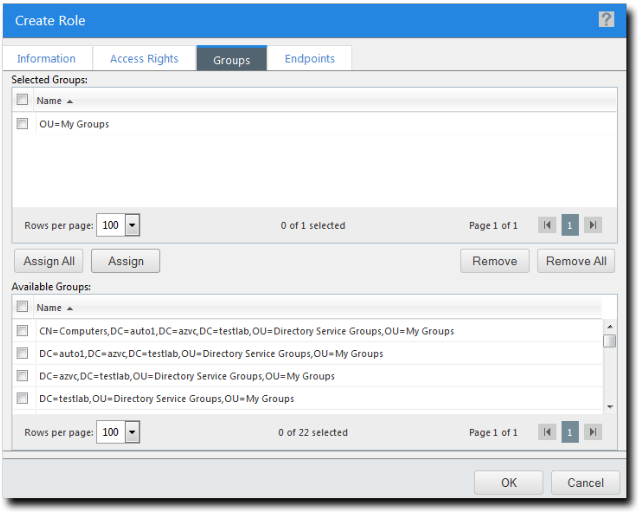
Accessible groups are specific groups of endpoints that a particular role can access and manage. Use this feature for granularity when assigning roles to users.

Accessible groups are only applicable to custom user roles.

Note: The **Accessible Groups** feature is disabled when working with a predefined system role. System roles can access all groups and endpoints within the system.

This feature allows you to restrict a user to specified groups. For example, a user assigned the access right to manage deployments can be limited to managing deployments for select groups.

The **Accessible Groups** feature is defined on the ***Groups*** tab in both the ***Create Role*** dialog and the ***Edit Role*** dialog.



Selected Groups:

□	Name ▲
□	OU=My Groups

Rows per page: 100 — 0 of 1 selected — Page 1 of 1

Available Groups:

□	Name ▲
□	CN=Computers,DC=auto1,DC=azvc,DC=testlab,OU=Directory Service Groups,OU=My Groups
□	DC=auto1,DC=azvc,DC=testlab,OU=Directory Service Groups,OU=My Groups
□	DC=azvc,DC=testlab,OU=Directory Service Groups,OU=My Groups
□	DC=testlab,OU=Directory Service Groups,OU=My Groups

Rows per page: 100 — 0 of 22 selected — Page 1 of 1

Figure 74: Roles Dialog Group Tab

The ***Groups*** tab contains the following lists, which are used to control what groups are associated with a particular role:

Table 98: Groups Tab List Descriptions

List	Description
Selected Groups	Lists the groups assigned to the role.
Available Groups	Lists the available groups that can be assigned to the role.

Defining Accessible Endpoints

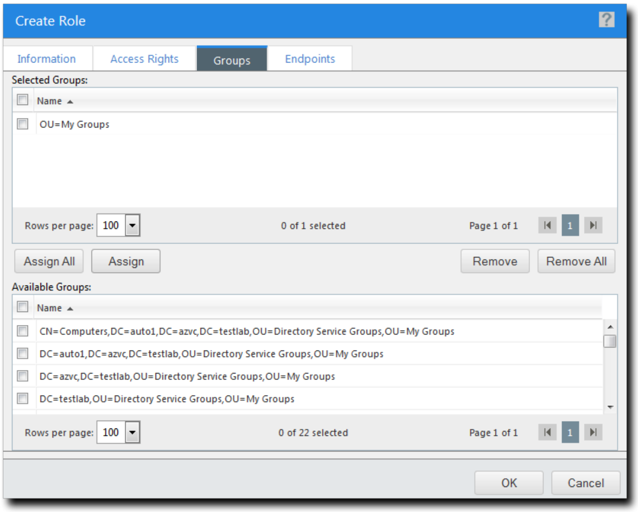
Accessible Endpoints are specific endpoints that a particular role can access and manage. This feature is similar to the **Accessible Groups** feature; it allows for granularity when assigning roles to system users.

Accessible endpoints are only applicable to custom user roles.

Note: The **Accessible Endpoints** feature is disabled when working with predefined system roles. System roles can access all groups and endpoints within the system.

As mentioned, this feature lets you define specific endpoints that users associated with the role can access and manage. For example, you can limit a user assigned the **Manage Endpoints** access right to management of a single endpoint.

This feature is are defined on the ***Endpoints*** tab in both the ***Create Role*** dialog and the ***Edit Role*** dialog.



Selected Groups:

□	Name ▲
□	OU=My Groups

Rows per page: 100 | 0 of 1 selected | Page 1 of 1

Available Groups:

□	Name ▲
□	CN=Computers,DC=auto1,DC=azvc,DC=testlab,OU=Directory Service Groups,OU=My Groups
□	DC=auto1,DC=azvc,DC=testlab,OU=Directory Service Groups,OU=My Groups
□	DC=azvc,DC=testlab,OU=Directory Service Groups,OU=My Groups
□	DC=testlab,OU=Directory Service Groups,OU=My Groups

Rows per page: 100 | 0 of 22 selected | Page 1 of 1

Figure 75: Roles Dialog Endpoints Tab

The ***Endpoints*** tab contains the following lists, which are used to control which endpoints are associated with a role:

Table 99: Endpoint Tab List Descriptions

List	Description
Selected Endpoints	Lists the endpoints assigned to the role.
Available Endpoints	Lists the available endpoints that can be assigned to the role.

The Roles Tab Toolbar

This toolbar contains buttons that let you create and manage user roles.

The following table describes the function of each ***Roles*** tab toolbar button.

Table 100: Roles Tab Toolbar

Button Name	Function
Enable	Enables the selected disabled custom role. For additional information, refer to Enabling User Roles on page 287.
Disable	Disables the selected custom role. For additional information, refer to Disabling User Roles on page 286.
Delete	Deletes the selected custom role. For additional information, refer to Deleting User Roles on page 287.
Create...	Creates a new user role. For additional information, refer to Creating User Roles on page 283.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 39. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu. For additional information, refer to The Options Menu on page 32.

The Roles Tab List

This list displays all user roles that exist within Ivanti Endpoint Security. Use the action icons to manage roles. Additionally, this list can be filtered to display only specified roles.

The following table describes each ***Roles*** tab list column.

Table 101: Roles Tab List

Column	Description
Action	Contains **Edit** and **Delete** icons. Use these icons to edit or delete the associated role. For addition information, refer to one of the following topics: • Editing User Roles on page 284 • Deleting User Roles on page 287
Status	Contains an icon that indicates the type of role. For additional information, refer to one of the following topics: • Predefined System Roles on page 274 • Custom Roles on page 275
Name	The name of the user role.
Type	The type of user role (`System` or `Custom`).
Access Rights	The number of access rights assigned to the role.
Users	The number of users assigned to the role.
Groups	The number of accessible groups assigned to the role.
Endpoints	The number of accessible endpoints assigned to the role.

Working with Roles

To perform tasks associated with roles, click a toolbar button or a list icon. To perform some tasks, selecting one or multiple roles from the list may be necessary.

- Creating User Roles on page 283
- Editing User Roles on page 284
- Disabling User Roles on page 286
- Enabling User Roles on page 287
- Deleting User Roles on page 287
- Exporting User Role Data on page 288

Creating User Roles

Custom roles let you select individual access rights, accessible groups, and accessible endpoints for that role. Create a custom role when predefined system roles do not contain the access rights needed for a particular user. Creating a custom role is also useful when you require a role that can only access specific groups or endpoints.

Create custom roles from the ***Roles*** tab.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Click **Create**.

   Step Result: The ***Create Role*** dialog opens to the ***Information*** tab.

4. Type a name in the **Name** field.
5. Type a description in the **Description** field.
6. Select a role template from the **Role Template** list.

   Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.
7. Select the ***Access Rights*** tab.
8. Select or clear the desired access rights.

   For additional information, refer to Predefined System Roles on page 274.

   Tip: Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

9. Select the ***Groups*** tab.
10. Assign the desired accessible endpoint groups to the role.

    Use one of the following methods to assign groups.

Method	Steps
To assign individual groups:	**1.** From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign. **2.** Click **Assign**.
To assign all groups:	Click **Assign All**.

Tip: Remove groups using **Remove** and **Remove All**.

11. Select the ***Endpoints*** tab.

12. Assign the desired accessible endpoints to the role.

    Use one of the following methods to assign endpoints.

Method	Steps
To assign individual endpoints:	**1.** From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign. **2.** Click **Assign**.
To assign all endpoints:	Click **Assign All**.

Tip: Remove endpoints using **Remove** and **Remove All**.

13. Click **OK**.

Result: Your new role is saved. It can now be assigned to users. Additionally, it can be edited from the ***Users and Roles*** page **Roles** tab.

Editing User Roles

Edit a custom user role as the needs of users associated with the role change. You can only edit custom roles (predefined system roles cannot be edited).

Edit roles from the ***Roles*** tab.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Click the **Edit** icon associated with the role you want to edit.

   Step Result: The ***Edit Role*** dialog opens to the ***Information*** tab.

4. Define the ***Information*** tab content.

   a) The **Name field** is a read-only and cannot be edited.

   b) [Optional] Edit the **Description** field.

   Tip: The optional description can be simple or detailed and may include information concerning the access right you are editing for the specific role.

   c) [Optional] Select a role template from the **Role Template** drop-down list.

   Tip: Any existing role can be used as a template. The selected role determines initial access rights. You can later change which access rights are assigned to the role.

5. Select the ***Access Rights*** tab.

6. [Optional] Selecting or clear the desired access rights.

> **Tip:** Select or clear the **All** check box to globally select or clear all access rights. Additionally, child access rights are unavailable until their parent access rights are selected.

7. Select the ***Groups*** tab.

8. [Optional] Assign accessible endpoint groups to the role.

   Use one of the following methods to assign groups.

Method	Steps
To assign individual groups:	**1.** From the **Available Groups** table, select the check box(es) associated with the group(s) you want to assign. **2.** Click **Assign**.
To assign all groups:	Click **Assign All**.

9. [Optional] Remove accessible endpoint groups from the role.

   Use one of the following methods to remove groups.

Method	Steps
To remove individual groups:	**1.** From the **Selected Groups** table, select the check box(es) associated with the group(s) you want to remove. **2.** Click **Remove**.
To remove all groups:	Click **Remove All**.

10. Select the ***Endpoints*** tab.

11. [Optional] Assign accessible endpoints to the role.

   Use one of the following methods to assign endpoints.

Method	Steps
To assign individual endpoints:	**1.** From the **Available Endpoints** table, select the check box(es) associated with the endpoint(s) you want to assign. **2.** Click **Assign**.
To assign all endpoints:	Click **Assign All**.

12.[Optional] Remove accessible endpoints from the role.

Use one of the following methods to remove endpoints.

Method	Steps
To remove individual endpoints:	**1.** From the **Selected Endpoints** table, select the check box(es) associated with the endpoint(s) you want to remove. **2.** Click **Remove**.
To remove all endpoints:	Click **Remove All**.

13. Click **OK**.

Result: Your edits are saved. The edited role is applied to all associated users.

Editing User Roles

Within Ivanti Endpoint Security, you can edit custom user roles, which can be assigned to users with unique access requirements.

Complete the dialog by defining the setting on each tab.

Disabling User Roles

You can disable any custom role, allowing you to maintain the role within Ivanti Endpoint Security without assigning it to users. You can enable, edit, and delete disabled roles. Disabled roles appear unavailable.

Disable roles from the ***Roles*** tab.

Note: You cannot disable system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Select the check box(es) associated with the enabled custom role(s) you want to disable.
4. Click **Disable**.

Result: The selected role(s) is disabled.

Caution: If you disable a role currently assigned to a user, they can still log in to Ivanti Endpoint Security, but their access rights are heavily restricted.

Enabling User Roles

Enable roles when you want to reactive them.

Prerequisites:

The role is a custom role and is disabled.

Note: You cannot disable system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

Enable roles from the ***Roles*** tab.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.
3. Find the desired role(s).
   a) Select `Disabled` from the **Status** drop-down list.

   Note: Custom role(s) must have a status of `Disabled` to be enabled.

   b) Click **Update View**.

   Step Result: The role list updates based on your search.
4. Select the check box associated with the disabled role(s) you want to enable.
5. Click **Enable**.

   Step Result: The role is disabled and the denoted **Wool Hat** (🎩) icon is active again.

Result: The selected role(s) is enabled. You can now assign it to users.

Note: Users already assigned the previously disabled role will again be able to access Ivanti Endpoint Security with their full access rights.

Deleting User Roles

Delete custom user roles when they are no longer needed. You can delete roles regardless of whether they are enabled or disabled.

Delete custom roles from the ***Roles*** tab.

Note: You cannot delete system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

1. From the **Navigation Menu**, select **Tools** > **Users and Roles**.
2. Select the ***Roles*** tab.

3. Find the desired user(s).

   Use one of the following methods.

Method	Steps
To search for roles(s) by name:	1. Type an applicable name in the **Name** field. 2. Click **Update View**.
To search for user(s) by role:	1. Select the applicable role from the **Status** drop-down list. 2. Click **Update View**.

   Step Result: The role list updates based on your search.

4. Delete the desired roles.

   Use one of the following methods.

Method	Steps
To delete a single user role:	1. Click the **Delete** icon associated with the role you want to delete. 2. Click **OK** to acknowledge the deletion.
To delete multiple user roles:	1. Select the check boxes associated with the user roles that you want to delete. 2. From the toolbar, click the **Delete** button. 3. Click **OK** to acknowledge the deletion.

   Note: You cannot delete system roles: **Administrator**, **Manager**, **Operator**, **Guest**.

Result: The role is deleted.

> **Caution:** If you delete a role currently assigned to a user, they can still log in to Ivanti Endpoint Security, but their access rights are heavily restricted.

Exporting User Role Data

You can export the data displayed on the ***Roles*** tab list so that it can be used in other applications. This data is exported to a comma-separated value (`.csv`) file.

To export data, click the **Export** button. For additional information, refer to Exporting Data on page 39.

Chapter

13

Using Ivanti Installation Manager

In this chapter:

The Ivanti Installation Manager is a utility you can use to install, uninstall, or update Ivanti Endpoint Security components.

The Ivanti Installation Manager (Installation Manager) is accessible following Ivanti Endpoint Security installation.

Ivanti Installation Manager

Ivanti Endpoint Security is a platform that supports various solutions to security threats. These solutions are called components and consist of *platform components* and *module components*, which are delivered by the Ivanti Installation Manager (Installation Manager).

The Installation Manager is installed during the initial Ivanti Endpoint Security installation and can be accessed following setup from the Ivanti Endpoint Security Web console or by using its own stand alone application in Windows. Use the Installation Manager to install, update, or uninstall Ivanti Endpoint Security components: both platform components and module components.

The Installation Manager allows for flexibility among module components as each module is installed independently. Your network security is based on which modules you have installed, as different security solutions are available to protect your network.

The Ivanti Endpoint Security Components List

Ivanti Endpoint Security consists of components. These components include *platform components* and *module components*, and both work together to protect and manage your network.

The following table describes platform and module components.

Table 102: Platform Component List

Component	Description
Platform Components	
Core	Provides a common framework and management console to support installtion of Ivanti feature modules.
Remote Systems Management	Provides administrators a simple way to remotely manage endpoints from the Ivanti Endpoint Security Web console.
Wake on LAN	Allows organizations to eliminate operational and security blind-spots by waking up powered-down systems.
Support Tools	Provides support utilities for platform maintenance.
Note: All Ivanti Endpoint Security platform components are available after initial replication with the Global Subscription Service and automatically included with a Ivanti Endpoint Security install. These components cannot be uninstalled	
Module Components	
Patch and Remediation	Provides a rapid, accurate and secure patch management for applications and operating systems.
AntiVirus	Protects against malware via signature-matching capabilities as well as proactive behavioural analysis technology.
Application Control	Prevents unwanted or dangerous programs from executing via basic snapshot, application whitelist and Trust Engine capabilities.

Component	Description
Device Control	Protects against data theft via blocking of externally attachable devices, monitoring of data transfer, and enforcement of encryption policies on transient data storage technologies.

Note: You can install, upgrade, or uninstall any module you are licensed for with the Ivanti Installation Manager. You can manage modules regardless of purchase time.

For information about purchasing additional modules, contact Ivanti Sales Support (sales@ivanti.com) .

Accessing Ivanti Installation Manager

Open Ivanti Installation Manager to manage Ivanti Endpoint Security components.

Ivanti Installation Manager can be accessed using one of the following methods.

Table 103: Access Methods

Access Method	Description
Ivanti Endpoint Security	You can access the Ivanti Installation Manager via Ivanti Endpoint Security. For additional information, refer to Accessing Installation Manager Via Ivanti Endpoint Security on page 291.
Windows Start Menu	You can also access the Ivanti Installation Manager via the Windows Start Menu on the server that hosts Ivanti Endpoint Security. For additional information, refer to Accessing Installation Manager Via Windows on page 292.

Note: Only users assigned the *Administrator* role or the **Installation Manager** access right within Ivanti Endpoint Security can access Installation Manager.

Accessing Installation Manager Via Ivanti Endpoint Security

You can open Installation Manager using one of several pages within the Ivanti Endpoint Security Web console.

Prerequisites:

- Install of Ivanti Endpoint Security is completed.
- You have been assigned the *Administrator* role or the **Installation Manager** access right.

You can perform this task from any endpoint in your network.

1. Log in to Ivanti Endpoint Security.

2. Open the Installation Manager in a new browser window using one of the following methods:

Method	Steps
Using the Navigation Menu:	Select **Tools** > **Launch Installation Manager**.
Using the *Subscription Updates* page:	1. Select **Tools** > **Subscription Updates**. 2. From the toolbar, select **Launch Installation Manager**.
Using the *Product Licensing* page:	1. Select **Help** > **Product Licensing**. 2. From the toolbar, select **Launch Installation Manager**.
Using the *System Alert* pane:	1. Click the system alert link. 2. Browse to ***Managing Components*** dialog and select **Installation Manager**. **Note:** Only system alerts related to Installation Manager contain a link to open Installation Manager.

Result: The Installation Manager opens in a new browser window to the ***New/Update Components*** tab.

> **Note:** When accessing a Ivanti Endpoint Security Server that uses SSL, Microsoft Silverlight may create notification dialogs that you must acknowledge.

Accessing Installation Manager Via Windows

Installation Manager can be opened one of several ways. You can access Installation Manager using the Windows Start Menu.

Prerequisites:

- Install of Ivanti Endpoint Security is completed.
- You have been assigned the *Administrator* role or the **Installation Manager** access right.

Perform this task from the server that hosts Ivanti Endpoint Security.

Select **Start** > **All Programs** > **Ivanti Installation Manager**.

Result: Installation Manager opens in a new browser window to the ***New/Update Components*** tab.

> **Note:** When accessing a Ivanti Endpoint Security Server that uses SSL, Microsoft Silverlight may create notification dialogs that you must acknowledge.

Logging Out

After you finish using Installation Manager, log out to ensure no unauthorized use takes place.

Log out of the Installation Manager browser window.

1. Ensure module download or installation has completed.
2. Click **Close**.

   Step Result: The Installation Manager browser window closes.

Result: You are logged out of Installation Manager.

The Navigation Menu

This menu appears on all Ivanti Installation Manager pages. Use this menu to navigate through the Web console.

This menu organizes product features based on functionality. When you select a menu item, a new page or dialog opens. You can access all features of the system from this menu.

Table 104: Navigation Menu

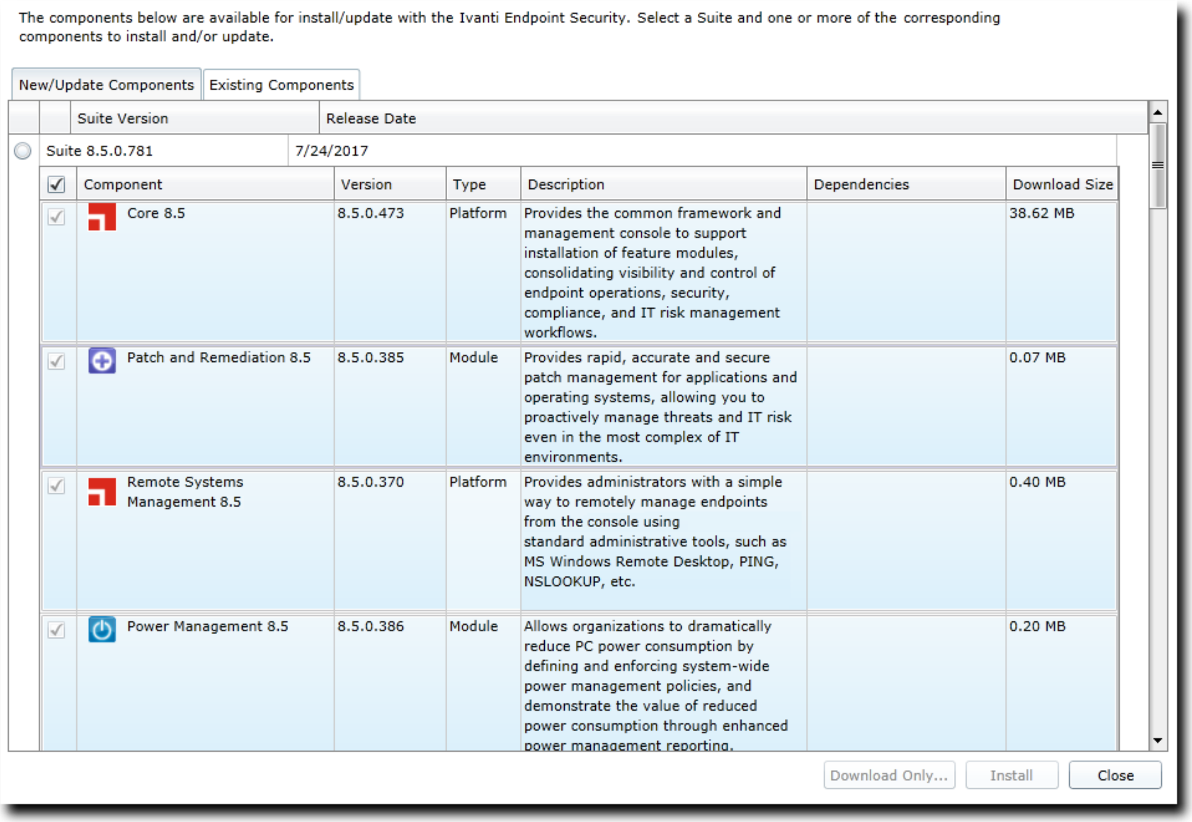
Menu	Menu Item	Function
Home		Opens the entrance page to Ivanti Installation Manager. For additional information, refer to The Home Page on page 294.
Tools	**View Install Log...**	Opens the ***Install Log*** dialog. For additional information, refer to The Installation Log on page 305.
Help	**Help Topics...**	Opens the Ivanti Endpoint Security Help system.
	Knowledge Base...	Opens the Ivanti Knowledge Base at Ivanti Self Service Support (https://support.heatsoftware.com) .
	Technical Support	Opens the ***Technical Support*** page. For additional information, refer to The Installation Manager Technical Support Page on page 308.
	Product Licensing	Opens the ***Product Licensing*** page. For additional information, refer to The Installation Manager Product Licensing Page on page 311.
	About...	Opens the ***About*** dialog.

The Home Page

This page is the entrance page to Ivanti Installation Manager. It consists of two tabs: the ***New/Update Components*** tab and the ***Existing Components*** tab.

For additional information on each tab, refer to:

- The New/Update Components Tab on page 295
- The Existing Components Tab on page 302



The components below are available for install/update with the Ivanti Endpoint Security. Select a Suite and one or more of the corresponding components to install and/or update.

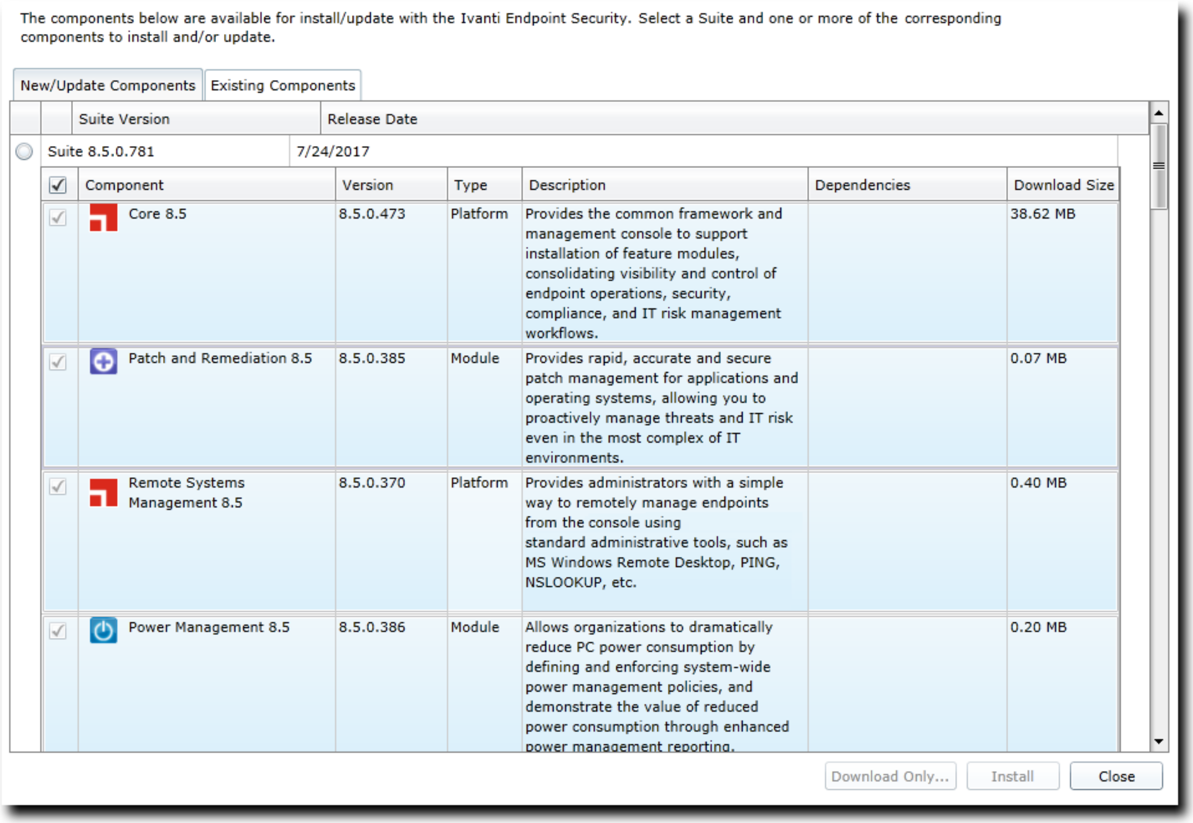
	Suite Version	Release Date
○	Suite 8.5.0.781	7/24/2017

☑	Component	Version	Type	Description	Dependencies	Download Size
☑	Core 8.5	8.5.0.473	Platform	Provides the common framework and management console to support installation of feature modules, consolidating visibility and control of endpoint operations, security, compliance, and IT risk management workflows.		38.62 MB
☑	Patch and Remediation 8.5	8.5.0.385	Module	Provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments.		0.07 MB
☑	Remote Systems Management 8.5	8.5.0.370	Platform	Provides administrators with a simple way to remotely manage endpoints from the console using standard administrative tools, such as MS Windows Remote Desktop, PING, NSLOOKUP, etc.		0.40 MB
☑	Power Management 8.5	8.5.0.386	Module	Allows organizations to dramatically reduce PC power consumption by defining and enforcing system-wide power management policies, and demonstrate the value of reduced power consumption through enhanced power management reporting.		0.20 MB

Figure 76: Home Page

The New/Update Components Tab

Use this tab to manage components and your Ivanti Endpoint Security version. This tab lists each yet-to-be installed component available for each Ivanti Endpoint Security release.



The components below are available for install/update with the Ivanti Endpoint Security. Select a Suite and one or more of the corresponding components to install and/or update.

	Suite Version	Release Date
○	Suite 8.5.0.781	7/24/2017

☑	Component	Version	Type	Description	Dependencies	Download Size
✓	Core 8.5	8.5.0.473	Platform	Provides the common framework and management console to support installation of feature modules, consolidating visibility and control of endpoint operations, security, compliance, and IT risk management workflows.		38.62 MB
✓	Patch and Remediation 8.5	8.5.0.385	Module	Provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments.		0.07 MB
✓	Remote Systems Management 8.5	8.5.0.370	Platform	Provides administrators with a simple way to remotely manage endpoints from the console using standard administrative tools, such as MS Windows Remote Desktop, PING, NSLOOKUP, etc.		0.40 MB
✓	Power Management 8.5	8.5.0.386	Module	Allows organizations to dramatically reduce PC power consumption by defining and enforcing system-wide power management policies, and demonstrate the value of reduced power consumption through enhanced power management reporting.		0.20 MB

Figure 77: New/Update Components Tab

Use this tab to complete the following component management tasks:

- Download components. For additional information, refer to Downloading Components on page 297.
- Install downloaded components. For additional information, refer to Installing Downloaded Components on page 298.
- Download and install components. For additional information, refer to Installing or Updating Components on page 299.

The New/Update Components Tab List

The tab list itemizes all unapplied components for each Ivanti Endpoint Security (Ivanti Endpoint Security) release.

This list is separated into two tiers.

- Tier one lists the Ivanti Endpoint Security release.
- Tier two lists unapplied components for the applicable Ivanti Endpoint Security release.

The following table describes the first tier of the ***New/Update Components*** tab list.

Table 105: New/Update Components Tab List (Tier One)

Column	Description
Suite Version	The version number of the applicable Ivanti Endpoint Security release.
Release Date	The date and time the associated Ivanti Endpoint Security update was released.

The following table describes the second tier of the ***New/Update Components*** tab list. This tier lists the components available for the applicable Ivanti Endpoint Security release.

Table 106: New/Update Components Tab List (Tier Two)

Column	Description
Component	The component available for installation.
Version	The version of the component.
Type	The type of component (`Platform` or `Module`).
Description	The description for the component.
Dependencies	The prerequisite component needed to install the component.
Download Size	The size of the component (in MBs).

The New/Update Components Tab Buttons

After selecting components from the ***New/Update Components*** tab list, use the available buttons to initiate installations or downloads.

The following table describes the ***New/Update Components*** tab button functions.

Table 107: New/Update Components Tab Buttons

Button	Function
Download Only...	Downloads the selected components. For additional information, refer to Downloading Components on page 297.

Button	Function
Install	Installs the selected components. For additional information, refer to Installing or Updating Components on page 299.
Close	Closes Installation Manager. For additional information, refer to Logging Out on page 293.

Working with Installs and Updates

You can download, install, or update Ivanti Endpoint Security components from the ***New/Update Components*** tab.

You can perform the following tasks from this tab:

- Downloading Components on page 297
- Installing Downloaded Components on page 298
- Installing or Updating Components on page 299

Note: Ivanti Installation Manager is updated periodically to take advantage of higher performance or added features. Refer to Updating Ivanti Installation Manager on page 313 for additional information.

Downloading Components

You can use the Ivanti Installation Manager to download components for later installation.

Prerequisites:

A full replication has completed prior to using the Ivanti Installation Manager. Refer to Updating Ivanti Endpoint Security System Files and Content on page 86 for additional information.

Complete downloads from the ***New/Update Components*** tab within the Installation Manager Web console.

Note: You download module component(s) to the storage directory of Ivanti Endpoint Security server when they are needed in an air-gap environment.

1. Within the Web console, select **Tools** > **Launch Installation Manager**.

   Step Result: Installation Manager opens.

2. If necessary, upgrade Silverlight by clicking **Install**.
3. If necessary, upgrade Installation Manager by clicking **Install**. Click **Close** when the upgrade finishes.
4. If necessary, click **Reboot Server**, and then log back into the Web console.

5. 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.

6. [Optional] Select any new components you want to install.

   When updating the suite version, modules already installed are automatically selected for update and cannot be deselected.

7. Click **Download Only**.

   Step Result: The ***Download Components*** dialog opens and the download begins.

   > **Note:** If downloading a component with unmet prerequisites, a notification dialog opens, prompting you to download the prerequisites. Click **Yes** to download the prerequisites or **No** to skip them. You cannot install the selected component(s) until the prerequisites are downloaded and installed.

8. When the download completes, click **Close**.

   Step Result: The ***Download Components*** dialog closes.

Result: The component(s) are downloaded.

> **Note:** The default location for downloaded components is %Installation Directory%\HEAT Software\EMSS\Content\.

After Completing This Task:

You may install the component at any time after downloading. Refer to Installing Downloaded Components on page 298 for install information.

Installing Downloaded Components

You can use Ivanti Installation Manager to install downloaded components.

Prerequisites:

The components require downloading. Refer to Downloading Components on page 297 for download information.

Complete install of downloaded components from the ***New/Update Components*** tab within the Installation Manager Web console.

1. Within the Web console, select **Tools** > **Launch Installation Manager**.

   Step Result: Installation Manager opens.

2. If necessary, upgrade Silverlight by clicking **Install**.

3. If necessary, upgrade Installation Manager by clicking **Install**. Click **Close** when the upgrade finishes.
4. If necessary, click **Reboot Server**, and then log back into the Web console.
5. 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.
6. [Optional] Select any new components you want to install.

   When updating the suite version, modules already installed are automatically selected for update and cannot be deselected.
7. Click **Install**.
8. If you haven't already, create a database backup before clicking **Next**.

   Step Result: The ***Ready to Install*** dialog opens.
9. Click the **terms and conditions** to review the user agreement.
10. 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.

Result: The downloaded component(s) are installed.

After Completing This Task:
Before you can begin using a newly installed module component, you must first install the module's endpoint component on endpoints hosting the Ivanti Endpoint Security agent.

Installing or Updating Components

You can use Ivanti Installation Manager to download new or update existing components and install them automatically.

Prerequisites:

Complete replication. Refer to Updating Ivanti Endpoint Security System Files and Content on page 86 for additional information.

Complete installs from the ***New/Update Components*** tab within the Installation Manager Web console.

1. Within the Web console, select **Tools** > **Launch Installation Manager**.

   Step Result: Installation Manager opens.

2. If necessary, upgrade Silverlight by clicking **Install**.
3. If necessary, upgrade Installation Manager by clicking **Install**. Click **Close** when the upgrade finishes.
4. If necessary, click **Reboot Server**, and then log back into the Web console.
5. 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.

6. [Optional] Select any new components you want to install.

    When updating the suite version, modules already installed are automatically selected for update and cannot be deselected.
7. Click **Install**.
8. If the ***Prerequisites*** dialog opens, resolve the requirements before continuing. Complete the substeps below.

    If the ***Database backup recommended*** dialog opens, proceed to Step 9.

    a) Click **Install** to install the requirements.

    > **Tip:**
    >
    > - Click **Retry** to re-access the system for requirements.
    > - Click **Print** to print the requirements.

    b) If necessary, **Reboot Server** and then log back in to Ivanti Endpoint Security.
9. If you haven't already, create a database backup before clicking **Next**.

    Step Result: The ***Ready to Install*** dialog opens.
10. Click the **terms and conditions** to review the user agreement.
11. Click **Install** to begin installation. If prompted, click **OK** to proceed.

    Installation takes several minutes.

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

   Tip:

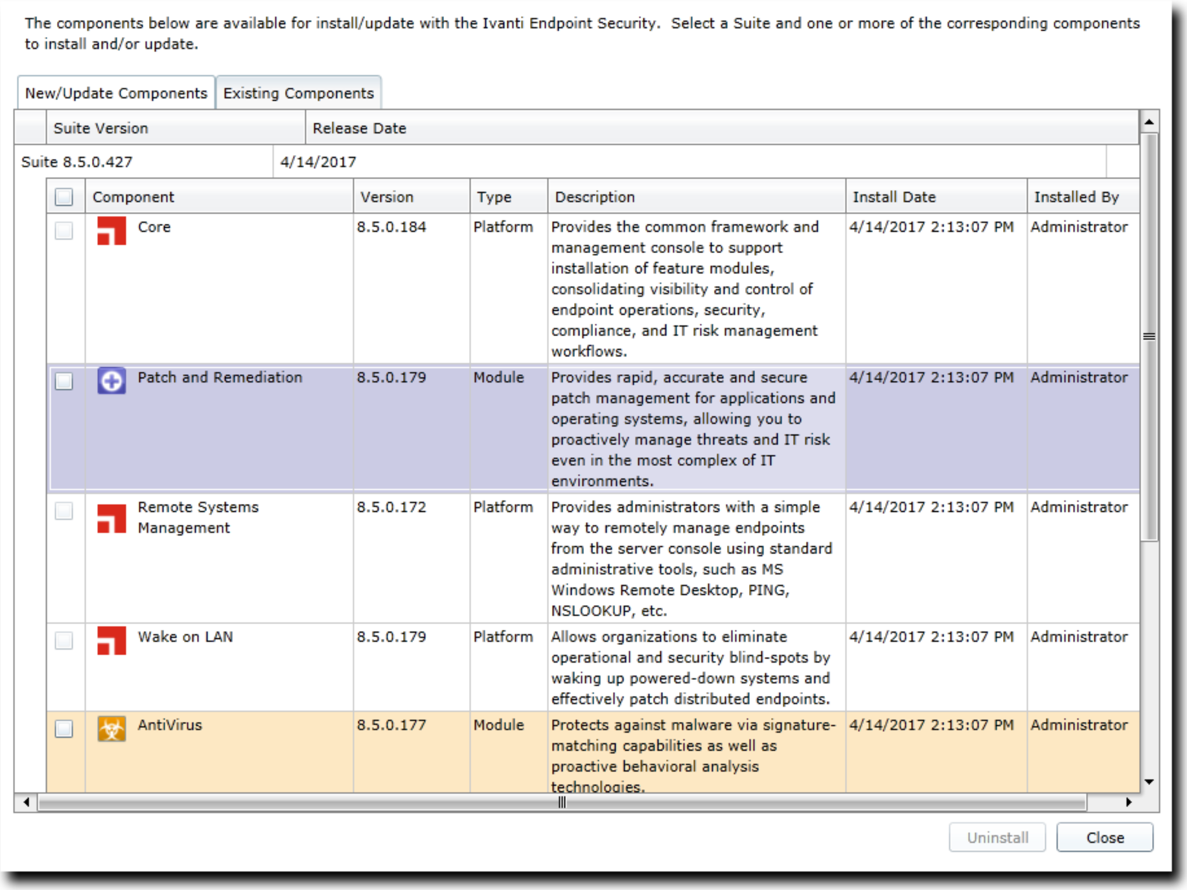
   - Click **View install log** to review the install log.
   - Clear the **Launch** checkbox to cancel relaunch of the Web console.

Result: The new components are installed.

After Completing This Task:
Before you can begin using a newly installed module component, you must first install the module's endpoint component on endpoints hosting the Ivanti Endpoint Security agent.

The Existing Components Tab

This tab lists the version of Ivanti Endpoint Security currently installed on your server and the installed components.



The components below are available for install/update with the Ivanti Endpoint Security. Select a Suite and one or more of the corresponding components to install and/or update.

Suite Version	Release Date
Suite 8.5.0.427	4/14/2017

□	Component	Version	Type	Description	Install Date	Installed By
□	Core	8.5.0.184	Platform	Provides the common framework and management console to support installation of feature modules, consolidating visibility and control of endpoint operations, security, compliance, and IT risk management workflows.	4/14/2017 2:13:07 PM	Administrator
□	Patch and Remediation	8.5.0.179	Module	Provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments.	4/14/2017 2:13:07 PM	Administrator
□	Remote Systems Management	8.5.0.172	Platform	Provides administrators with a simple way to remotely manage endpoints from the server console using standard administrative tools, such as MS Windows Remote Desktop, PING, NSLOOKUP, etc.	4/14/2017 2:13:07 PM	Administrator
□	Wake on LAN	8.5.0.179	Platform	Allows organizations to eliminate operational and security blind-spots by waking up powered-down systems and effectively patch distributed endpoints.	4/14/2017 2:13:07 PM	Administrator
□	AntiVirus	8.5.0.177	Module	Protects against malware via signature-matching capabilities as well as proactive behavioral analysis technologies.	4/14/2017 2:13:07 PM	Administrator

Figure 78: Existing Components Tab

Use this tab to uninstall existing module components.

The Existing Components Tab List

This list identifies which version of Ivanti Endpoint Security (Ivanti Endpoint Security) is installed on your server and itemizes the components installed.

This list is separated into two tiers.

- Tier one lists the version of Ivanti Endpoint Security installed on your server.
- Tier two lists components installed on your platform. The list contains information about each platform and module component installed.

The following table describes the first tier of the ***Existing Components*** tab list.

Table 108: Existing Components Tab List (Tier One)

Column	Description
Suite Version	The version number of the applicable Ivanti Endpoint Security release.
Release Date	The date and time the associated Ivanti Endpoint Security update was released.

The following table describes the second tier of the ***Existing Components*** tab list.

Table 109: Existing Components Tab List (Tier Two)

Column	Description
Component	The name of the component installed on your Ivanti Endpoint Security Server.
Version	The version of the component.
Type	The type of component (`Platform` or `Module`).
Description	The description for the component.
Install Date	The date and time the component was downloaded from the Global Subscription Service.
Installed By	The person who installed the component.

The Existing Components Tab Buttons

Use tab buttons to uninstall existing Ivanti Endpoint Security module components.

The following table describes the ***Existing Components*** tab button functions.

Button	Function
Uninstall	Uninstalls selected module components. For additional information, refer to Uninstalling Module Components on page 304. **Note:** Platform components cannot be uninstalled.
Close	Closes the Ivanti Installation Manager.

Working with Uninstalls

You can uninstall existing Ivanti Endpoint Security module components when they are no longer used or needed.

You can perform the following tasks from this tab:

- Uninstalling Module Components on page 304

Uninstalling Module Components

You can uninstall module components when they are no longer used or needed.

Uninstall module components from the ***Existing Components*** tab within the Installation Manager Web console.

1. From the navigation menu, select **Home**.
2. Select the ***Existing Components*** tab.
3. From the list, select the module component(s) you want to uninstall.

   Note: You may have to uninstall dependent modules as well. Platform components cannot be uninstalled.

4. Click **Uninstall**.

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

5. Click **Next**.

   Step Result: The ***Ready to Uninstall*** page opens displaying a list of components that will be uninstalled.

6. Click **Uninstall**.

   Step Result: A warning dialog opens, notifying you that all data associated with the selected components will be lost.

7. Click **Yes**

   Step Result: Selected components begin uninstalling.

   > **Tip:** Selecting the **No** or **Cancel** button cancels the uninstall, and you are returned to the ***New/Update Components*** tab.

8. When the component removal finishes, the ***Confirmation*** page listing uninstalled components displays.

   > **Note:** Select the following options if needed:
   >
   > - Click the **View install log** link to view the install log. For additional information, refer to The Installation Log on page 305.
   > - Deselect the **Launch Ivanti Endpoint Security** check box to cancel the launch of Ivanti Endpoint Security.

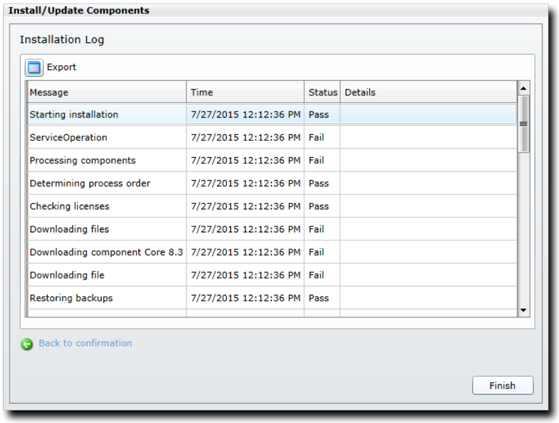
9. Click **Finish**.

   Step Result: Closes the ***Confirmation*** page.

Result: The selected Ivanti Endpoint Security module component(s) are uninstalled.

The Installation Log

The ***Installation Log*** is a dialog that lists details about Ivanti Installation Manager events. The log lists occurrences from the last installation or removal of a component.



Install/Update Components

Installation Log

Message	Time	Status	Details
Starting installation	7/27/2015 12:12:36 PM	Pass	
ServiceOperation	7/27/2015 12:12:36 PM	Fail	
Processing components	7/27/2015 12:12:36 PM	Fail	
Determining process order	7/27/2015 12:12:36 PM	Pass	
Checking licenses	7/27/2015 12:12:36 PM	Pass	
Downloading files	7/27/2015 12:12:36 PM	Fail	
Downloading component Core 8.3	7/27/2015 12:12:36 PM	Fail	
Downloading file	7/27/2015 12:12:36 PM	Fail	
Restoring backups	7/27/2015 12:12:36 PM	Pass	

Figure 79: Installation Log

This log is especially useful for troubleshooting installation or removal failures. The log features a list and buttons.

Viewing the Installation Log

View the ***Installation Log*** for details about the events that occurred during the most recent installation or removal of Ivanti Endpoint Security components.

View the ***Installation Log*** using the navigation menu within the Installation Manager Web console.

Tip: You can view the ***Installation Log*** from various locations in the Ivanti Installation Manager console. For additional information, refer to one of the following topics:

- Installing or Updating Components on page 299
- Uninstalling Module Components on page 304

1. From the navigation menu, select **Tools** > **View Install Log**.

   Step Result: The ***Installation Log*** opens.

2. Review the log details. For additional information, refer to The Installation Log List on page 306.

The Installation Log List

After selected components are installed or removed, you may view a log of events that occurred during the process.

The following reference describes each column in installation log table.

Table 110: Installation Log Table Columns

Column	Description
Message	The name of the event.
Time	The date and time the event occurred.
Status	The outcome of the event (`Pass` or `Fail`).
Details	The notes regarding the event.

The Installation Log Buttons

Use ***Installation Log*** buttons to perform tasks within the dialog.

The following table describes the ***Installation Log*** button functions.

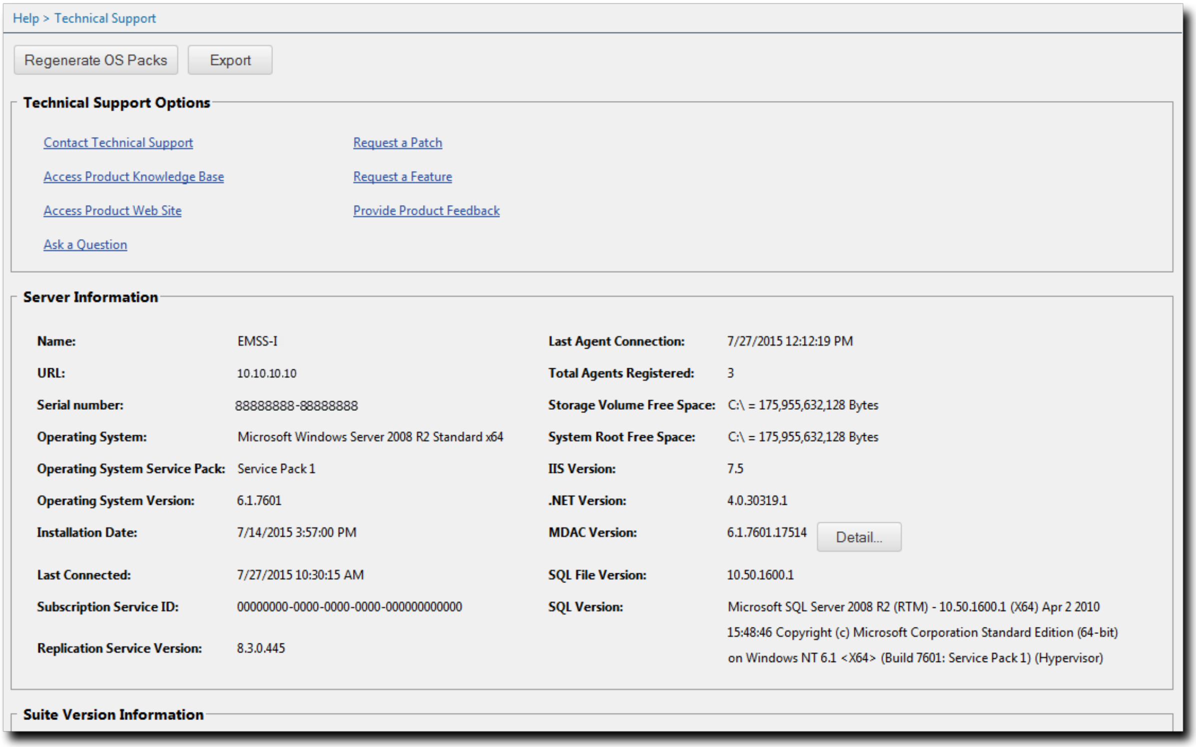
Table 111: Install Log Buttons

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. **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.
Finish	Closes the ***Installation Log***.

Note: When viewing the log following an installation completion or failure, a **back to confirmation** link is available. Click this link to return to the installer ***Confirmation*** page. This link is not available when opening the log via the navigation menu.

The Installation Manager Technical Support Page

Use this page to contact technical support. Technical support provides assistance for Ivanti Installation Manager or any other Ivanti product.



Name:	EMSS-I	**Last Agent Connection:**	7/27/2015 12:12:19 PM
URL:	10.10.10.10	**Total Agents Registered:**	3
Serial number:	88888888-88888888	**Storage Volume Free Space:**	C:\ = 175,955,632,128 Bytes
Operating System:	Microsoft Windows Server 2008 R2 Standard x64	**System Root Free Space:**	C:\ = 175,955,632,128 Bytes
Operating System Service Pack:	Service Pack 1	**IIS Version:**	7.5
Operating System Version:	6.1.7601	**.NET Version:**	4.0.30319.1
Installation Date:	7/14/2015 3:57:00 PM	**MDAC Version:**	6.1.7601.17514
Last Connected:	7/27/2015 10:30:15 AM	**SQL File Version:**	10.50.1600.1
Subscription Service ID:	00000000-0000-0000-0000-000000000000	**SQL Version:**	Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64) Apr 2 2010 15:48:46 Copyright (c) Microsoft Corporation Standard Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
Replication Service Version:	8.3.0.445		

Figure 80: Technical Support Page

This page features multiple support links. You can also use this page to contact support or provide comments for product improvement. In addition, this page also provides information about your Ivanti Endpoint Security server and its components.

The page is divided into the following sections:

- Technical Support Options on page 309
- Server Information on page 309
- Suite Version Information (Installation Manager) on page 310

Viewing the Technical Support Page (Installation Manager)

Navigate to this page to access support assistance for Ivanti Installation Manager or any other Ivanti product.

You can access this page at any time from the Installation Manager navigation menu.

1. Select **Help** > **Technical Support**.
2. View the page.

Technical Support Options

Ivanti Installation Manager provides access to various support assistance pages. Use these pages to communicate with Ivanti. Click each link to open the applicable page in a new window.

The following table describes each link.

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

Server Information

These fields list general information regarding the Ivanti Endpoint Security (Ivanti Endpoint Security) system.

Table 112: Server Information Fields

Field	Description
Server Name	The name of the computer Ivanti Endpoint Security is installed on.
URL	The URL of the server Ivanti Endpoint Security is installed on.
Serial Number	The serial number used by Ivanti Endpoint Security.
Operating System	The operating system installed and running on the Ivanti Endpoint Security server.
OS Version	The operating system version number.

Field	Description
OS Service Pack	The service pack applied to the operating system, if applicable.
Last Connected	The date and time Ivanti Endpoint Security last connected to the Global Subscription Service (GSS).
Subscription Service ID	The ID assigned to Ivanti Endpoint Security upon registration with the GSS.
Replication Service Version	The replication service version number.
Last Agent Connection	The date and time a registered Ivanti Endpoint Security Agent last connected to the Ivanti Endpoint Security server.
Total Agents Registered	The total number of agents registered with Ivanti Endpoint Security.
Storage Volume Free Space	The amount of free disk space on your storage volume.
System Root Free Space	The amount of free disk space on your system volume.
IIS Version	The Internet Information Services (IIS) version installed.
.NET Version	The .NET Framework version(s) installed.
MDAC Version	The Microsoft Data Access Components (MDAC) version. The **Detail** button adjacent to the field opens the ***MDAC File Version Information*** dialog.
SQL File Version	The SQL Server file version installed.
SQL Version	The SQL Server version number followed by detailed information.

Suite Version Information (Installation Manager)

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

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

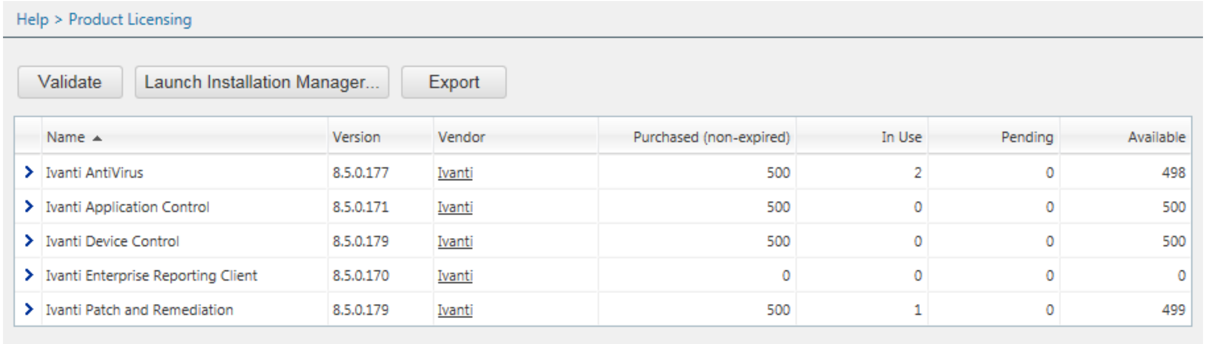
Table 113: Suite Version Information Fields

Field	Description
Server Suite Version	The version of Ivanti Endpoint Security installed on your Ivanti Endpoint Security server.
Core Version	The version of the Ivanti Endpoint Security core component installed on your Ivanti Endpoint Security server.
Installation Manager Version	The version of the Installation Manager installed on your Ivanti Endpoint Security server.

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

The Installation Manager Product Licensing Page

Use this page to view, validate, and export license information. It summarizes product component licenses applicable to your endpoint management activities including their expiration date. Product information is updated during daily replication with the Global Subscription Service.



Name ▲	Version	Vendor	Purchased (non-expired)	In Use	Pending	Available
Ivanti AntiVirus	8.5.0.177	Ivanti	500	2	0	498
Ivanti Application Control	8.5.0.171	Ivanti	500	0	0	500
Ivanti Device Control	8.5.0.179	Ivanti	500	0	0	500
Ivanti Enterprise Reporting Client	8.5.0.170	Ivanti	0	0	0	0
Ivanti Patch and Remediation	8.5.0.179	Ivanti	500	1	0	499

Figure 81: Product Licensing Page

Viewing the Product Licensing Page

View this page for information about the modules you are currently licensed for.

View the ***Product Licensing*** page using the navigation bar.

Select **Help** > **Product Licensing**.

Result: The ***Product Licensing*** page opens.

The Product Licensing Page Buttons

Click these buttons to use functions related to licensing information.

The following table describes each button.

Table 114: Product Licensing Page Buttons

Button	Function
Validate	Initiates a license replication that searches for any changes to your license data. For additional information, refer to Validating License Information on page 312.

Button	Function
Export	Exports the page data to a comma-separated value (`.csv`) file. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Product Licensing Page List

The page list itemizes information about each Ivanti Endpoint Security module you are licensed for.

The following table describes each ***Product Licensing*** page list column.

Table 115: Product Licensing Page List Column

Column	Description
Description	The module you are licensed for.
Version	The version number of the module.
Purchase Date	The date and time you purchased the module.
Vendor	The vendor that you purchased the module from.
Effective Date	The date that the module went into effect (not necessarily the purchase date).
Expiration Date	The date the module licensing expires.
Purchased	The total number of licences purchased for the module.

Validating License Information

Validating license information refreshes information about how many module licenses are available and in use. Validate license information after installing new modules.

Validate license information from the ***Product Licensing*** page.

1. Select **Help** > **Product Licensing**.
2. Click **Validate**.

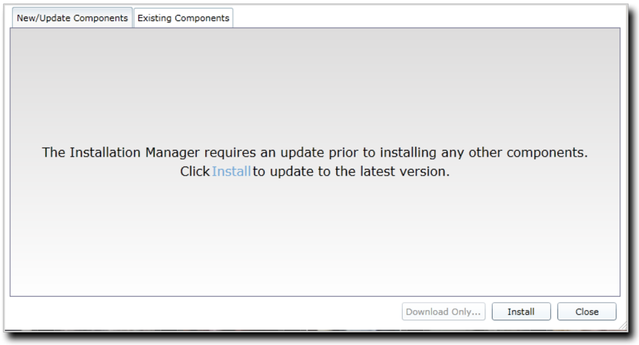
Installation Manager Reference

Within Ivanti Endpoint Security, you can use Installation Manager to install Ivanti Endpoint Security components.

Occasionally, after upgrading Ivanti Endpoint Security, you may be asked to update Installation Manager after opening it.

Updating Ivanti Installation Manager

Ivanti Installation Manager is updated periodically. Install the new version to take advantage of higher performance or added features.



The Installation Manager requires an update prior to installing any other components. Click Install to update to the latest version.

Figure 82: New/Update Components Tab

Ivanti Installation Manager updates are downloaded and applied by Ivanti Endpoint Security, or you can install them manually as any other component. For additional information, refer to Installing or Updating Components on page 299. Ivanti recommends installing updates immediately.

Note: If you are upgrading to Ivanti Endpoint Security 8.6 using the Ivanti Installation Manager, you may be asked to reboot the server to continue the update process.

Chapter 14

Using the Ivanti Endpoint Security Agent

In this chapter:

The Ivanti Endpoint Security Agent is the software component that excutes commands from the Ivanti Endpoint Security server on the agent's host endpoint. After you have installed the agent on an endpoint, you can access its available controls using its user interface.

Following initial installation, the agent registers with the Ivanti Endpoint Security server, and the two components begin communication.

The agent downloads the following data from the Ivanti Endpoint Security server:

- Agent policies, which contain information about how the agent should behave.
- Agent packages, which contain files to modify the agent.

The agent uploads the following messages to the Ivanti Endpoint Security server:

- Host endpoint operating system information.
- Heartbearts, which are notification messages the agent sends to the server. This message is used continually to notify the server that the agent is available within the network.

Additionally, if you are licensed for additional Ivanti Endpoint Security modules, you can install these modules on the Ivanti Endpoint Security Agent, which expands its functions.

Following installation, endpoint users can view the agent using the ***Agent Control Panel***. From this control panel, you can restart the agent, view information for each installed endpoint module, or define a proxy server to mediate communication with the Ivanti Endpoint Security Server.

Note: Functions for each Ivanti Endpoint Security Agent module may only be accessible from separate user interfaces.

> After installing the Ivanti Endpoint Security Agent, no additional user action is generally required.

Upgrading Agents on Endpoints

Upgrading an agent on an endpoint installs an updated version of the agent on the endpoint.

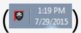
Versions of the Ivanti Endpoint Security Agent 7.3 and later can be upgraded using the Ivanti Endpoint Security Web console. During upgrades, the agent data and configuration are maintained. For additional information, refer to one of the following topics:

- To upgrade agents based on a complete list of endpoints in the system, refer to Upgrading Endpoints on page 173.
- To upgrade agents based on individual endpoints Upgrading the Agent on a Single Endpoint on page 187.
- To upgrade agents based on groups, refer to Defining the Endpoint Agent Version (Groups Page) on page 215.

Agent Notifications

The Ivanti Endpoint Security agent displays notifications to alert users of agent actions.

Table 116: Agent Notifications

Type	Description
System Tray Notification	These notifications usually display information that a routine agent action has completed. **Note:** System tray notifications appear above the agent icon () that is displayed in the system tray.
Notification Dialogs	Notification dialogs, which are dialogs that display on the endpoint desktop, are notifications that display when the agent makes an significant action. For example, when an endpoint user tries to open a denied application, the ***Blocked File*** dialog opens, informing the user that the application is blocked.

System administrators can create or edit Agent Policy Set to hide the agent icon and notifications. For additional information, refer to one of the following topics:

- About the Hide Agent Control Panel Policy on page 317
- Creating an Agent Policy Set on page 244
- Editing an Agent Policy Set on page 247

About the Hide Agent Control Panel Policy

By default, the Ivanti Endpoint Security agent creates an easily accessible system tray icon on its host endpoint. Endpoint users can use this icon to access the ***Agent Control Panel***. However, you can use agent policy sets to hide this icon and most of the agent UI.

Often, endpoint users are unaware that the Ivanti Endpoint Security agent is present on their endpoints. Therefore, when the agent alerts users to its presence, they may try to tamper with the agent because they think it is malicious in nature.

However, you can control ***Agent Control Panel*** accessibility by defining the **Hide Agent Control Panel** policy setting when creating or editing an agent policy. Applying this policy can reduce agent-related IT help requests or eliminate unauthorized uninstall attempts.

To hide the ***Agent Control Panel*** from endpoint users, set the **Hide Agent Control Panel** policy to **True** when creating or editing an applicable agent policy set. For additional information, refer to the following topics:

- Creating an Agent Policy Set on page 244
- Editing an Agent Policy Set on page 247

Note:

- This policy will not take effect until the agent is restarted.
- When set to **True**, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***.
- This policy can hide only the Ivanti Endpoint Security Agent for Windows. Agents installed on Linux, Unix, or Mac endpoints cannot be hidden.
- This policy cannot hide the Patch Agent or the Ivanti Device and Application Control Agent. Patch Agent and Ivanti Device and Application Control Agent UI controls will continue to display on endpoints with the Patch and Remediation module or Device Control module installed.

The following table lists all visible portions of the Ivanti Endpoint Security agent UI according to module, and then lists whether that portion is hideable using agent policy sets.

Note: Although the ***Agent Control Panel*** cannot be called using system tray icon, endpoint users can still open the ***Agent Control Panel*** using ***Windows Control Panel***. When a user opens the ***Agent Control Panel*** using Windows, the ***Agent Control Panel*** and the system tray icon display until user logs off. The ***Agent Control Panel*** and the system tray icon will be hidden again the next time the user logs on.

Table 117: Module Notification Hideability

Module	Notification	Hideable
Core	***Agent Control Panel***	Yes
	System Tray Icon	Yes
Application Control	Local Authorization	Yes

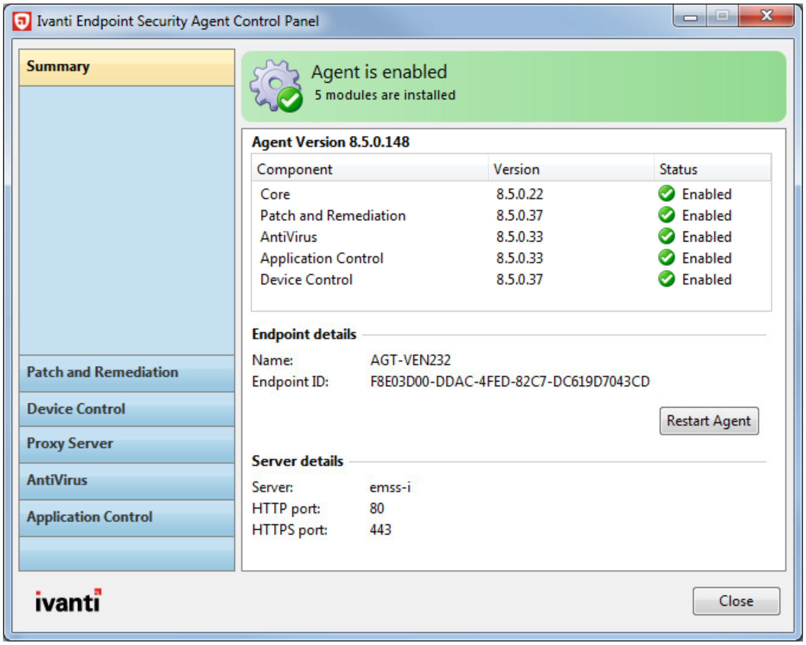
Module	Notification	Hideable
	Blocked Application Dialog	No
AntiVirus	Definition Update Notification	Yes
	Virus and Malware Alert Notification	Yes
	Scan Now Start/Stop Notification	Yes
	Scan Summary Dialog	Yes
	Email Notificaitons	No
	Server Notifications	No
Patch and Remediation (Patch Agent)	***Patch Agent*** Dialog	No
	Install Notification Dialog	No
	Reboot Notification Dialog	No
Device Control (Ivanti Device and Application Control Agent)	***Reboot from Install Notification*** Dialog	No
	Ivanti Device and Application Control Agent Settings Dialog	No
	Ivanti Device and Application Control System Tray Icon	No
	Device Connect Notifications	No
	Encryption Dialogs	No

The Agent Control Panel

The ***Agent Control Panel*** is the interface used to control the Ivanti Endpoint Security Agent. After installing the agent, you can view information about the agent and the modules it supports from this panel.

Use this control panel to manage Ivanti Endpoint Security Agent functionality. The control panel contains several tabs.

Note: Based on the agent modules installed, different tabs display.



Agent is enabled

5 modules are installed

Agent Version 8.5.0.148

Component	Version	Status
Core	8.5.0.22	✓ Enabled
Patch and Remediation	8.5.0.37	✓ Enabled
AntiVirus	8.5.0.33	✓ Enabled
Application Control	8.5.0.33	✓ Enabled
Device Control	8.5.0.37	✓ Enabled

Endpoint details

Name: AGT-VEN232

Endpoint ID: F8E03D00-DDAC-4FED-82C7-DC619D7043CD

Server details

Server: emss-i

HTTP port: 80

HTTPS port: 443

Figure 83: Agent Control Panel

The ***Agent Control Panel*** contains the following features:

Status Banner	This banner indicates the current status of the agent.

Main Menu Tab	This contains tabs for viewing general and module-specific information about the agent. Additional tabs appear each time a new module is installed. Select a tab to display related information in the main panel. This menu contains the following items: • The Summary Panel on page 321 • The Proxy Server Panel on page 323 **Note:** Additional tabs are added and removed as modules are installed or uninstalled on the agent.
Main Panel	This panel displays information related to the selected tab.

Accessing the Agent Control Panel

Access the panel to view and edit agent information.

Access the ***Agent Control Panel*** from an endpoint hosting a Ivanti Endpoint Security (Ivanti Endpoint Security Agent.

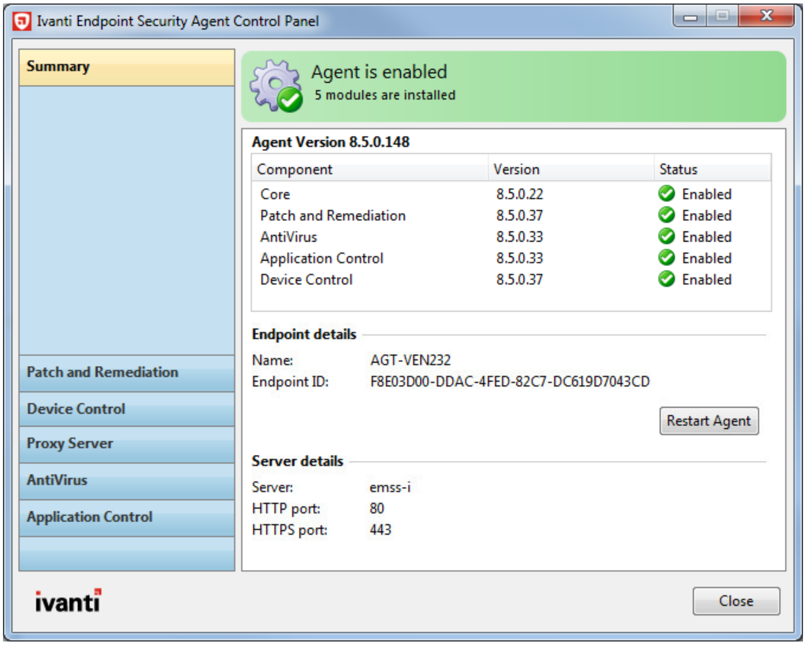
> **Note:** The system tray on the endpoint can contain a Ivanti Endpoint Security Agent icon (1:19 PM 7/29/2015). Double-clicking the icon opens the ***Agent Control Panel***. Refer to Agent Notifications on page 316 for further information on the agent icon.

1. Select **Start** > **Control Panel**.
2. Double-click **Agent Control Panel**.

Result: The ***Agent Control Panel*** opens to the ***Summary*** panel.

The Summary Panel

This panel displays agent information, endpoint details, and server details. This panel is the ***Agent Control Panel*** default panel.



Ivanti Endpoint Security Agent Control Panel

Agent is enabled

5 modules are installed

Agent Version 8.5.0.148

Component	Version	Status
Core	8.5.0.22	✓ Enabled
Patch and Remediation	8.5.0.37	✓ Enabled
AntiVirus	8.5.0.33	✓ Enabled
Application Control	8.5.0.33	✓ Enabled
Device Control	8.5.0.37	✓ Enabled

Endpoint details

Name: AGT-VEN232

Endpoint ID: F8E03D00-DDAC-4FED-82C7-DC619D7043CD

Server details

Server: emss-i

HTTP port: 80

HTTPS port: 443

Figure 84: Summary Panel

This panel contains the following sections:

- Agent Information on page 321
- Endpoint Details on page 322
- Server Details on page 322

Agent Information

This section lists the agent version and the module versions installed on the agent.

The following table defines each **Agent Information** field.

Note: Module entries only display when the applicable module is installed.

Table 118: Agent Information

Column	Description
Module Name	The name of the module installed on the agent.
Version Number	The version number of the module installed on the agent.

Column	Description
Status	The status of the module installed on the agent.

Endpoint Details

This sections lists information about the endpoint hosting the agent.

The following table describes the items in the **Endpoint details** area.

Table 119: Endpoint Detail Descriptions

Field	Description
Name	The name of the endpoint hosting the agent.
Endpoint ID	The ID assigned to the endpoint by Ivanti Endpoint Security.
Restart Agent (button)	This restarts the Ivanti Endpoint Security Agent on the endpoint. For additional information, refer to Restarting the Ivanti Endpoint Security Agent on page 322..

Restarting the Ivanti Endpoint Security Agent

If needed, you can restart the Ivanti Endpoint Security Agent using the ***Agent Control Panel***.

Restart the agent from the ***Summary*** panel.

Click **Restart Agent**.

Step Result: The banner current status changes to `Restarting agent`, and the button is deactivated until the agent is started.

Result: The ***Agent Control Panel*** closes and the agent restarts. After the restart completes, you can reopen the ***Agent Control Panel*** from ***Windows Control Panel***.

Server Details

This section lists information about the Ivanti Endpoint Security (Ivanti Endpoint Security) server the agent reports to.

The following table describes each **Server details** field.

Table 120: Server Details Field Descriptions

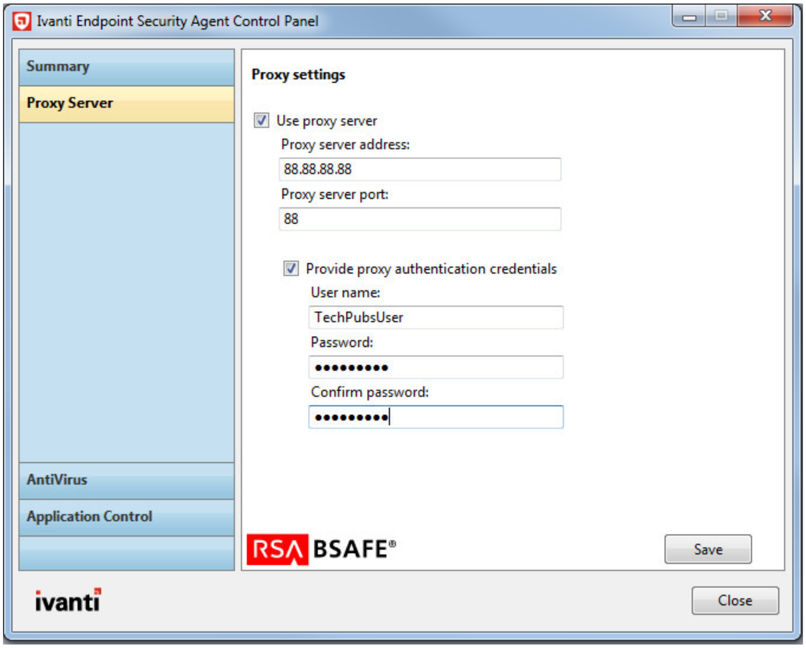
Field	Description
Server Identity	The name of the Ivanti Endpoint Security server in `http://ServerName.com` format. **Note:** If a proxy server is configured, the proxy name displays in the **Server Identity** field.

Field	Description
HTTP port	The port number the server uses for communication with the agent.
HTTPS port	The port number the server uses for secure communication with the agent.

The Proxy Server Panel

You can use this panel to define a proxy server that the agent will use to communicate with the Ivanti Endpoint Security Server.

You can use proxy servers to facilitate the communication between the agent and the server.



Proxy settings

☑ Use proxy server

Proxy server address: 88.88.88.88

Proxy server port: 88

☑ Provide proxy authentication credentials

User name: TechPubsUser

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

Figure 85: Proxy Server Panel

If you have configured a proxy server to serve as an intermediary between your Ivanti Endpoint Security Agents and your Ivanti Endpoint Security server, you can configure your Ivanti Endpoint Security Agent to use that proxy from the ***Proxy Server*** panel. This panel features user-definable fields you can complete to enable the Ivanti Endpoint Security Agent for proxy communication.

Note: If the Patch and Remediation endpoint module is installed on your endpoint, the fields for this panel are unavailable. On endpoints featuring the Patch and Remediation endpoint module, proxy configuration is defined using the Patch Agent.

Defining Proxy Settings

In environments that use a proxy server for communication between the server and agent, you must first define the proxy settings to enable proxy communication. You can also use this page to redefine proxy settings if change your reconfigure or remove your proxy server.

Prerequisites:

Your network features a functioning proxy server.

Edit proxy settings from the ***Proxy Server*** panel.

Note: You can also use this panel to redefine proxy settings or remove your proxy settings. On endpoints that have the Patch and Remediation endpoint module installed, proxy settings are unavailable. Instead, use the Patch Module to define proxy settings.

1. Select **Proxy Server** from the main menu.
2. Select the **Use proxy server** check box.
3. In **Proxy server address** field, type the proxy server IP address.
4. In the **Proxy server port** field, type the port number that the proxy server uses for communication.
5. If the proxy server required authentication, complete the following substeps.
   a) Select the **Provide proxy authentication credentials** check box.
   b) In the **User Name** field, type a user name that authenticates with the proxy.
   c) In the **Password** field, type the password associated with the user name.
   d) In the **Re-enter password** field, re-type the password.
6. Click **Save**.

Result: The agent is configured to communicate using the proxy.

Chapter 15

Purging Events from the Database

In this chapter:

The ***Database Maintenance*** page lets you schedule regular Ivanti Endpoint Security database purges to remove old Application Control and Device Control events. This frees up disk space and improves query performance.

Note: You must have Application Control and/or Device Control for the ***Database Maintenance*** feature to be available in the Server Console (**Tools** > **Database Maintenance**).

About Event Purging

Stored events become less useful and relevant over time, and their build-up can lead to performance issues. The ***Database Maintenance*** page lets you safely remove old events and keep a smaller, faster database.

Note: You must have Application Control and/or Device Control for the ***Database Maintenance*** feature to be available in the Server Console (**Tools** > **Database Maintenance**).

Device Control records all connections and other events related to devices, while Application Control records applications being allowed to run or blocked. As events can lead to the database quickly expanding in size, periodically removing them will:

- make all related reports and dashboard widgets load faster;
- free-up disk space for storing new events.

By default the database does not automatically remove events it stores. Running regular purges is a best practice we recommend you set up in your environment. The number and types of events kept should be according to your organization's business needs.

Caution: Purging is irreversible! Use care when configuring a purge job to avoid removing necessary data by accident. Once purged the events no longer appear in the server console.

Consider backing-up the database or exporting the results of a log query for a date range that matches the age of events you plan to purge.

You can configure a regular purge job using the ***Schedule Maintenance: Recurring Purge Job*** wizard on the **Tools** > **Database Maintenance** page. Events become eligible for purging when they exceed the minimum age you specify in the **Purge events older than X days** field.

Tip: The events that occur the most are:

- Device Control: `READ-DENIED`, `DEVICE-ATTACHED`
- Application Control: `Application execution granted`, `Trusted Updater added file to whitelist`, `Trusted Updater action information`

They are selected by default on the ***Select Events to Purge*** panel of the ***Schedule Maintenance: Recurring Purge Job*** wizard.

Though purge jobs can run while new events are being processed, we recommend that you schedule them for off-peak hours. Use a purge job's **Maximum purge duration** to manage purge time (minutes) and server load. At time-out the system finishes the event batch it is purging and then stops.

Scheduling a Recurring Purge Job for Events

You can ensure database performance stays healthy by scheduling a purge job that regularly removes old events (for example, all those older than three months).

Prerequisites:

- You must have a role with **Database Maintenance** Access Rights, both **View Purge Data And Log Files Tab** and **Manage Maintenance**.
- You have checked that no purge job will be running at your planned start date and time, or else your job will fail.
- If you need to keep a history of events, you must do one of the following:
  - back-up the database;
  - export the results of a log query for a date range that matches the age of events you plan to purge.

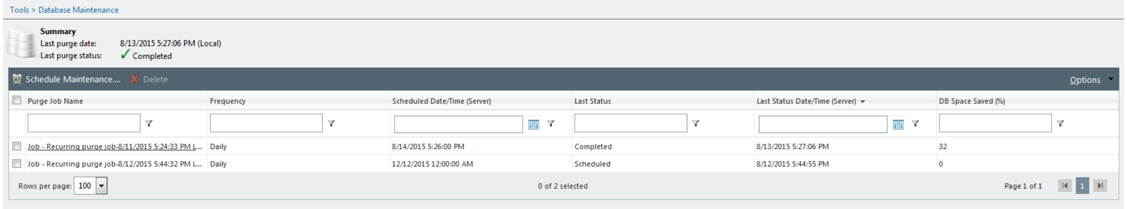
Periodically reviewing and purging old event data will ensure your query times are kept as low as possible, and generally improve system performance.

Caution: Purging is irreversible! Use care when configuring a purge job to avoid removing necessary data by accident. Once purged the events no longer appear in the server console.

Consider backing-up the database or exporting the results of a log query for a date range that matches the age of events you plan to purge.

1. From the Navigation Menu, select **Tools** > **Database Maintenance**.

   Step Result: The ***Database Maintenance*** page displays.



Tools > Database Maintenance

Summary
Last purge date: 8/13/2015 5:27:06 PM (Local)
Last purge status: ✓ Completed

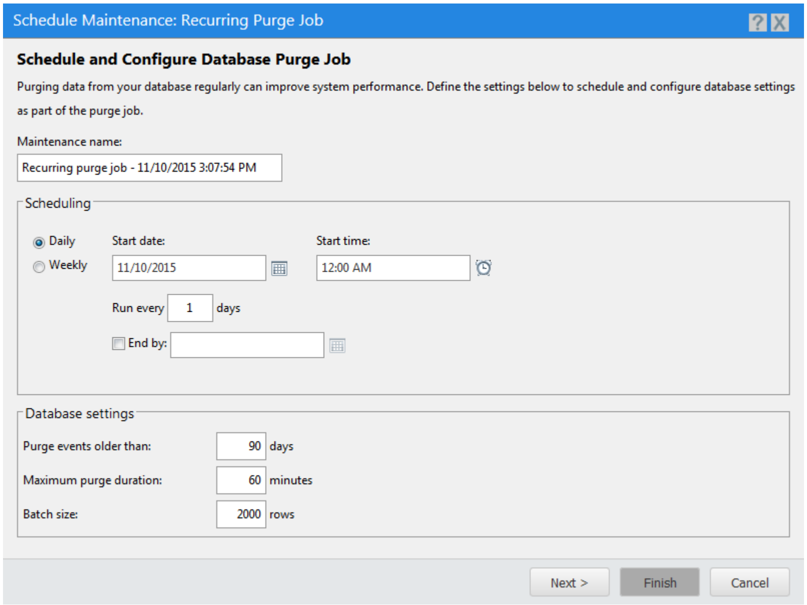
Schedule Maintenance.... Delete | Options

□	Purge Job Name	Frequency	Scheduled Date/Time (Server)	Last Status	Last Status Date/Time (Server)	DB Space Saved (%)
□	Job - Recurring purge job-8/11/2015 5:24:33 PM L...	Daily	8/14/2015 5:26:00 PM	Completed	8/13/2015 5:27:06 PM	32
□	Job - Recurring purge job-8/12/2015 5:44:32 PM L...	Daily	12/12/2015 12:00:00 AM	Scheduled	8/12/2015 5:44:55 PM	0

Rows per page: 100 | 0 of 2 selected | Page 1 of 1 | 1

2. Click **Schedule maintenance**.

   Step Result: The ***Schedule Maintenance: Recurring Purge Job*** wizard opens to the ***Schedule and Configure Database Purge Job*** panel.



Schedule Maintenance: Recurring Purge Job

Schedule and Configure Database Purge Job

Purging data from your database regularly can improve system performance. Define the settings below to schedule and configure database settings as part of the purge job.

Maintenance name: Recurring purge job - 11/10/2015 3:07:54 PM

Scheduling

● Daily
○ Weekly

Start date: 11/10/2015
Start time: 12:00 AM
Run every 1 days
□ End by:

Database settings

Purge events older than: 90 days
Maximum purge duration: 60 minutes
Batch size: 2000 rows

3. Enter a name for the purge job in the **Maintenance name** field.

   Specify a unique name for the job to help you destinguish it among others on the ***Database Maintenance*** page. By default the name is `Recurring purge job -[current date][current time]`.

   Consider using a name that reflects characteristics of the job, such as:

   - Type of events it purges (`PurgeDeviceDeniedEvents_Daily`)
   - Time it runs (`8:30AM_Daily_Purge_Job`)
   - Days it runs (`Mon_Wed_Fri_Purge_Job`)
   - Age of events to purge (`Remove_90_Day_Events`)

4. Select the frequency of the job: **Daily** or **Weekly**.
5. Enter or select the date you want the job to start in the **Start date** field. It must be in the MM/DD/YYYY date format (for example, `05/18/2015`).
6. Enter or select the time you want the recurring purge job to start in the **Start time** field. It must be in the 12-hour time format (for example, `1:00 PM`).
7. Enter the interval that you want the purge to occur in the **Run every** field. If you selected a frequency of Weekly, also select the days of the week the purge is to take place.
8. [Optional] Enter or select the date on which you want to job to end. It must be in the MM/DD/YYYY date format (for example, `05/18/2015`).

Now configure the database settings for the job.

9. Set the minimum age of events (integer representing days) you want the job to purge in the **Purge events older than** field.

   Only events older than the specified number are eligible for deletion. For example, if you enter 100 days all events 101 days and older are removed. Default: 90 days

10. Set the maximum number of minutes that the purge job can run in the **Maximum purge duration** field.

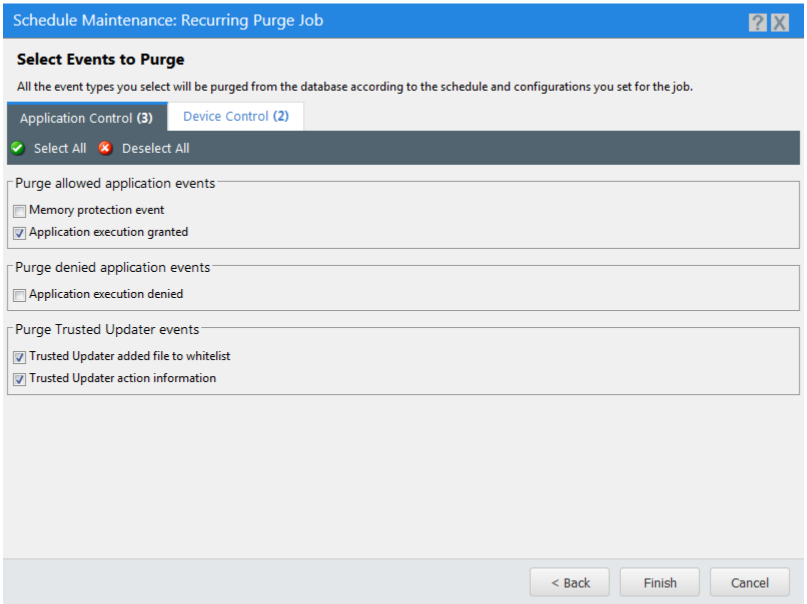
    You may want to limit the purge duration so, for example, it does not coincide with replication or import/export tasks. The purge stops when the minutes set expire and the system finishes the current batch it is purging. Depending on how long it takes your database to purge a batch of a particular size, this can add several minutes to the actual purge duration. Default: 60 minutes

11. Set the number of rows to be included in each batch operation in the **Batch size** field.

    A single purge typically includes multiple batch deletions. Larger batch sizes mean bigger database transactions and more database locks, as well as a purge durations exceeding your maximum setting. Default: 2000 rows

12. Click **Next**.

    Step Result: The ***Select Events to Purge*** panel is displayed.



Select Events to Purge

All the event types you select will be purged from the database according to the schedule and configurations you set for the job.

Purge allowed application events

- □ Memory protection event
- ☑ Application execution granted

Purge denied application events

- □ Application execution denied

Purge Trusted Updater events

- ☑ Trusted Updater added file to whitelist
- ☑ Trusted Updater action information

13. Select all the event types (minimum one) you want purged from the database according to the schedule and configurations you have set for the job.

The most common events are selected by default:

- Device Control: `READ-DENIED`, `DEVICE-ATTACHED`
- Application Control: `Application execution granted`, `Trusted Updater added file to whitelist`, `Trusted Updater action information`

The events types available are:

Application Control tab

Table 121: Purge allowed application events

Event	Description
Memory protection event	Unauthorized code from outside the local file system was block from executing within an authorized process running in memory.

Event	Description
Application execution granted	An Application Control policy allowed an application to run on an endpoint.

Table 122: Purge denied application events

Event	Description
Application execution denied	An Application Control policy prevented an application from running on an endpoint.

Table 123: Purge Trusted Updater events

Event	Description
Trusted Updater added file to whitelist	A Trusted Updater policy specified an executable file that is allowed to run on an endpoint.
Trusted Updater action information	Information about actions performed by the Trusted Updater.

Device Control tab

Table 124: Purge device connection events

Event	Description
MEDIUM-INSERTED	User inserted a CD/DVD or removable media reader.
DEVICE-ATTACHED	Device was connected to an endpoint. (selected by default)

Table 125: Purge device denied events

Event	Description
QUOTA-EXCEEDED	User exceeded the daily copy limit.
READ-DENIED	User attempted to access an unauthorized device. (selected by default)
WRITE-DENIED	User attempted to write a file to a read-only device.

Event	Description
WLAN-BLOCKED	User attempted to connect to a device through WLAN.

Table 126: Purge file/print shadowing events

Note: Purging these events will not remove the Full File Shadow files associated with them. Device Control stores the files in `<install_dir>\DeviceControl\Shadow` and you need to be remove them separately.

The `<install_dir>` can be changed in **Tools** > **Options** > **Device Control tab** > **Server shadow directory field**.

Event	Description
WRITE-GRANTED	User copied data to an authorized device.
READ-GRANTED	User accessed data on an authorized device.

Table 127: Purge keylogger events

Event	Description
KEYLOGGER-DETECTED	A keylogger was detected.
KEYBOARD-DISABLED	User keyboard was disabled because a keylogger may be present.

14. Click **Finish**.

Result: You have scheduled a recurring purge job and it appears in the ***Database Maintenance*** page list.

After Completing This Task:

- After a job has run (Completed or Failed) you can click its name in the list to view its Purge Result Details page.
- Delete a purge job from the Database Maintenance list.

Viewing Scheduled Recurring Purge Jobs

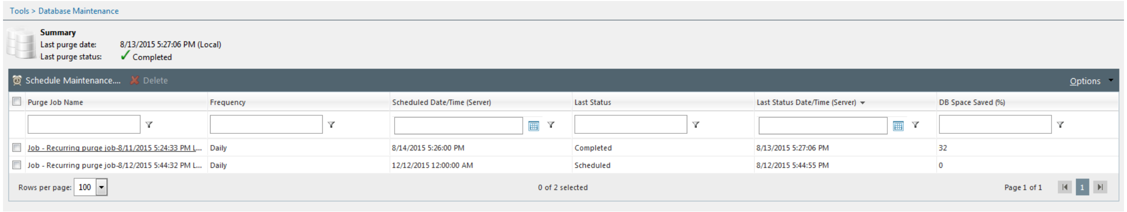
You can view a list of scheduled recurring purge jobs on the ***Database Maintenance*** page.

Prerequisites:

You must have a role with the **Database Maintenance** access right **View Purge Data And Log Files Tab**.

From the Navigation Menu, select **Tools** > **Database Maintenance**.

Result: The ***Database Maintenance*** page displays and scheduled recurring purge jobs are listed. If necessary, sort the list to find a specific job.



Tools > Database Maintenance

Summary
Last purge date: 8/13/2015 5:27:06 PM (Local)
Last purge status: ✓ Completed

Schedule Maintenance.... Delete — Options

□	Purge Job Name	Frequency	Scheduled Date/Time (Server)	Last Status	Last Status Date/Time (Server)	DB Space Saved (%)
□	Job - Recurring purge job-8/11/2015 5:24:33 PM L...	Daily	8/14/2015 5:26:00 PM	Completed	8/13/2015 5:27:06 PM	32
□	Job - Recurring purge job-8/12/2015 5:44:32 PM L...	Daily	12/12/2015 12:00:00 AM	Scheduled	8/12/2015 5:44:55 PM	0

Rows per page: 100 — 0 of 2 selected — Page 1 of 1

Table 128: Application Control Log Queries

Column	Description
Purge Job Name	Unique name of the purge job. The name is a hyperlink if the purge has run already.
Frequency	Repeat frequency of the purge job: Daily, Weekly.
Scheduled Date/Time (server)	Point in time when the next scheduled purge job is to take place.
Last Status	Current status of the purge job: Scheduled, In progress, Failed, Completed.
Last Status Date/Time (server)	Point in time when the current status was taken.
DB Space Saved (%)	Amount of database space saved by the purge in percent. This is an approximate figure as the system continues to log events while the purge is being performed.

Viewing the Results of a Completed Recurring Purge Job

You can examine the details of a completed Recurring Purge Job on its ***Purge Result Details*** page.

Prerequisites:

- You must have a role with **Database Maintenance** Access Rights, both **View Purge Data And Log Files Tab** and **Manage Maintenance**.
- The purge job must have a **Last Status** of `Completed`.

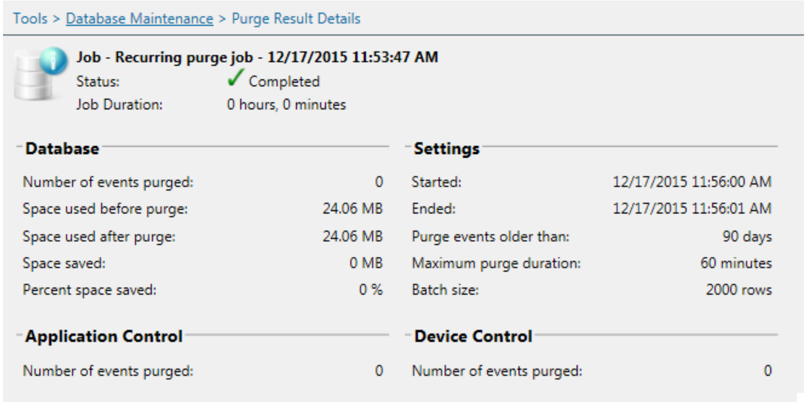
1. From the Navigation Menu, select **Tools** > **Database Maintenance**.

   Step Result: The ***Database Maintenance*** page displays and scheduled recurring purge jobs are listed. If necessary, sort the list to find the job you want to view.

2. In the **Purge Job Name** column, click the name of the job you want to view details for.

Result: The ***Purge Result Details*** page is displayed, containing information about the last job that completed for the selected recurring job.

> **Tip:** You can also view the purge trace log file `edsrolling_Workflow.DatabaseMaintenance.log`, stored on the Ivanti Endpoint Security server in `<install_dir>/EMSS/Endpoint Distribution services/logs`.



Tools > Database Maintenance > Purge Result Details

Job - Recurring purge job - 12/17/2015 11:53:47 AM

Status: ✓ Completed

Job Duration: 0 hours, 0 minutes

Database

Number of events purged:	0
Space used before purge:	24.06 MB
Space used after purge:	24.06 MB
Space saved:	0 MB
Percent space saved:	0 %

Settings

Started:	12/17/2015 11:56:00 AM
Ended:	12/17/2015 11:56:01 AM
Purge events older than:	90 days
Maximum purge duration:	60 minutes
Batch size:	2000 rows

Application Control

Number of events purged: 0

Device Control

Number of events purged: 0

Table 129: General Purge Job Information

Field	Description
Recurring Purge Job	The name of the recurring purge job.
Status	The purge job's status: Completed or Failed.
Job Duration	The duration of the purge job (displayed in hours and minutes).

Table 130: Database Section

Field	Description
Number of events purged	Quanity of events purged during the job.
Space used before purge	Amount of space the database occupied before the purge (in MB).

Field	Description
Space used after the purge	Amount of space the database occupies following the purge (in MB).
Space saved	Amount of space freed during the purge (in MB).
Percent space saved	Percentage of hard drive space saved when comparing the **Space used after the purge** and the **Space saved** values. This is an approximate figure as the system continues to log events while the purge is being performed.

Table 131: Settings Section

Field	Description
Started	Date and time the purge job commenced (server time).
Ended	Date and time the purge job ended (server time).
Purge events older than	Minimum age of events (integer representing days) that the job purged. Only events older than the specified number were eligible for deletion.
Maximum purge duration	Maximum number of minutes that the purge job was set to run.
Batch size	Number of rows set to be included in each batch operation.

Table 132: Application Control and Device Control Sections

Field	Description
Number of events purged	Quanity of Application Control and/or Device Control purged during the job.

Deleting a Scheduled Recurring Purge Job

You can delete a recurring purge job if it is no longer needed, even if it has never run.

Prerequisites:

- You must have a role with **Database Maintenance** Access Rights, both **View Purge Data And Log Files Tab** and **Manage Maintenance**.
- The purge job must not have a **Last Status** of `Running`.

Removing a purge job also deletes information about its last completed job.

1. From the Navigation Menu, select **Tools** > **Database Maintenance**.

   Step Result: The ***Database Maintenance*** page displays and scheduled recurring purge jobs are listed. If necessary, sort the list to find the job you want to delete.

2. Select the check box next to the purge job you want to delete.
3. Click **Delete**.

   Step Result: A confirmation dialog opens.

4. Click **Yes**.

Result: You have deleted the scheduled recurring purge job.

After Completing This Task:
You can now schedule a new Recurring Purge Job.

Schedule and Configure Database Purge

Use this wizard panel to set the frequency and at which the purge jobs are to occur.

Field	Description
Maintenance name	Specify a unique name for the job to help you destinguish it among others on the ***Database Maintenance*** page. By default the name is `Recurring purge job -[current date][current time].` Consider using a name that reflects characteristics of the job, such as: • Type of events it purges (`PurgeDeviceDeniedEvents_Daily`) • Time it runs (`8:30AM_Daily_Purge_Job`) • Days it runs (`Mon_Wed_Fri_Purge_Job`) • Age of events to purge (`Remove_90_Day_Events`)

Scheduling

Field	Description
Daily	Select if you want to run the purge daily.
Weekly	Select if you want to run the purge weekly.
Start date	Enter the date you want the recurring purge job to start. It must be in the MM/DD/YYYY date format (for example, `05/18/2015`), not text such as "May 18, 2015". Click the date icon 📅 to display a calendar from which you can select a date.

Field	Description
Start time	Enter the time you want the recurring purge job to start. It must be in the 12-hour time format (for example, `1:00 PM`). Click the time icon 🕒 to display 30-minute intervals you can select.
Run every	Enter the interval that you want the purge to occur. If you selected a frequency of Weekly, also select the days you want the job to run.

Database settings

Field	Description
Purge events older than	Set the minimum age of events (integer representing days) you want the job to purge. Only events older than the specified number are eligible for deletion. For example, if you enter 100 days all events 101 days and older are removed. Default: 90 days
Maximum purge duration	Set the maximum number of minutes that the purge job can run. You may want to limit the purge duration so, for example, it does not coincide with replication or import/export tasks. The purge stops when the minutes set expire and the system finishes the current batch it is purging. Depending on how long it takes your database to purge a batch of a particular size, this can add several minutes to the actual purge duration. Default: 60 minutes
Batch size	Set the number of rows to be included in each batch operation. A single purge operation typically includes multiple batch deletions. Larger batch sizes mean bigger database transactions and more database locks. Default: 2000 rows

Select Events to Purge

Use this wizard panel to select the types of events you want to purge from the database. The most common events types are selected by default.

Application Control tab

Table 133: Purge allowed application events

Event	Description
Memory protection event	Unauthorized code from outside the local file system was block from executing within an authorized process running in memory.

Event	Description
Application execution granted	An Application Control policy allowed an application to run on an endpoint.

Table 134: Purge denied application events

Event	Description
Application execution denied	An Application Control policy prevented an application from running on an endpoint.

Table 135: Purge Trusted Updater events

Event	Description
Trusted Updater added file to whitelist	A Trusted Updater policy specified an executable file that is allowed to run on an endpoint.
Trusted Updater action information	Information about actions performed by the Trusted Updater.

Device Control tab

Table 136: Purge device connection events

Event	Description
MEDIUM-INSERTED	User inserted a CD/DVD or removable media reader.
DEVICE-ATTACHED	Device was connected to an endpoint. (selected by default)

Table 137: Purge device denied events

Event	Description
QUOTA-EXCEEDED	User exceeded the daily copy limit.
READ-DENIED	User attempted to access an unauthorized device. (selected by default)
WRITE-DENIED	User attempted to write a file to a read-only device.

Event	Description
WLAN-BLOCKED	User attempted to connect to a device through WLAN.

Table 138: Purge file/print shadowing events

Note: Purging these events will not remove the Full File Shadow files associated with them. Device Control stores the files in `<install_dir>\DeviceControl\Shadow` and you need to be remove them separately.

The `<install_dir>` can be changed in **Tools** > **Options** > **Device Control tab** > **Server shadow directory field**.

Event	Description
WRITE-GRANTED	User copied data to an authorized device.
READ-GRANTED	User accessed data on an authorized device.

Table 139: Purge keylogger events

Event	Description
KEYLOGGER-DETECTED	A keylogger was detected.
KEYBOARD-DISABLED	User keyboard was disabled because a keylogger may be present.

Database Maintenance

Use this page to view and manage your database purge jobs.

Summary	Information about the last completed purge date and status.
Schedule maintenance button	Click to launch the ***Schedule Maintenance: Recurring Purge Job*** wizard.
Delete button	Deletes scheduled and completed purge jobs you select in the list.

Column	Description
Purge Job Name	Unique name of the purge job. The name is a hyperlink if the purge has run already.
Frequency	Repeat frequency of the purge job.
Scheduled Date/Time (server)	Point in time when the next scheduled purge job is to take place.

Column	Description
Last Status	Current status of the purge job: Scheduled, In progress, Failed, Completed.
Last Status Date/Time (server)	Point in time when the current status was taken.
DB Space Saved (%)	Amount of database space saved by the purge in percent. This is an approximate figure as the system continues to log events while the purge is being performed.

Purge Result Details

Use this page to review the results for a recurring purge job.

Table 140: General Purge Job Information

Field	Description
Recurring Purge Job	The name of the recurring purge job.
Status	The recurring purge job's status.
Job Duration	The duration of the purge job (displayed in hours and minutes).

Table 141: Database Section

Field	Description
Number of events purged	Quanitty of events purged during the job.
Space used before purge	Amount of space the database occupied before the purge (in MB).
Space used after the purge	Amount of space the database occupies following the purge (in MB).
Space saved	Amount of space freed during the purge (in MB).
Percent space saved	Percentage of hard drive space saved when comparing the **Space used after the purge** and the **Space saved** values. This is an approximate figure as the system continues to log events while the purge is being performed.

Table 142: Settings Section

Field	Description
Started	Date and time the purge job commenced (server time).

Field	Description
Ended	Date and time the purge job ended (server time).
Purge events older than	Minimum age of events (integer representing days) that the job purged. Only events older than the specified number were eligible for deletion.
Maximum purge duration	Maximum number of minutes that the purge job was set to run. The purge terminates when the number of minutes expires and the system finishes the current batch it is purging.
Batch size	Number of rows set to be included in each batch operation.

Chapter 16

Reporting

In this chapter:

Ivanti Endpoint Security can generate a variety of reports summarizing network conditions.

Use these reports for internal reporting, management briefing, and assistance when using Ivanti Endpoint Security.

About Reports

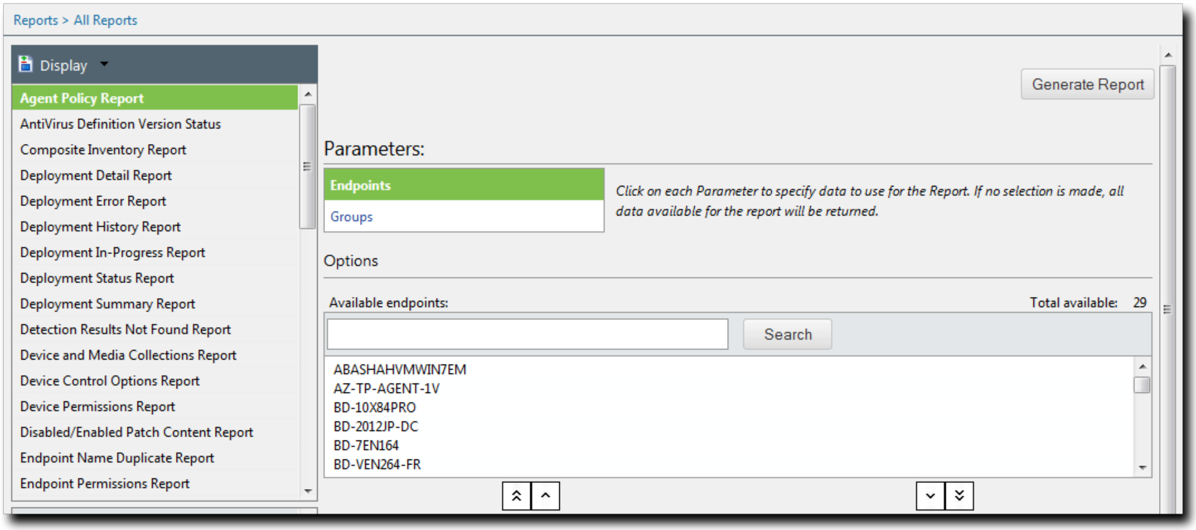
Reports are records that document activity and information pertaining to your network environment.

Generate reports to brief management or to view network behavior and statistics. Ivanti Endpoint Security offers multiple predefined report templates that list and/or depict data collected during network management. Data included in these reports range from general (endpoints, Discovery Scan Jobs) to highly detailed (operating systems installed on network endpoint). Reports are created by selecting a report type and defining its parameters.

Additionally, report formats vary. Some reports are in a HTML (`.html`) file format, while others are in a PDF (`.pdf`) format.

The All Reports Page

From this page, you can generate all available reports. Use this page to generate reports related Ivanti Endpoint Security functionality. Before generating a report, you select the report type and then define report parameters.


Reports > All Reports
Display
Agent Policy Report
AntiVirus Definition Version Status
Composite Inventory Report
Deployment Detail Report
Deployment Error Report
Deployment History Report
Deployment In-Progress Report
Deployment Status Report
Deployment Summary Report
Detection Results Not Found Report
Device and Media Collections Report
Device Control Options Report
Device Permissions Report
Disabled/Enabled Patch Content Report
Endpoint Name Duplicate Report
Endpoint Permissions Report
Generate Report
Parameters:
Endpoints
Groups
Options
Available endpoints:
Total available: 29
Search
ABASHAHVMWIN7EM
AZ-TP-AGENT-1V
BD-10X84PRO
BD-2012JP-DC
BD-7EN164
BD-VEN264-FR

Click on each Parameter to specify data to use for the Report. If no selection is made, all data available for the report will be returned.

Figure 86: All Reports Page

Note: From the **Reports** menu, you can select multiple ***All Reports*** page variants. Based on which **Reports** menu item you select, the resulting page that opens groups its **Display** menu differently. For example, selecting **Reports > Configuration** opens a reports page containing a **Display** menu with an expanded **Configuration** group. See the following table for a description of each **Reports** menu command.

Table 143: Reports Menu Commands

Command	Description
All Reports	Displays all reports ungrouped.
Configuration	Reports are grouped with the **Configuration** group expanded. Configuration reports display information about agent and job configurations.
Inventory	Reports are grouped with the **Inventory** group expanded. Inventory reports display information related to network assets and endpoint hardware and software.

Command	Description
Policy and Compliance	Reports are grouped with the **Policy and Compliance** group expanded. These reports display information about agent policy sets, Mandatory Baselines, and Mandatory Baseline endpoint compliance.
Management/Status	Reports are grouped with the **Management/Status** group expanded. These reports display information related to content deployments.

Viewing the All Reports Page

Navigate to this page to generate either HTML or PDF reports. Use this page to generate reports.

Access this page from the navigation menu.

1. Select **Reports** > **All Reports**.
2. [Optional] Generate the desired report.

   For additional information, refer to Generating a Report on page 345.

The Display List

This list displays all reports for generation. To generate a report, select it from the list.

If you select an ***All Reports*** page variant, the **Display** list items are grouped in a directory tree structure.

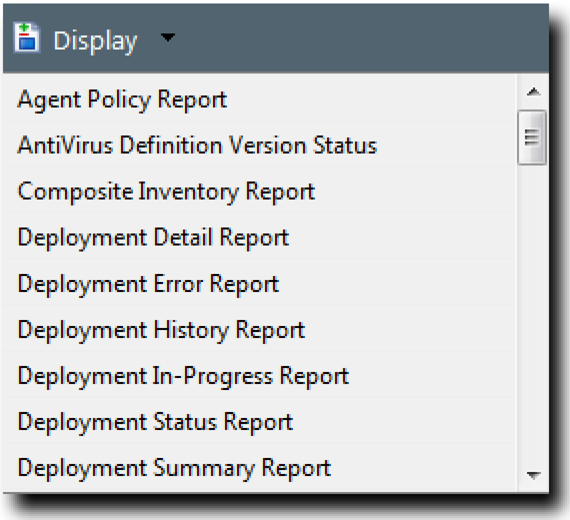

Display
Agent Policy Report
AntiVirus Definition Version Status
Composite Inventory Report
Deployment Detail Report
Deployment Error Report
Deployment History Report
Deployment In-Progress Report
Deployment Status Report
Deployment Summary Report

Figure 87: Display List

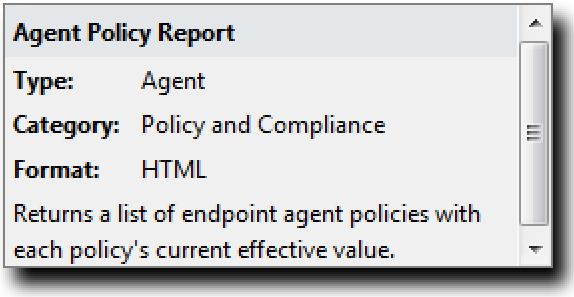
Additionally, the **Display** list contains the **Display** menu, which appears in the list's header. This menu lets you reorganize list items alphabetically or in a grouped directory tree structure. The following table describes each **Display** menu item.

Table 144: Display Menu Items

Item	Description
Sort Ascending	Sorts **Display** list items and/or groups in ascending alphabetical order. This is the default selection.
Sort Descending	Sorts **Display** list items and/or groups in descending alphabetical order.
All	Lists all available reports in an ungrouped format. This is the default selection.
Categories	Groups reports into different expandable and collapsible categories.

The Report Description

The report description summarizes the report selected from the **Display** list. Read this for a brief overview of the report you have selected.



Agent Policy Report

Type: Agent

Category: Policy and Compliance

Format: HTML

Returns a list of endpoint agent policies with each policy's current effective value.

Figure 88: Report Description

The following table describes the fields that appear in the report description, including the header.

Table 145: Report Description Fields

Field	Description
Report Description Header	The name of the report currently selected from the **Display** list.
Type	The data source of the report. Report data derives from either agents or network-based scans (Discovery Scan Jobs).
Category	The category of the report.
Format	The format of the report (`PDF` or `HTML`).

Generating a Report

Ivanti Endpoint Security provides multiple predefined reports. These reports comprehensively detail your computing environment, reflecting your content and vulnerability management activities. Generate reports to brief management or to view network behavior and statistics.

Generate reports from the ***All Reports*** page.

1. Select **Reports** > **All Reports**.
2. From the **Display** list, select the report you want to generate.
3. Define parameters using the available fields, drop-downs, lists, and so on. Each report has distinct required and optional parameters.

   Note: Refer to Available Core Reports on page 347 and the individual report descriptions for details regarding which parameters are required and which parameters are optional.

4. [Optional] Select the optional report parameters.
5. Click **Generate Report**.

   Step Result: The report generates.

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

Result: The report is generated in a new window.

Working with HTML Reports

After generating an HTML report, the report opens in a new window. Within this window, you can perform a number of tasks specific to the report.

- Displaying Time and Date in HTML Reports on page 346
- Exporting HTML Reports on page 346
- Previewing and Printing HTML Reports on page 346

Displaying Time and Date in HTML Reports

Some HTML reports generate date range data. For these reports, you can change how this data is formatted: either by local time or Coordinated Universal Time.

The following table describes the options for displaying date and time information.

Table 146: HTML Report Time and Date Display Options

Option	Description
Local Time	The date and time established by the Ivanti Endpoint Security Server.
UTC Time	Coordinated Universal Time. Also known as Universal Time, Zulu Time, or Greenwich Mean Time.

Exporting HTML Reports

After generating an HTML, you can export its data values into other file formats. You can then edit this data using other applications.

Once the HTML (`.html`) report is created, you have the option of exporting the report into another file format.

Reports are presented in standard HTML (`.html`) and can be exported into several file formats for your convenience.

- Comma Separated Values (`.csv`)
- Microsoft Excel Worksheet (`.XLS`)
- XML Document

To export the report, select an option from the list and click **Export**.

Note: All data results will export, not just selected results. However, some of the data may not export in a readable format.

Previewing and Printing HTML Reports

After generating a HTML (`.html`) report, you can format it specifically for printing. Use this feature before printing a report rather than using your Web browser print feature.

Prerequisites:

Generate a report.

1. Click the **Printer-friendly Version** link.

   Step Result: The report refreshes with the data in print preview mode.

2. [Optional] Click the **Send to Printer** link to print the report.

Result: The ***Print*** dialog opens. Finish printing your report by completing the ***Print*** dialog.

> **Note:** If printer connectivity is not established, you cannot print your report. Complete the ***Add Printer Wizard*** prior to printing reports if needed.

Working with PDF Reports

After generating a PDF (`.pdf`) report, you can view it within a PDF reader.

To generate a PDF (`.pdf`) report, you must have Adobe® Reader® (or another program such as Foxit® Reader) installed on your computer. When reading a generated report, the functions of these programs aid your report viewing.

For more information on system requirements for Adobe Reader, refer to Adobe Reader (http://get.adobe.com/reader/).

> **Tip:** For information on report creation, refer to How to create a PDF file from Adobe Reader (http://tv.adobe.com/watch/acrobat-xi-tips-tricks/how-to-create-a-pdf-file-from-adobe-reader/).

Available Reports

Ivanti Endpoint Security features a variety of reports. Each report documents Ivanti Endpoint Security activities and statistics.

The reports available for generation change based on which modules you have installed.

- Available Core Reports on page 347

Available Core Reports

Ivanti Endpoint Security provides various HTML and PDF formatted reports that display core data.

The following reports are available within Ivanti Endpoint Security when no modules are installed.

- Agent Policy Report on page 347
- Composite Inventory Report on page 348
- Job Configuration Report on page 349
- Network Inventory Report on page 351

Agent Policy Report

This report returns a list of endpoint agent policies. In the report, each policy value is listed in the **Policy Name** column. When using groups as a parameter to select multiple endpoints, the group policies are not part of the actual results.

Optional Parameters: `Endpoints`, `Groups`

> **Note:** If no parameter selection is made, the report generates using all available data.

The following table describes each report field.

Table 147: Agent Policy Report Column Definitions

Column	Definition
Device Name	The name of the endpoint.
Policy Name	The name of the agent policy.
Current Value	The policy setting.
Policy Desc	The agent policy's description.

Composite Inventory Report
This report lists details for endpoints associated with the specified agent groups and job (Discovery Scan or Agent Management). This report includes a pie chart that shows the agent status counts for the agent groups and scan job. A `Not Installed` agent status assigned to an endpoint that exists only in the job and not a selected agent group. Details are also displayed for each endpoint.

Required Parameters: Selection of one or multiple `agent group(s)` and one `completed job`.

Optional Parameters (default setting): `Sort by` (IP address, machine name, operating system [OS]), `Included OSs`, `Included IP addresses`.

This following table describes each report field and column.

Table 148: Composite Inventory Report Field and Column Definitions

Field / Column	Definition
General Information	
Server Name	The Ivanti Endpoint Security server name.
Agent Groups	The agent groups included in the report.
Job Name	The job name.
Date and Time Information	
Run Date	The date the selected job ran.
Start Time	The time the selected job began.
Duration	The duration of the selected job.
Version	The version of the scan engine in use.
Endpoint Inventory Summary	
Total Known Endpoints	The total number of endpoints with agents installed.
Agents Checking In	The number of agents checking in to the Ivanti Endpoint Security.

Field / Column	Definition
Online	The total number/percentage of endpoints online.
Agents Not Checking In	The number of agents that are not checking in to Ivanti Endpoint Security.
Offline	The number (or percentage) of agents that are offline.
Disabled	The number (or percentage) of agents that are disabled.
No Agent Installed	The number (or percentage) of endpoints with no agent installed.
Not Installed	The number (or percentage) of endpoints with no agent installed.
Endpoint Inventory Summary Graph	
Disabled	The number (or percentage) of agents that are disabled.
Not Installed	The number (or percentage) of endpoints with no agent installed.
Offline	The number (or percentage) of agents that are offline.
Online	The total number/percentage of endpoints online.
Total	The total number of endpoints assessed.
Composite Inventory Table	
Agent IP	The IP address of the endpoint the agent is installed on.
Agent Name	The name endpoint that hosts the agent.
Operating System	The operating system name and description.
Agent Status	The current status of the endpoint.

Job Configuration Report

This report comprehensively details a selected job's configuration. Use the ***Job Configuration*** report to document all configuration settings and options assigned to a selected job (Discovery Scan or Agent Management). This report generates a listing of discovery options used by a specific job and can be used to maintain configuration control.

Required Parameters: Selection of one `completed job`.

The following table describes each report field.

Table 149: Job Configuration Report Field Definitions

Field	Definition
General Information	
Job Name	The job name.

Field	Definition
Job Type	The job type.
Merged Job	Indicates if the job is a merged job (`True` or `False`).
Schedule Information	
Schedule Method	The job schedule method.
Start Time	The time the selected job began.
Version	The version of the scan engine in use.
Discovery Options	
Verify with Ping	Indicates if the **Verify with Ping** discovery option was selected.
ICMP Discovery	Indicates if **ICMP Discovery** was selected.
Port Scan Discovery	Indicates if **Port Scan Discovery** was selected.
SNMP Discovery	Indicates if **SNMP Discovery** was selected.
Windows Version Discovery	Indicates if **Windows Version Discovery** was selected.
Resolve DNS Names	Indicates if **Resolve DNS Names** was selected.
Resolve MAC Addresses	Indicates if **Resolve MAC Addresses** was selected.
Resolve NetBIOS Names	Indicates if **Resolve NetBIOS Names** was selected.
Scan Options	
Scan for Services	Indicates if the **Scan for Services** scan option was selected.
Scan for Shares	Indicates if **Scan for Shares** was selected.
Scan for Users	Indicates if **Scan for Users** was selected.
Scan for Groups	Indicates if **Scan for Groups** was selected.
Discovery Methods	
IP Range	Indicates a single IP address, wildcard IP address, or IP range designated for detection during a job. This field is associated with the **Single/Wildcard IP** and **IP Range** discovery methods.
Machine Name	Indicates the NetBIOS or DNS name of an endpoint designated for discovery during a job. This field is associated with the **Named Target** discovery method.

Field	Definition
Network Discovery	Indicates a network neighborhood designated for discovery during a job. This field is associated with the **Network Neighborhood** discovery method.
Credentials included in the credential set	
Credential Type	The type of credentials entered during job configuration (`Windows`, `Posix`, `SNMP`).
Description	A description of the credentials used.
User Name	The user name entered during job credential configuration. This field is associated with `Windows` and `Posix` credentials.
Community String	The community string entered during job credential configuration. This field is associated with `SNMP` credentials.
Note: The **Discovery Methods** and **Credentials included in the credential set** fields displayed depend on how the job was configured. For example, a report representing a job that did not use the **IP Range** discovery method will not display an **IP Range** field. Similarly, **Credential included in the credential set** fields are only populated if you entered credentials during job configuration.	

Network Inventory Report

This report lists the endpoints, along with basic identification information, that were discovered during a job (Discovery Scan or Agent Management).

Required Parameters: Selection of one `completed job`.

Optional Parameters: `Sort by` (IP Address, Machine Name, Operating System [OS]), `Included OSs`, `Included IP addresses`.

Note: Enter a single IP or a range of IP addresses (leave blank for all).

The following table describes the report field and columns.

Table 150: Network Inventory Report Field and Column Definitions

Field / Column	Definition
General Information	
Job Name	The job name.
Version	The version of the scan engine in use.
Target Information	
Targets Found	The number of endpoints discovered during scanning.

Field / Column	Definition
Non-responsive IP's	The number of IP addresses designated for discovery during job configuration that were unresponsive.
Date and Time Information	
Run Date	The date the selected job ran.
Start Time	The time the selected job began.
Duration	The duration of the selected job.
Network Inventory Table Columns	
Target IP	The IP address of the discovered endpoint.
Target Name	The DNS name of the endpoint.
Operating System	The operating system name and description.
MAC Address	The MAC address of the endpoint.

Appendix A

Server Reference

In this appendix:

Within Ivanti Endpoint Security, certain pages or code messages notify you of errors or events.

Refer to this appendix for a thorough definition of these pages and codes messages. This appendix also contains reference information regarding endpoint statuses, how to define scan targets using imported files, and how to restart the STATEngine Service.

Server Security

Ivanti Endpoint Security limits access to only authorized users. Referring to the definitions in this topic will help you understand how security operates within Windows and the product.

There are multiple layers of security for Ivanti Endpoint Security (Ivanti Endpoint Security). These layers include:

Web Site Authentication	Internet Information Services (IIS) controls authentication for access to the Ivanti Endpoint Security Web site, which means the operating system itself is validating credentials.
Web Site Encryption via SSL	SSL provides an encrypted wrapper around all Web communication to and from the product. Therefore, installing Ivanti Endpoint Security with SSL provides an additional level of protection.

User (Security) Roles	Every feature, page, and action throughout Ivanti Endpoint Security is assigned to a series of access rights. These access rights combine to form a user role. Roles also contain a list of accessible endpoints and endpoint groups. Regardless of how a user is authenticated, the access and permissions are defined solely by the Ivanti Endpoint Security administrator.

Server Error Pages

When an error occurs within Ivanti Endpoint Security, a special page opens that explains the error. Understanding these pages and what they mean will help you resume operations.

The Ivanti Endpoint Security (Ivanti Endpoint Security) server provides several distinct error pages. These pages are:

Access Denied	Displays when a user fails to provide valid credentials during log in to the Ivanti Endpoint Security server. Also display when a user attempts to access a page or feature they do not have access to.
Internal Server Error	Displays when an unspecified internal error occurs. In most cases, closing the browser window and restarting your task will resolve the issue.
Refresh User Data	Displays when the current session expires. Usually displays following an extended period of inactivity.
Requested Page Not Found	Displays when a user attempts to navigate to a nonexistent server address. This page features links to other pages. Users can navigate from these links back to the desired page.
System Component Version Conflict	Displays when a system component version conflict is detected. To ensure optimal behavior, the system components of Ivanti Endpoint Security are checked every time a user logs in. If a conflict is detected, this page identifies the component(s) that caused the conflict. **Note:** Ivanti Endpoint Security also sends a notification email to the Ivanti Endpoint Security administrator when a conflict occurs.
Cache Expired	Displays when the user session expires. Usually displays following an extended period of inactivity.
Unsupported Browser Version	Displays when a user attempts to open the Ivanti Endpoint Security server with an unsupported browser.

WinInet Error Codes

Ivanti Endpoint Security uses Microsoft Window Internet application programming interface (WinInet API) for communication between the server and agents. When agent-server communication fails, a WinInet error code displays. Understanding these codes can help you resolve the communication errors.

The following table defines the most common error codes.

Note: Refer to Microsoft Knowledgebase article #193625 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;193625) for additional WinInet error code descriptions.

Table 151: WinInet Error Code Descriptions

Agent Error Description	WinInet Error Code	Description
`Head failed: Head request failed. Error is 12002. . Host=1116 HTTP Error=0`	`12002`	The Internet connection timed out.
`Head failed: Head request failed. Error is 12031. . Host=1109 HTTP Error=0`	`12031`	The connection with the server has been reset.
`Head failed: Head request failed. Error is 12007. . Host=1109 HTTP Error=0`	`12007`	The server name could not be resolved.

HTTP Status Codes

As a Web-based application that uses Internet Information Services (IIS), Ivanti Endpoint Security subsequently uses HTTP status codes. These codes appear when an HTTP error occurs while using the product. Understanding these codes will help you solve any issue that may arise.

While many of the status codes are informational only, the following table defines a few of the common error codes.

Table 152: HTTP Status Codes

Code	Description
`HTTP 401.1 - Login failed`	Log in attempt was unsuccessful (typically due to invalid user name or password). **Note:** Ivanti Endpoint Security (Ivanti Endpoint Security) will display a custom error page (as defined under Server Error Pages on page 354) instead of the default ***HTTP 401.1 - Logon failed*** error page.
`HTTP 403.4 - SSL required`	You must use HTTPS instead of HTTP when accessing this page.
`HTTP 403.9 - Too many users`	The number of connected users exceeds the defined connection limit.
`HTTP 404 - Not found`	The requested file cannot be found. **Note:** Ivanti Endpoint Security will display a custom error page (as defined under Server Error Pages on page 354) instead of the default ***HTTP 404 - Not Found*** error page.

Defining Targets Using Wildcards

When configuring a Discovery Scan Job or Agent Management Job, you can define scan targets using *wildcard* IP addresses. Wildcards are characters can be used to substitute for any other character or characters in a string. In otherwords, you can use wildcards to scan for numerous IP address instead of just one. Use wildcards to scan specific IP address ranges.

The following table lists examples of how to define targets using wildcards.

Table 153: Wildcard Examples

Discovery Method	Step	Example	Targets Defined
To define wildcard IP addresses:	Type a wildcard IP address using commas (,). Type a wildcard IP address using dashes (-). Type a wildcard IP address using asterisks (*).	10.1.1.2,9 10.1.1.2-5 10.1.1.*	10.1.1.2 and 10.1.1.9 10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5 10.1.1.0 through 10.1.1.255
To define wildcard IP addresses using dashes in various octets:	Type a wildcard IP address using dashes, placing the dashes where applicable. You can use dashes in any octet.	10.2-4.5.9	10.2.5.9, 10.3.5.9, 10.4.5.9
To define wildcard IP addresses using asterisks in various octets:	Type a wildcard IP address using asterisks, placing the asterisks where applicable. You can use asterisks in any octet.	*.6.65.92 10.25.*.*	1.6.65.92 through 255.6.65.92 10.25.0.0 through 10.25.255.255
To define wildcard IP addresses using commas in various octets:	Type a wildcard IP address using commas, placing the commas where applicable. You can use commas in any octet.	10,12,19.2.5.9	10.2.5.9, 12.2.5.9, 19.2.5.9

Discovery Method	Step	Example	Targets Defined
To define wildcard IP addresses using a combination of wildcard characters:	Type a wildcard IP address using dashes, commas, and asterisks.	10-13.*.12.2,4,7 10.2-4.5,23.*	10, 11, 12, 13.0-255.12.2, 4, 7 10.2, 3, 4.5, 23.0-255

Defining Targets Within an Imported File

Using imported files, you can define job targets using a combination of single IP addresses, wildcard IP addresses, IP ranges, DNS names, NetBIOS names, and so on. To create a file containing targets, open a text editor that allows you to create `.txt` or `.csv` (like Notepad). This topic also explains how to use wildcards for any job type.

Using the ***Install Agents Wizard*** within an Agent Management Job you may define targets using an imported file.

The following table lists the methods you can use to define discovery methods within an importable file type, and then follows those methods with examples. Use one method per line.

Table 154: Basic Use

Discovery Method	Step	Example	Targets Defined
To define single IP addresses:	Type a single address.	10.1.1.2	10.1.1.2
To define wildcard IP addresses:	Type a wildcard IP address using commas (,). Type a wildcard IP address using dashes (-). Type a wildcard IP address using asterisks (*).	10.1.1.2,9 10.1.1.2-5 10.1.1.*	10.1.1.2 and 10.1.1.9 10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5 10.1.1.0 through 10.1.1.255
To define IP ranges:	Type two IP addresses separated by a greater-than sign (>). Type two IP addresses separated by a dash (-).	10.1.1.2 > 10.1.1.9 10.1.1.2 - 10.1.1.9	10.1.1.2 through 10.1.1.9 10.1.1.2 through 10.1.1.9
To define DNS names:	Type a DNS host name for an endpoint.	DNS.dom.com	The defined DNS name.

Discovery Method	Step	Example	Targets Defined
To define NetBIOS names:	Type a NetBIOS name for an endpoint.	NetBIOSname	The defined NetBIOS name.

Table 155: Advanced Use

Discovery Method	Steps	Examples	Targets Defined
To define wildcard IP addresses using dashes in various octets:	Type a wildcard IP address using dashes, placing the dashes where applicable. You can use dashes in the first, second, and last octet.	10.2-4.5.9	10.2.5.9, 10.3.5.9, 10.4.5.9
To define wildcard IP addresses using asterisks in various octets:	Type a wildcard IP address using asterisks, placing the asterisks where applicable. You can use asterisks in any octet.	*.6.65.92 10.25.*.*	1.6.65.92 through 255.6.65.92 10.35.0.0 through 10.35.255.255
To define wildcard IP addresses using commas in various octets:	Type a wildcard IP address using commas, placing the commas where applicable. You can use commas in first, second, and last octet.	10,12,19.2.5.9	10.2.5.9, 12.2.5.9, 19.2.5.9
To define wildcard IP addresses using a combination of wildcard characters:	Type a wildcard IP address using dashes, commas, and asterisks. You can use the dash and comma wildcards in the first, second, and lost octets. The asterick can be used in all octets.	10-13.*.12.2,4,7 10.2-4.5,23.*	10, 11, 12, 13.0-255.12.2, 4, 7 10.2, 3, 4.5, 23.0-255

Setting Up Ivanti Endpoint Security

Following installation and initial log in, the ***Application Setup Manager*** dialog opens. This dialog appears only once, the first time you log in to Ivanti Endpoint Security and you use it to configure basic options within the system.

Prerequisites:

Complete Ivanti Endpoint Security installation and open the Web console in your browser.

You cannot reopen this dialog following its completion. However, you can access these settings from various Ivanti Endpoint Security pages.

1. Log in to Ivanti Endpoint Security. For additional information, refer to Logging In on page 20.

   Step Result: Ivanti Endpoint Security opens to the ***Customer Info*** tab of the ***Application Setup Manager*** page. This dialog only appears the first time Ivanti Endpoint Security is opened.

2. Ensure the ***Customer Info*** tab is selected.
3. Type the applicable information in the following fields.

Field	Description
First name	Your first name.
Last name	Your last name.
Company name	Your company name. **Note:** The company name specified during installation appears by default, but can be edited.

4. Click **Apply**.

   Step Result: The information is saved.

5. Ensure the ***Uninstall Password*** tab is selected.
6. Define the **Global uninstall password**.

   This password is used to manually uninstall Ivanti Endpoint Security agents and should be kept confidential. Type the password in the following fields.

   a) In the **Global uninstall password** field, type the desired password.

b) In the **Confirm password** field, retype the password.

> **Tip:** For information on how to edit this password outside of the ***Application Setup Manager***, refer to Changing the Global Uninstall Password on page 250.

7. Click **Apply**.

   Step Result: The information is saved.

8. Select the ***Email Notifications*** tab.

9. Define the host and email information.

   Email notifications are alerts sent by Ivanti Endpoint Security when certain system events occur. Type the applicable information in the following fields.

Field	Description
SMTP Host	The local SMTP mail host name. Ivanti Endpoint Security uses your corporate Internet (SMTP) mail server.
'From' email address	The email address used when the system sends email notifications.
'To' email address	An email address you use to receive system notifications.

> **Important:** For additional details regarding Email Notifications, refer to The Email Notifications Page section within the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

10. Click **Apply**.

    Step Result: The information is saved.

11. Select the ***Install an Agent*** tab.

12. [Optional] The **Automatically install an agent on the server** check box is checked by default.

    This installs the agent on the server and is the recommended setting.

    a) Select the check boxes for the applicable modules.

       Selecting these modules activates agent functionality associated with the module.

> **Tip:** For additional information about installing an agent on the server outside of the ***Application Setup Manager***, refer to Downloading the Agent Installer on page 173.

13. Click **Apply**.

    Step Result: Your initial settings are saved.

14. Click **Close**.

    Step Result: The ***Application Setup Manager*** closes with your saved changes.

Result: Initial configuration is complete. You are now ready to begin monitoring your network with Ivanti Endpoint Security.

Restarting the STATEngine Service

If the STATEngine service is disabled on the Ivanti Endpoint Security, you will need to restart it before you can successfully complete Discovery Scan Jobs and Agent Management Jobs.

You can restart the STATEngine service using a command prompt.

Note: If you try to configure a Discovery Scan Job or Agent Management Job while the STATEngine service is stopped, a dialog will open, notifying you that the engine is stopped.

1. Log in to the Ivanti Endpoint Security server.
2. Select **Start** > **Run**.
3. Type `net start statengine`.
4. Click **OK**.

Result: The STATEngine is restarted. You can now configure Discovery Scan Jobs and Agent Management Jobs.

Appendix B

Securing Your Server

In this appendix:

Ivanti Endpoint Security protects your network endpoints. Server operation is critical to your network's overall security.

To ensure your server is secure as possible, Ivanti suggests implementing the following security practices:

- Secure Your Server With SSL on page 363
- Use Secure Passwords on page 364
- Disabling File and Printer Sharing on page 364
- Placing Your Server Behind a Firewall on page 364
- Disable Non-Critical Services on page 364
- Lock Down Unused TCP and UDP Ports on page 365
- Apply All Security Patches on page 365

Note: For additional information on securing your server, refer to Securing Your Application Server (http://msdn.microsoft.com/en-us/library/ff648657.aspx).

Secure Your Server With SSL

Implement Secure Sockets Layer (SSL) to secure all Ivanti Endpoint Security communication.

SSL is a protocol which is designed to provide secure data transmission over the Internet. SSL support is included in Web browsers, Web servers, and operating systems.

Ivanti Endpoint Security uses SSL when downloading vulnerability data and packages from the Global Subscription Service.

In addition, SSL can be used for transmitting data between the Ivanti Endpoint Security server and Ivanti Endpoint Security Agent by enabling SSL during the installation of Ivanti Endpoint Security. The installation process requires obtaining a SSL certificate (`.CER`). For details regarding installing with SSL enabled, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .

Use Secure Passwords

When setting passwords for Ivanti Endpoint Security, using secure passwords significantly lowers the probability that your server can be compromised.

Worm attacks, which attempt to install malicious software on a target endpoint, frequently test log ins with weak and commonly used passwords. For secure passwords, Ivanti recommends a 12 character password that combines mixed-case alpha characters, numeric characters, and punctuation characters.

Disabling File and Printer Sharing

When installing Ivanti Endpoint Security, you should disable the File and Printer Sharing for Microsoft Networks protocol on the target server. If this protocol is left active, it creates a security risk that intruders can exploit: a Windows networking share. Therefore, File and Printer Sharing for Microsoft Networks should be disabled.

Placing Your Server Behind a Firewall

Ivanti recommends placing your Ivanti Endpoint Security server behind a firewall. This procedure is considered best-practice.

Since the Ivanti Endpoint Security (Ivanti Endpoint Securityserver receives content updates from the Global Subscription Service (GSS), allowing the Ivanti Endpoint Security server specific Internet access is unnecessary. However, access to the GSS must be specified in your firewall configuration.

For details regarding install requirements, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .

Disable Non-Critical Services

Ivanti Endpoint Security only requires several essential services to operate. Disabling services that are not critical to its operation reduces security risks.

The default installation of Microsoft Windows sets most features and services to active. Therefore, there may be a number of services that can be disabled (e.g.: RPC, Remote Registry, etc.) to reduce security compromises. Ivanti does not encourage a lock down by disabling Windows services. However, it can be an effective method to reduce the risk of hacker attacks.

The following services are required to run Ivanti Endpoint Security:

- World Wide Web Publishing Service
- IIS Admin Service
- SQL Server
- Replication Service
- STATEngine
- EDS Server
- EDS InstallerService

Prior to disabling non-essential services, contact Ivanti Self Service Support (https://support.heatsoftware.com) to ensure disabling services does not impact your server performance.

Lock Down Unused TCP and UDP Ports

Unused ports within the Windows Server operating system pose a security risk to Ivanti Endpoint Security Servers. Therefore, these ports should be closed.

Use a firewall to prevent network traffic on various unused and vulnerable TCP and UDP ports. However, if a firewall is not available or additional server-level disablement is desired, TCP and UDP ports can be disabled as a function of the network connection.

Apply All Security Patches

The Ivanti Endpoint Security server should have the most recent security patches installed.

Apply all applicable Microsoft Security Patches to ensure that the server remains protected against all known security threats. Be sure to apply the most recent patches for Internet Information Services, SQL Server, and the version of Windows server in use.

Appendix C

Configuring the Server and Endpoints for Agent Management Jobs

In this appendix:

After installing Ivanti Endpoint Security on a server, you must perform additional configuration on the endpoints that you want to manage so that Agent Management Jobs will complete successfully.

Agent Management jobs consist of two parts: endpoint discovery and agent management itself. During discovery, the Ivanti Endpoint Security server locates the endpoint you want to install an agent on. During agent management, the agent is installed (or uninstalled). Discovery jobs run only the discovery process. Agent Management Jobs run the discovery process and the agent management process.

To configure a Windows endpoint for discovery or agent management, complete one of the following tasks:

1. Configuring Endpoints for Discovery on page 370
2. Configuring Endpoints for Agent Management Jobs on page 380

Tip: In environments where you want to prohibit Agent Management Jobs for security purposes, you can still discover endpoints with minimal security risk. To activate discovery functions (but not agent management) complete only the listed discovery procedures.

Agent Management Job Checklist

This checklist itemizes the information and tasks an administrator needs to perform prior to an Agent Management Job.

Prior to configuring your network to successfully use Agent Management Jobs, confirm the following information:

Tasks Performed on the Endpoint

- □ Verify that your target endpoints are all supported Windows endpoints. You cannot complete an Agent Management Job on Linux, UNIX, or Mac endpoints. For additional information, refer to the Ivanti Endpoint Security: Requirements Guide (https://help.ivanti.com) for a complete list of supported Windows operating systems.
- □ Ensure any antivirus software installed on target endpoints is disabled.
- □ Verify that your target endpoints have applicable ports open. Refer to Port and ICMP Requirements for an Agent Management Job on page 369.
- □ Configure your target endpoints to accept an Agent Management Job. Target endpoints must be configured to allow the Agent Management Job access to the endpoint. This includes verifying that the C$ and ADMIN$ network shares are enabled. Refer to Configuring Endpoints for Agent Management Jobs on page 380

Tasks Performed on the Server

- □ Verify that your Ivanti Endpoint Security server can utilize the Discovery Scanning process needed in by the Agent Management Job. Refer to Configuring the Ivanti Endpoint Security Server for Discovery Scanning on page 368.
- □ Gather credentials for the endpoints. A user name and password that authenticates with Windows-based endpoints is required during configuration of the Agent Management Job. Type the user name in a local format (UserName) or a domain format (DOMAIN\UserName).
- □ Gather proxy information if your agents will be required to use a proxy to access your Ivanti Endpoint Security server. The proxy information is required during configuration of the Agent Management Job that is using a proxy server.

Note: A Squid proxy server will only properly resolve using a fully qualified domain name.

Refer to Ivanti Community Article 59102 for additional information on a Squid proxy server configuration.

Configuring the Ivanti Endpoint Security Server for Discovery Scanning

The Ivanti Endpoint Security server must be configured to accept session security encryption so that you may run the Agent Management Job on your managed endpoints.

Prerequisites:

- Ivanti Endpoint Security (Ivanti Endpoint Security) is installed and initial replication has been completed. For details regarding installing Ivanti Endpoint Security, refer to the Ivanti Endpoint Security: Server Installation Guide (https://help.ivanti.com) .

On the server the authentication package for the local security authority has values defined in the server registry. You need to authenticate that the server has the correct security encryption value in order to run the Agent Management Job on endpoints within your network.

1. Log in to the Ivanti Endpoint Security server using an account with System Administrator privileges.
2. Open the ***Registry Editor***.
   a) From the **Start Menu** or **Start Screen**, open a **Run** prompt.
   b) Type `regedit.exe` and press `ENTER`.

   Step Result: The ***Registry Editor*** window opens.
3. Expand the registry tree to `HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Control\Lsa`.
4. Ensure the value for the `LmCompatibilityLevel` registry value is set to `3`.
   a) Ensure Lsa is selected in the registry tree.
   b) In the right-window area, select the `LmCompatibilityLevel` binary value.
   c) Right-click on the `LmCompatibilityLevel` binary value select **Modify**.

   Step Result: The ***Edit Binary*** dialog opens.

   d) Ensure `3` is visible in the **Value data** field. If not present, then change the value to `3`.

   > **Note:** Under most network conditions, a setting of 3 (Send NTLM 2 response only) is sufficient. However, in some networks, this key may require a different value. To determine which value to use, refer to How to Enable NTLM 2 Authentication (http://support.microsoft.com/kb/239869).

Result: The Ivanti Endpoint Security server is configured to utilize discovery scanning.

After Completing This Task:
If you are configuring the Ivanti Endpoint Security server for scanning in preparation for an Agent Management Job, ensure you have completed the tasks needed for an Agent Management Job. For additional information about endpoint configuration for an Agent Management Job, refer to Agent Management Job Checklist on page 367 for a description.

Port and ICMP Requirements for an Agent Management Job

Certain ports are required on the endpoint during the installation process of the Agent Management Job. Firewall configuration changes may be required to access applicable ports.

> **Note:** If your firewall policies cannot allow needed port access, contact Ivanti Self Service Support (https://support.heatsoftware.com) for a recommended configuration.

On the endpoint, open the ports listed in the following table.

Table 156: Required Ports

Required Ports	Direction	Description
• 445/TCP • 139/TCP • 135/UDP • 137/UDP	Inbound	Ivanti Endpoint Security uses these ports to access the endpoint during the installation of the Agent Management Job. After the Agent Management Job completes, you can close these ports. **Tip:** In addition, the Discovery Scan Job also use these ports to discover information about the endpoint.
• 443/TCP • 80/TCP	Outbound	Following agent installation, the Ivanti Endpoint Security Agent uses these ports to register and communicate with the Ivanti Endpoint Security server. After the Agent Management Job completes, you need to leave these ports open.

Both the Discovery Scan Job and the Agent Management Job requires the endpoint to accept ping requests from the Ivanti Endpoint Security server. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. Therefore, you need an exception within your endpoint firewall for inbound Internet Control Message Protocol (ICMP) echo request.

Refer to Enable or disable Internet Control Message Protocol requests for ICF (http://technet.microsoft.com/en-us/library/cc738771(v=ws.10).aspx) for additional information.

Configuring Endpoints for Discovery

For Ivanti Endpoint Security to discover Windows endpoints, they must have both network discovery and file sharing enabled. Target endpoints without these features enabled will not be discovered.

Note: If your organization uses a third-party firewall:

- Do not complete the steps in this procedure for creating Windows Firewall exceptions. Your third-party firewall makes them unnecessary.
- You must create exceptions for Ivanti Endpoint Security within you third-party firewall. For additional information, refer to Port and ICMP Requirements for an Agent Management Job on page 369.

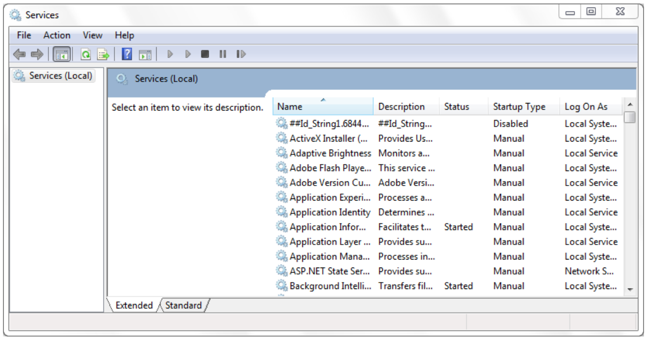
You can perform this procedure on endpoints with the following operating systems:

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

First, ensure that the services necessary for successful discovery scanning are started.

1. Open **Administrative Tools**.
2. Double-click **Services**.

   Step Result: The ***Services*** dialog opens.



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
##Id_String1.6844...	##Id_String...		Disabled	Local Syste...
ActiveX Installer (...	Provides Us...		Manual	Local Syste...
Adaptive Brightness	Monitors a...		Manual	Local Service
Adobe Flash Playe...	This service ...		Manual	Local Syste...
Adobe Version Cu...	Adobe Versi...		Manual	Local Service
Application Experi...	Processes a...		Manual	Local Syste...
Application Identity	Determines ...		Manual	Local Service
Application Infor...	Facilitates t...	Started	Manual	Local Syste...
Application Layer ...	Provides su...		Manual	Local Service
Application Mana...	Processes in...		Manual	Local Syste...
ASP.NET State Ser...	Provides su...		Manual	Network S...
Background Intelli...	Transfers fil...	Started	Manual	Local Syste...

Figure 89: Services Dialog

3. Ensure the necessary services are started.

   The following list itemizes the services that must be started for job completion.

   Note: In environments that use a third-party firewall, ensure the Windows Firewall service is instead *disabled*.

   - **DCOM Server Process Launcher**
   - **Remote Procedure Call (RPC)**
   - **Server**
   - **Windows Firewall**
   - **Windows Management Instrumentation**

   If all of the listed services required for your configuration purposes have a **Server status** of **Started**, continue to the next step. If any of the listed services for your configuration purposes are not started, complete the following substeps to start them.

   a) Right-click the applicable service and select **Properties**.

      Step Result: The properties dialog for the service opens.

   b) Ensure the **Startup type** list is set to **Automatic**. If edits are necessary, click **Apply** after selecting **Automatic** from the list.

   c) Click **Start**.

      Step Result: The service starts.

   d) Click **OK**

      Step Result: The properties dialog for the service closes.

   e) If necessary, repeat the substeps for each unstarted service.

4. Close the ***Services*** dialog and the ***Administrative Tools*** dialog.

   Tip: Leave ***Control Panel*** open.

Next, ensure your Network and Discovery settings are configured to allow discovery. The discovery setting allows the endpoint to be seen by the Ivanti Endpoint Security server during discovery scanning.

5. From ***Control Panel***, click **Network and Internet**.

   Step Result: ***Control Panel*** opens to the **Network and Internet** options.

6. Click **Network and Sharing Center**.

   Step Result: ***Control Panel*** opens to the ***Network and Sharing Center***.

7. Ensure **Network discovery** is enabled. Enabling this setting makes the endpoint publically known within network. Ivanti Endpoint Security uses the information shared by this setting to return more detailed information about the endpoint during discovery scanning.

   Based on the endpoint operating system, complete the applicable substeps that follow.

Operating System	Substep
Windows Server 2008 R2:	1. Click the arrow icon adjacent to **Network discovery**. 2. Ensure the **Turn on network discovery** option is selected. 3. If necessary, click **Apply**.
Windows 7:	1. Click **Change advanced sharing settings**. 2. Expand one of the following sections: • **Home or Work** • **Public** • **Domain** 3. Scroll to **Network discovery**. 4. Ensure the **Turn on network discovery** option is selected. 5. If necessary, click **Save Changes**. 6. Repeat these substeps for each profile section.
Windows 8 or Windows Server 2012:	1. Click **Change advanced sharing settings**. 2. Expand one of the following sections: • **Private** • **Guest or Public** • **Domain** 3. Scroll to **Network discovery**. 4. Ensure the **Turn on network discovery** option is selected. 5. Ensure the **Turn on automatic setup of network connected devices** option is cleared. 6. If necessary, click **Save Changes**. 7. Repeat these substeps for each profile section.

8. [Optional] Ensure **File sharing** is enabled.

   Tip: Completion of this step is optional. However, if you enable File Sharing, you must also create a firewall exception for it.

Based on the endpoint operating system, complete the applicable substeps that follow.

Operating System	Steps
Windows Server 2008 R2:	**1.** Click the arrow icon adjacent to **File Sharing**. **2.** Ensure the **Turn on file sharing** option is selected. **3.** If necessary, click **Apply**.
Windows 7:	**1.** Ensure you have clicked **Advanced sharing settings**. **2.** Expand one of the following sections: • **Home or Work** • **Public** • **Domain** **3.** Scroll to **File and printer sharing**. **4.** Ensure the **Turn on file and printer sharing** option is selected. **5.** If necessary, click **Save Changes**. **6.** Repeat these substeps for each profile section.
Windows 8 or Windows Server 2012:	**1.** Click **Change advanced sharing settings**. **2.** Expand one of the following sections: • **Private** • **Guest or Public** • **Domain** **3.** Scroll to **File and printer**. **4.** Ensure the **Turn on file and printer sharing** option is selected. **5.** If necessary, click **Save Changes**. **6.** Repeat these substeps for each profile section.

9. Close ***Network and Sharing Center***.

Step Result: ***Network and Sharing Center*** closes.

Next, ensure the Windows Firewall is configured to allow exceptions for discovery scans. A Windows Firewall that does not allow exceptions will blocks pings and other discovery scan processes. Ensure that firewall exceptions are in place for successful discovery scanning.

Create the firewall exceptions using the ***Local Group Policy Editor***. Create exceptions for both the standard and domain profiles.

Note: In environments using a third-party firewall, do not complete the steps to create Windows Firewall exceptions. Instead, create exceptions in your third-party firewall. For additional information, refer to Port and ICMP Requirements for an Agent Management Job on page 369.

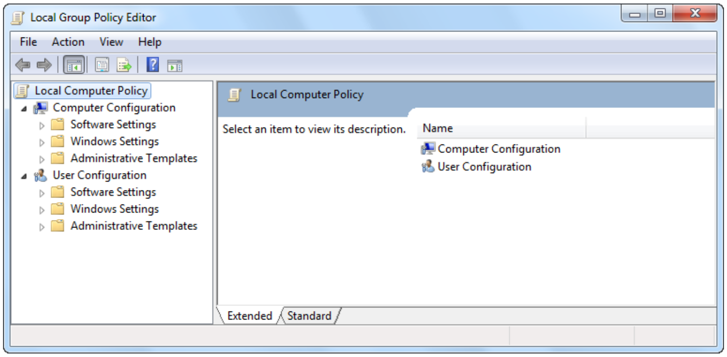
10. Open a run prompt.

Operating System	Steps
Windows 7 and Windows Server 2008 R2:	**1.** Select the **Start** menu. **2.** Type `run` in the **Search** field and press ENTER.
Windows 8 or Windows Server 2012:	**1.** Press the Windows Logo key. **2.** Type `run` and press ENTER.

Step Result: The ***Run*** prompt opens.

11. Type `gpedit.msc` in the **Open** field and press ENTER.

Step Result: The ***Local Group Policy Editor*** opens.



Select an item to view its description.

Figure 90: Local Group Policy Editor

Once you have selected the domain profile, you must configure the following firewall exception settings (and their subsettings) for discovery purposes.

- **Windows Firewall: Do not allow exceptions**
- **Windows Firewall: Allow inbound file and printer sharing exceptions**
- **Windows Firewall: Allow ICMP exceptions**

The following steps fully explain how to configure eash setting.

12. Expand the local computer policy tree to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profiles**. Ensure the **Domain Profiles** folder is selected.

13. Disable the **Windows Firewall: Do not allow exceptions** setting.

    a) From the main pane, right-click **Windows Firewall: Do not all exceptions** and select **Edit** (or **Properties**).

    Step Result: The setting dialog opens.

    b) Ensure the **Disabled** option is selected.
    c) Click **OK**.

    Step Result: The **Windows Firewall: Do not allow exceptions** setting is configured for agent management.

14. [Optional] Configure the **Windows Firewall: Allow inbound file and printer sharing exceptions** setting.

    Tip: Enable this setting if you turned on File and Printer Sharing earlier in the procedure.

    a) From the main pane, right-click **Windows Firewall: Allow inbound file and printer sharing exceptions** and select **Edit** (or **Properties**).

    Step Result: The setting dialog opens.

    b) Ensure the **Enabled** option is selected.
    c) [Optional] Define an IP range in the **Allow unsolicited incoming messages from** field. Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address.

    To define a range, you may use the following syntax. This input is not validated.

    - *`*`* (any IP address)
    - *`10.3.2.0/24`* (specific Class C subnet)
    - *`localsubnet`* (for local subnetwork access only)

    d) Click **OK**.

    Step Result: The **Windows Firewall: Allow inbound file and printer sharing exceptions** setting is configured for discovery scanning.

15. Configure the **Windows Firewall: Allow ICMP exception** setting.

    a) From the main pane, right-click **Windows Firewall: Allow ICMP exceptions** setting and select **Edit** (or **Properties**).

    Step Result: The setting dialog opens.

    b) Ensure the **Enabled** option is selected.
    c) Within **Options**, ensure the **Allow inbound echo request** check box is selected.
    d) Within **Options**, ensure all other check boxes are cleared.

e) Click **OK**.

Step Result: The **Windows Firewall: Allow ICMP exceptions** setting is configured for agent management.

After configuring firewall exceptions for the domain profile, you must also complete identical steps to configure firewall exceptions for your standard profile.

Configure the following settings for discovery purposes:

- **Windows Firewall: Do not allow exceptions**
- **Windows Firewall: Allow inbound file and printer sharing exception**
- **Windows Firewall: Allow ICMP exceptions**

The following steps fully explain how to configure each setting.

16. Expand the local computer policy tree to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Standard Profile**. Ensure the **Standard Profile** folder is selected.

17. Disable the **Windows Firewall: Do not allow exceptions** setting.

a) From the main pane, right-click **Windows Firewall: Do not all exceptions** and select **Edit** (or **Properties**).

Step Result: The setting dialog opens.

b) Ensure the **Disabled** option is selected.

c) Click **OK**.

Step Result: The **Windows Firewall: Do not allow exceptions** setting is configured for agent management.

18.[Optional] Configure the **Windows Firewall: Allow inbound file and printer sharing exceptions** setting.

Tip: Enable this setting if you turned on File and Printer Sharing earlier in the procedure.

a) From the main pane, right-click **Windows Firewall: Allow inbound file and printer sharing exceptions** and select **Edit** (or **Properties**).

Step Result: The setting dialog opens.

b) Ensure the **Enabled** option is selected.

c) [Optional] Define an IP range in the **Allow unsolicited incoming messages from** field. Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address.

To define a range, you may use the following syntax. This input is not validated.

- `*` (any IP address)
- *`10.3.2.0/24`* (specific Class C subnet)
- *`localsubnet`* (for local subnetwork access only)

d) Click **OK**.

Step Result: The **Windows Firewall: Allow inbound file and printer sharing exceptions** setting is configured for discovery scanning.

19. Configure the **Windows Firewall: Allow ICMP exception** setting.

a) From the main pane, right-click **Windows Firewall: Allow ICMP exceptions** setting and select **Edit** (or **Properties**).

Step Result: The setting dialog opens.

b) Ensure the **Enabled** option is selected.
c) Within **Options**, ensure the **Allow inbound echo request** check box is selected.
d) Within **Options**, ensure all other check boxes are cleared.
e) Click **OK**.

Step Result: The **Windows Firewall: Allow ICMP exceptions** setting is configured for agent management.

20. Close the ***Local Group Policy Editior*** (or the ***Group Policy Object Editor***).

Step Result:

Note: The creation of Windows Firewall exceptions opens the following ports, which are required for job completion:

- 445/TCP
- 139/TCP
- 135/UDP
- 137/UDP

Finally, complete configuration of your endpoint by ensuring the C$ and ADMIN$ network shares are shared. Enabling these shares lets the Ivanti Endpoint Security server access your endpoint.

21. Open the ***Command Prompt***.

Operating System	Steps
Windows 7 and Windows Server 2008 R2:	**1.** Select the **Start** menu. **2.** Type `cmd` in the **Search** field and press ENTER.
Windows 8 or Windows Server 2012:	**1.** Press the Windows Logo key. **2.** Type `cmd` and press ENTER.

22. From the ***Command Prompt***, type `net share` and press ENTER.

Step Result: The endpoint network shares are listed.

23. Ensure that the following shares are listed in the `Share name` column.

- `C$`
- `ADMIN$`

If they are already listed, proceed to the next step. If these shares are not listed, complete the following substeps to enable them. If one of the necessary shares is enabled but not the other, only enable the share that needs to be enabled.

a) From the ***Command Prompt***, type the necessary command(s) to enable any required network shares.

- To enable the C$ share, type `NET SHARE C$=C` and press ENTER.
- To enable the ADMIN$ share, type `NET SHARE ADMIN$` and press ENTER.

Step Result: You have enabled the required share(s). All enabled shares remain active until the system reboots.

24. Close the ***Command Prompt***.

Step Result: The ***Command Prompt*** closes.

Result: The endpoint is configured for discovery.

Configuring Endpoints for Agent Management Jobs

Prior to using an Agent Management Job to install agents on your Windows endpoints, you must first configure your endpoints.

Prerequisites:

Prior to configuring, review the following requirements:

- You can perform these steps on endpoints with the following operating systems:
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
- You have gathered and confirmed the information and tasks in the Agent Management Job checklist. Refer to Agent Management Job Checklist on page 367 for a description.

Note: If your organization uses a third-party firewall:

- Do not complete the steps for creating Windows Firewall exceptions. Your third-party firewall makes them unnecessary.
- However, you must create exceptions for Ivanti Endpoint Security within you third-party firewall. For additional information, refer to Port and ICMP Requirements for an Agent Management Job on page 369.

1. Start applicable Windows services.

Tip: There are specific Windows services that are necessary for successful Agent Management Job completion.

a) Open **Administrative Tools**.

b) Double-click **Services**.

Step Result: The ***Services*** dialog opens.

c) Ensure the necessary Windows services are started for an Agent Management Job.

The following list itemizes the services that must be started for Agent Management Job completion.

- **DCOM Server Process Launcher**
- **Remote Procedure Call (RPC)**
- **Server**
- **Windows Firewall**
- **Windows Management Instrumentation**

Note: In environments that use a third-party firewall, ensure the Windows Firewall service is instead *disabled*.

d) If all of the listed services required for your configuration purposes have a **Server status** of **Started**, continue to the next step. If any of the listed services for your configuration purposes are not started, complete the following:

1. Right-click the applicable service and select **Properties**.
2. Ensure **Startup type** list is set to **Automatic**. If edits are necessary, click **Apply** after selecting **Automatic** from the list.
3. Click **Start**.
4. Click **OK**.
5. If necessary, repeat the previous steps for each unstarted service.

e) Close the ***Services*** dialog and the ***Administrative Tools*** dialog.

Step Result: The applicable Windows services for a successful Agent Management Job are started.

2. Configure **Sharing and Discovery** settings.

Tip: The discovery setting allows the endpoint to be seen by the Ivanti Endpoint Security server, while the file sharing setting allows the Ivanti Endpoint Security server to install the agent during agent management. These settings are necessary for a successful Agent Management Job.

a) From ***Control Panel***, click **Network and Internet**.

Step Result: ***Control Panel*** opens to the **Network and Internet** options.

b) Click **Network and Sharing Center**.

Step Result: ***Control Panel*** opens to the ***Network and Sharing Center***.

c) Ensure **Network discovery** is enabled.

Enabling this setting makes the endpoint publicly known within the network.

Tip: Ivanti Endpoint Security uses the information shared by this setting to return more detailed information about the endpoint during discovery scanning.

Based on the endpoint operating system, complete the applicable steps.

Operating System	Step
Windows Server 2008 R2	**1.** Click the arrow icon adjacent to **Network discovery**. **2.** Ensure **Turn on network discovery** option is selected. **3.** If necessary, click **Apply**.
Windows 7	**1.** Click **Change advanced sharing settings**. **2.** Expand one of the following network locations: • **Home or Work** • **Public** • **Domain** **3.** Scroll to **Network discovery**. **4.** Ensure **Turn on network discovery** option is selected. **5.** If necessary, click **Save Changes**. **6.** Repeat these steps for each profile section.
Windows 8 or Windows Server 2012	**1.** Click **Change advanced sharing settings**. **2.** Expand one of the following network locations: • **Private** • **Guest or Public** • **Domain** **3.** Scroll to **Network discovery**. **4.** Ensure **Turn on network discovery** option is selected. **5.** Ensure **Turn on automatic setup of network connected devices** option is cleared. **6.** If necessary, click **Save Changes**. **7.** Repeat these steps for each profile section.

d) Ensure **File sharing** is enabled.

Based on the endpoint operating system, complete the applicable steps.

Operating System	Step
Windows Server 2008 R2	**1.** Click the arrow icon adjacent to **File Sharing**. **2.** Ensure **Turn on file sharing** option is selected. **3.** If necessary, click **Apply**.

Operating System	Step
Windows 7	**1.** Click **Advanced sharing settings**. **2.** Expand one of the following network locations: • **Home or Work** • **Public** • **Domain** **3.** Scroll to **File and printer sharing**. **4.** Ensure **Turn on printer sharing** option is selected. **5.** If necessary, click **Save Changes**. **6.** Repeat these steps for each profile section.
Windows 8 or Windows Server 2012	**1.** Click **Change advanced sharing settings**. **2.** Expand one of the following sections: • **Private** • **Guest or Public** • **Domain** **3.** Scroll to **File and printer**. **4.** Ensure **Turn on file and printer sharing** option is selected. **5.** If necessary, click **Save Changes**. **6.** Repeat these steps for each profile section.

e) Close ***Network and Sharing Center***.

Step Result: ***Network and Sharing Center*** closes.

Step Result: The **Sharing and Discovery** settings is configured for the Agent Management Job.

3. Ensure Windows Firewall is configured to allow exceptions.

Tip: A Windows Firewall that does not allow exceptions will block pings and other agent management processes necessary for a successful Agent Management Job.

a) Open a run prompt.

Operating System	Step
Windows 7 or Windows Server 2008 R2	**1.** Select the **Start** menu. **2.** Type `run` in the **Search** field and press `ENTER`.

Operating System	Step
Windows 8, or Windows Server 2012	**1.** Press the Windows Logo key. **2.** Type `run` and press `ENTER`.

Step Result: The ***Run*** prompt opens.

b) Type `gpedit.msc` in the **Open** field and press `ENTER`.

Step Result: The ***Local Group Policy Editor*** opens.

c) Expand the local computer policy tree to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profiles**. Ensure **Domain Profiles** folder is selected.

Step Result: The ***Domain Profile*** windows opens.

d) Ensure the following settings (and their subsettings) are configured for the **Domain Profile**.

Name	Step
Windows Firewall: Do not allow exceptions	**1.** Right-click and select **Edit** to open the setting dialog. **2.** Ensure **Disabled** option is selected. **3.** Click **OK**.
Windows Firewall: Allow inbound file and printer sharing exception	**1.** Right-click and select **Edit** to open the setting dialog. **2.** Ensure **Enabled** option is selected. **3.** Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • *`10.3.2.0/24`* (specific Class C subnet) • *`localsubnet`* (for local subnetwork access only) **4.** Click **OK**.

Name	Step
Windows Firewall: Allow ICMP exceptions	**1.** Right-click and select **Edit** to open the setting dialog. **2.** Ensure **Enabled** option is selected. **3.** Click **OK**.
Windows Firewall: Allow inbound remote administration exception	**1.** Right-click and select **Edit** to open the setting dialog. **2.** Ensure **Enabled** option is selected. **3.** Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • `10.3.2.0/24` (specific Class C subnet) • `localsubnet` (for local subnetwork access only) **4.** Click **OK**.

e) Expand the local computer policy tree to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Domain Profiles**. Ensure **Standard Profiles** folder is selected.

Step Result: The ***Standard Profile*** windows opens.

f) Ensure the following settings (and their subsettings) are configured for the **Standard Profile**.

Tip: These settings will mimic the **Domain Profile**.

Name	Step
Windows Firewall: Do not allow exceptions	**1.** Right-click and select **Edit** to open the setting dialog. **2.** Ensure **Disabled** option is selected. **3.** Click **OK**.

Name	Step
Windows Firewall: Allow inbound file and printer sharing exception	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • `10.3.2.0/24` (specific Class C subnet) • `localsubnet` (for local subnetwork access only) 4. Click **OK**.
Windows Firewall: Allow ICMP exceptions	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Click **OK**.
Windows Firewall: Allow inbound remote administration exception	1. Right-click and select **Edit** to open the setting dialog. 2. Ensure **Enabled** option is selected. 3. Define an IP range in the **Allow unsolicited incoming messages from** field. **Note:** Ivanti recommends defining this field using your Ivanti Endpoint Security Server IP address. This input is not validated. To define a range, you may use the following syntax: • `*` (any IP address) • `10.3.2.0/24` (specific Class C subnet) • `localsubnet` (for local subnetwork access only) 4. Click **OK**.

g) Close the ***Local Group Policy Editior*** (or the ***Group Policy Object Editor***).

Step Result:

> **Note:** The creation of Windows Firewall exceptions opens the following ports, which are required for job completion:
>
> - 445/TCP
> - 139/TCP
> - 135/UDP
> - 137/UDP

Step Result: The Windows Firewall is configured to allow exceptions for an Agent Management Job.

4. Complete the configuration of your endpoint by verifying that the C$ and ADMIN$ network shares are enabled.

> **Tip:** The C$ and ADMIN$ network shares are necessary for remote management. This is necessary for a successful Agent Management Job completion.

a) Open ***Control Panel***.

Operating System	Step
Windows 7 or Windows Server 2008 R2	**1.** Select the **Start** menu. **2.** Type `cmd` in the **Search** field and press `ENTER`.
Windows 8 or Windows Server 2012	**1.** Press the Windows Logo key. **2.** Type `cmd` and press `ENTER`.

b) From the ***Command Prompt***, type `net share` and press `ENTER`.

Step Result: The endpoint network shares are listed.

c) Ensure that the following shares are listed in the `Share name` column.

- `C$`
- `ADMIN$`

> **Note:** If these shares are not listed, complete the following steps to enable them. If one of the necessary shares is enabled but not the other, only enable the share that needs to be enabled.

d) From the ***Command Prompt***, type the necessary commands to enable the required network shares.

- To enable the C$ share, type `NET SHARE C$=C` and press `ENTER`.
- To enable the ADMIN$ share, type `NET SHARE ADMIN$` and press `ENTER`.

Step Result: You have enabled the required share(s). All enabled shares remain active until the system reboots.

e) Close the ***Command Prompt*** window.

Step Result: The ***Command Prompt*** closes.

Step Result: You have completed the configuration of your endpoint for an Agent Management Job by verifying that the C$ and ADMIN$ network shares are enabled.

Result: You have completed all necessary configuration steps.

After Completing This Task:
Refer to Agent Management Job Checklist on page 367 prior beginning the Agent Management Job.

Troubleshooting Agent Management Jobs

If agent managements are not completing successfully, additional configuration may be required.

If the Ivanti Endpoint Security server or an applicable network endpoint has lost its trust relationship with the domain, Agent Management Jobs will fail with an error of `access denied`.

To verify if this issue is causing Agent Management Job failure, ensure that the Ivanti Endpoint Security server can connect to the applicable endpoints C$, and that the applicable endpoints can connect to the server's C$. To verify these connections, type the following command from the applicable endpoint or server prompt: `\\`*`EndpointIPAddress`*`\C$`.

If the following system output results from the command, your endpoint or server has lost its trust relationship with the domain: `The trust relationship between this workstation and the primary domain failed`.

To resolve this issue, remove the applicable server or endpoint from the domain, and then add it back. This process forces the domain to refresh the endpoint password. The endpoint password prompts users for resetting at scheduled intervals according to its security settings.

To disable password changes, complete Disabling Password Changes on page 389.

Resolving Endpoint UAC Issues

On endpoints running Windows, UAC security features are set to highly restrictive levels by default. These settings must be configured properly to ensure Agent Management Job success.

When a Windows endpoint is in this default UAC configuration, Agent Management Jobs fail with an `access denied` error.

Use one of two methods to resolve this issue:

Add a domain account	Adding a domain account to the applicable endpoint's local administrator's group will typically resolve the issue. To use this method, add the endpoint to a domain (provided it isn't already added), and then add a domain user to the endpoint's local administrator group. Running an Agent Management Job configured to use this domain account's credentials will allow the job to complete successfully. **Note:** The domain account added to the local administrator's group *must* be an individual domain account; you cannot add a domain group.
Set a Registry Value	If the user of a local administrative account is desired or required, you can set a registry value to resolve this issue. Create a `DWORD` registry value named *LocalAccountTokenFilterPolicy* in the `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\` registry hive. Set its value to *1*. No reboot is required. This method allows a local administrative account to successfully run Agent Management Jobs. **Note:** Refer to How to change the Remote UAC LocalAccountTokenFilterPolicy registry setting (http://support.microsoft.com/kb/942817) for additional information about this method.

Disabling Password Changes

Do disable password changes, create a registry key for the applicable endpoint.

Perform this task from the applicable endpoint.

1. Select **Start** > **Run**.

   Step Result: The ***Run*** dialog opens.

2. Type `regedit` in the **Open** field.
3. Click **OK**.

   Step Result: The ***Registry Editor*** opens.

4. Expand the directory tree structure to `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`.
5. Right-click `DisablePasswordChange`.
6. Select **Modify**.

   Step Result: The ***Edit DWORD Value*** dialog opens.

7. In the **Value data** field, type `1`.
8. Click **OK**.

Result: The key value is updated. User profile passwords can no longer be edited on the applicable endpoint.

Appendix D

Creating a Disaster Recovery Solution

In this appendix:

- Preparing Your Database
- Creating a Manual Solution
- Creating an Automated Solution

Ivanti Endpoint Security uses Microsoft SQL Server to store data values; therefore, you should prepare your instance of Microsoft SQL Server for a disaster.

The most important part of an effective disaster recovery solution is having a current and valid backup. You can create backups either manually or as part of a Database Maintenance Plan.

Note: This appendix applies to Microsoft SQL Server 2008 and requires the Microsoft SQL Server Management Studio. The Management Studio is available by upgrading to SQL Server 2008 Standard or Enterprise. For further information, see Microsoft SQL Server 2008 (http://www.microsoft.com/sqlserver/2008/en/us/default.aspx).

Preparing Your Database

In the event of a disaster, detailed transaction logs are useful when restoring your database. You can control the level of detail that your logs record.

The installation of Ivanti Endpoint Security sets your database to a recovery model of `Simple`. To use *Transaction Logs*, and thus increase the quality of your disaster recovery solution, you should change the recovery model to `Full`.

Changing the Database Recovery Model

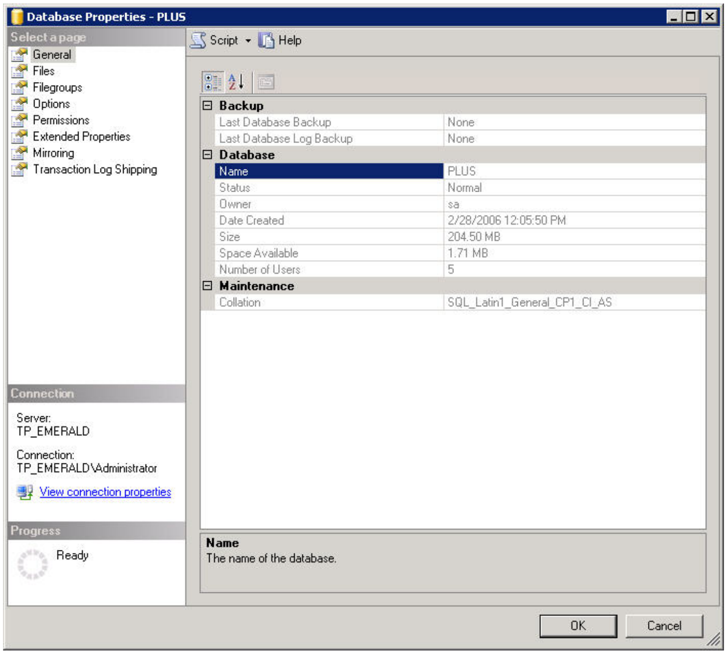
Modify the database recovery model to record more robust details about the events leading to a disaster.

Database recovery model edits take place in the ***SQL Server Management Studio***.

1. Open the ***Microsoft SQL Server Management Studio***.
2. Log into your database server.
3. In the directory tree, expand ***Server Name\SQL Instance*** > **Databases**.

4. Right-click the `PLUS` database.
5. Select **Properties**.

   Step Result: The ***Database Properties*** window opens.



Server:
TP_EMERALD

Connection:
TP_EMERALD\Administrator

Backup	
Last Database Backup	None
Last Database Log Backup	None
Database	
Name	PLUS
Status	Normal
Owner	sa
Date Created	2/28/2006 12:05:50 PM
Size	204.50 MB
Space Available	1.71 MB
Number of Users	5
Maintenance	
Collation	SQL_Latin1_General_CP1_CI_AS

Name
The name of the database.

Figure 91: Database Properties

6. In the **Select a Page** pane, click **Options**.

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

7. In the **Recovery model** list, select **Full**.

> **Note:** A full database backup backs up the whole database. This includes part of the transaction log so that full database backup can be recovered.

8. Click **OK**.

   Step Result: The changes are saved and the ***Database Properties*** window closes.

9. Repeat the recovery model modification process for the following databases:

Table 157: Database Names

Database Name	Product
`STAT_Guardian`	Ivanti Endpoint Security
`UPCCommon`	Ivanti Endpoint Security

Database Name	Product
UPCExtended	Ivanti Endpoint Security
PLUS_Reports	Ivanti Enterprise Reporting Client
ERS	Ivanti Enterprise Reporting
ERS_Staging	Ivanti Enterprise Reporting
ReportServer [(1)]	Microsoft SQL Server Reporting Services
ReportServerTempDB [(1)]	Microsoft SQL Server Reporting Services
SafeGuard [(2)]	powered by Sophos®
(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in Ivanti Enterprise Reporting. By default, the database names are ReportServer and ReportServerTempDB. (2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a Safeguard database.	

After Completing This Task:

You must create a backup of each database before any Transaction logs will be created. Refer to Creating a Database Backup on page 393 to create a one-time backup of your database.

Creating a Manual Solution

To prevent data loss, create a database solution, and implement it in the event of a disaster.

While a Maintenance Plan will allow you to automate the backup of your databases and transaction logs, you can also create and restore individual backups using the SQL Server Management Studio.

Creating a Database Backup

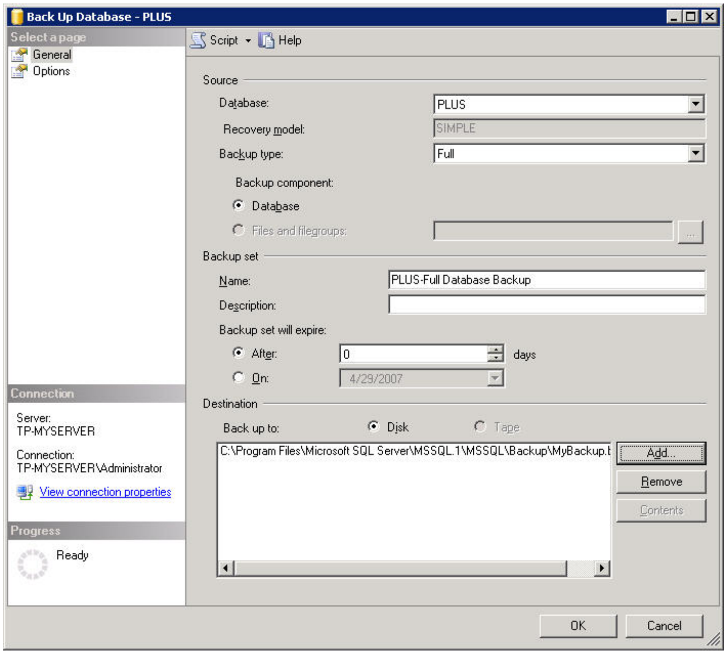
The most important part of an effective disaster recovery technique is having a current and valid backup. Create a backup for the SQL Server instance associated with Ivanti Endpoint Security to assure minimal system data is lost if a disaster occurs.

Backups are created within SQL Server Management Studio.

1. Open the ***Microsoft SQL Server Management Studio***.
2. Log into your database server.
3. In the directory tree, expand to **Databases** (***Server Name*** > ***SQL Instance*** > **Databases**).
4. Right-click the PLUS database.

5. Select **Tasks** > **Backup**.

   Step Result: The ***Back Up Database*** window opens.



Back Up Database - PLUS

Source

Database: PLUS

Recovery model: SIMPLE

Backup type: Full

Backup component:

● Database

○ Files and filegroups:

Backup set

Name: PLUS-Full Database Backup

Description:

Backup set will expire:

● After: 0 days

○ On: 4/29/2007

Destination

Back up to: ● Disk ○ Tape

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\MyBackup.b

Connection

Server:
TP-MYSERVER

Connection:
TP-MYSERVER\Administrator

Progress

Ready

Figure 92: Back Up Database

6. Ensure that the Source values are set as follows:

   - **Database**: `PLUS`
   - **Recovery model**: `Full`

   Note: If the **Recovery model** is not set to Full, refer to Changing the Database Recovery Model on page 391.

   - **Backup Type**: `Full`
   - **Backup Component**: `Database`

7. Define the **Backup set** identification fields.

   The following table describes each field.

Field	Description
Name	The name of the backup set.
Description	The description of the backup set.

8. Define the backup set expiration date.

Use one of the following methods.

Method	Steps
To define an expiration date based on a set number of days:	**1.** Select the **After** option. **2.** Type the desired number in the **After** field.
To define an expiration date based on a set date:	**1.** Select the **On** option. **2.** Select the desired date frm the **On** list.

9. Define your backup **Destination** settings.

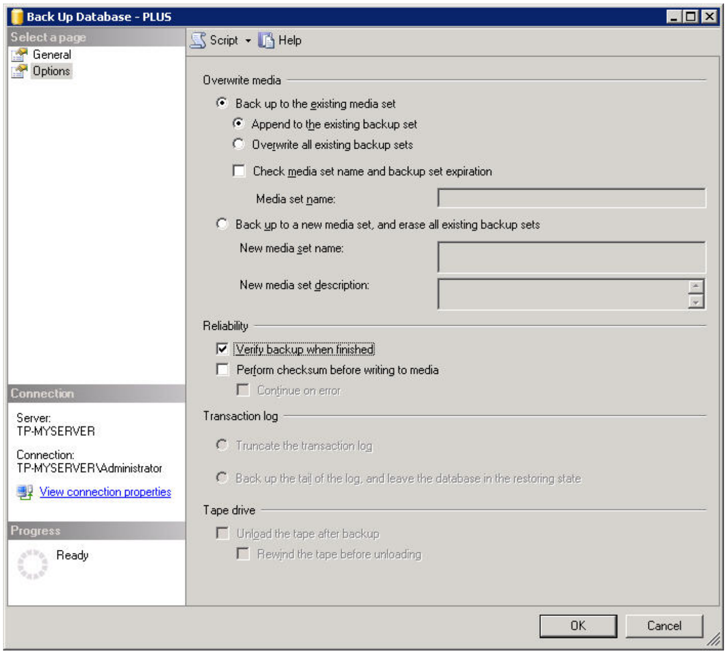
a) Select either the **Disk** or **Tape** option.

b) Define the destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

10. Select `Options` within the **Select a page** pane.

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



Back Up Database - PLUS

Select a page

General

Options

Script ▾ Help

Overwrite media

● Back up to the existing media set

● Append to the existing backup set

○ Overwrite all existing backup sets

□ Check media set name and backup set expiration

Media set name:

○ Back up to a new media set, and erase all existing backup sets

New media set name:

New media set description:

Reliability

☑ Verify backup when finished

□ Perform checksum before writing to media

□ Continue on error

Transaction log

○ Truncate the transaction log

○ Back up the tail of the log, and leave the database in the restoring state

Tape drive

□ Unload the tape after backup

□ Rewind the tape before unloading

Connection

Server:
TP-MYSERVER

Connection:
TP-MYSERVER\Administrator

View connection properties

Progress

Ready

OK Cancel

Figure 93: Back Up Database - Options

11. Select whether to **Backup up to the existing media set** or **Back up to a new media set, and erase all existing backup sets** as is appropriate for your organization.
12. Select the **Verify backup when finished** option to ensure a valid backup.
13. Click **OK**.
14. Repeat steps 5 through 13 for the following databases:

Table 158: Database Names

Database Name	Product
`STAT_Guardian`	Ivanti Endpoint Security
`UPCCommon`	Ivanti Endpoint Security
`UPCExtended`	Ivanti Endpoint Security
`PLUS_Reports`	Ivanti Enterprise Reporting Client
`ERS`	Ivanti Enterprise Reporting
`ERS_Staging`	Ivanti Enterprise Reporting
`ReportServer` (1)	Microsoft SQL Server Reporting Services
`ReportServerTempDB` (1)	Microsoft SQL Server Reporting Services
`SafeGuard` (2)	powered by Sophos®
(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in Ivanti Enterprise Reporting. By default, the database names are `ReportServer` and `ReportServerTempDB`. (2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a `Safeguard` database.	

After Completing This Task:
You must also backup the Ivanti Endpoint Security content directory.

Tip: The default location of the content directory is `<Installation Directory>\HEAT\EMSS\Content`. However, if this directory was modified during installation, you can verify its location by viewing the `\HKEY_LOCAL_MACHINE\SOFTWARE\Patchlink.com\Update\ISAPI\Storage` registry key.

Restoring a Database Backup

Another important part of an effective Disaster Recovery Solution is having a process defined in which to restore your database backup.

Prerequisites:

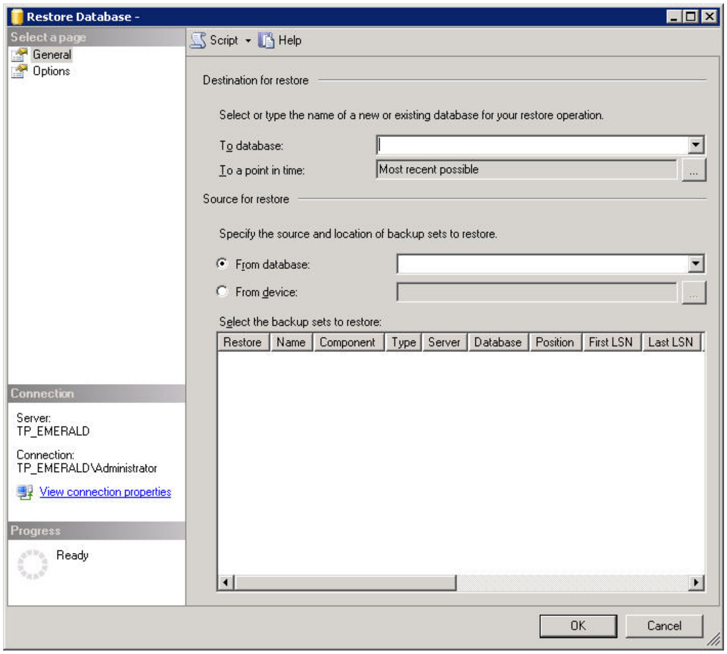
Prior to restoring the database backup you must install the Ivanti Endpoint Security server using the same serial number that was used previously.

Important: After installing the Ivanti Endpoint Security server do not open the user interface until after you have restored the databases.

1. Open the ***Services Management Console***.
2. Right-click the `World Wide Web Publishing` service.
3. Select **Stop** to stop the `World Wide Web Publishing` (IIS) service.
4. Repeat steps 2 and 3 for the following services:
   - `EDS Server`
   - `EDS InstallerService`
   - `Replication Service`
   - `STATEngine`
5. Restore the backup you made of the content directory, over the new content directory (`<Installation Directory>\HEAT\EMSS\Content` by default). However, if this directory was modified during installation, you can verify its location by viewing the `\HKEY_LOCAL_MACHINE\SOFTWARE\Patchlink.com\Update\ISAPI\Storage` registry key.
6. Open the ***Microsoft SQL Server Management Studio*** (**Start** > **Programs** > **Microsoft SQL Server 2008** > **SQL Server Management Studio**).
7. Using an user account that has *sysadmin* rights, log into your database server.
8. In the directory tree, expand ***Server Name\SQL Instance* > Databases**.
9. Right-click on the **Databases** folder.

10. Select **Restore Database**

Step Result: The ***Restore Database*** window opens.



Restore Database -

Select a page

General

Options

Script ▾ Help

Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database:

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

● From database:

○ From device:

Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position	First LSN	Last LSN

Connection

Server:
TP_EMERALD

Connection:
TP_EMERALD\Administrator

View connection properties

Progress

Ready

OK Cancel

Figure 94: Restore Database

11. In the **To database** field, type or select the `PLUS` database.

12. Select **From device** and click the **Ellipses** button (...).

Step Result: The ***Specify Backup*** dialog opens.

13. Click **Add**.

Step Result: The ***Locate Backup File*** dialog opens.

14. Locate and select your backup (`.bak`) file.

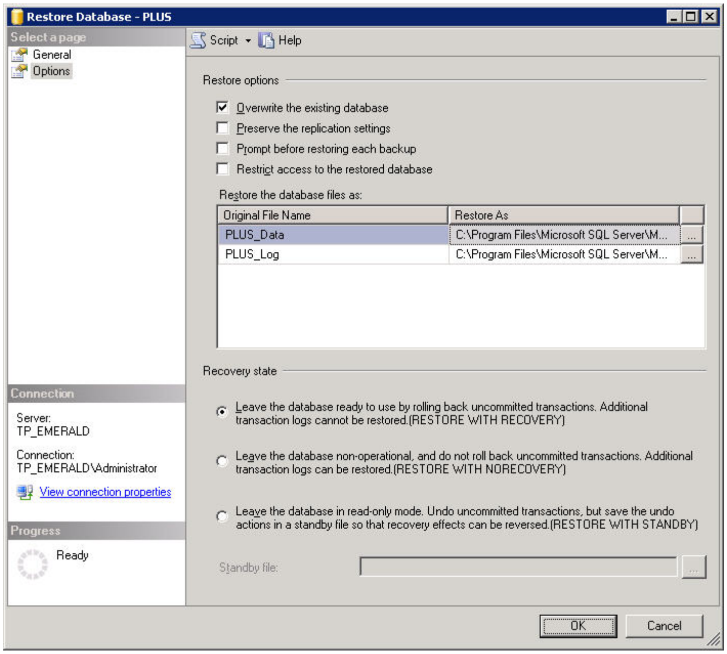
15. Click **OK**.

16. Click **OK** to return to the ***Restore Database*** window.

17. Select the check-box associated with your backup within the **Select the backup sets to restore** table.

18. Click `Options` within the **Select a page** pane.

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



Restore options

☑ Overwrite the existing database

□ Preserve the replication settings

□ Prompt before restoring each backup

□ Restrict access to the restored database

Restore the database files as:

Original File Name	Restore As
PLUS_Data	C:\Program Files\Microsoft SQL Server\M...
PLUS_Log	C:\Program Files\Microsoft SQL Server\M...

Recovery state

● Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs cannot be restored.(RESTORE WITH RECOVERY)

○ Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored.(RESTORE WITH NORECOVERY)

○ Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reversed.(RESTORE WITH STANDBY)

Standby file:

Connection

Server:
TP_EMERALD

Connection:
TP_EMERALD\Administrator

View connection properties

Progress

Ready

Figure 95: Restore Database - Options

19. Ensure the **Overwrite the existing database** option is selected.

20. Verify, and correct if necessary, the directory path within the **Restore the database files as** table.

21. Ensure the **Leave the database ready to use** option is selected.

22. Click **OK** to begin the database restoration.

23. After the restore is complete run the following SQL command against the database.

```
exec sp_changedbowner 'sa'
```

24. Repeat steps 9 through 23, restoring each of the following databases:

Table 159: Database Names

Database Name	Product
`STAT_Guardian`	Ivanti Endpoint Security
`UPCCommon`	Ivanti Endpoint Security
`UPCExtended`	Ivanti Endpoint Security
`PLUS_Reports`	Ivanti Enterprise Reporting Client

Database Name	Product
ERS	Ivanti Enterprise Reporting
ERS_Staging	Ivanti Enterprise Reporting
ReportServer [1]	Microsoft SQL Server Reporting Services
ReportServerTempDB [1]	Microsoft SQL Server Reporting Services
SafeGuard [2]	powered by Sophos®
(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in Ivanti Enterprise Reporting. By default, the database names are ReportServer and ReportServerTempDB. (2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a Safeguard database.	

25. Against the master database run the following SQL command.

```
exec sp_dboption N'STAT_Guardian', N'DB CHAINING', N'true'
exec sp_dboption N'UPCCommon', N'DB CHAINING', N'true'
exec sp_dboption N'UPCExtended', N'DB CHAINING', N'true'
exec sp_dboption N'PLUS', N'DB CHAINING', N'true'
exec sp_dboption N'PLUS_Reports', N'DB CHAINING', N'true'

exec sp_dboption N'ERS', N'DB CHAINING', N'true'
exec sp_dboption N'ERS_Staging', N'DB CHAINING', N'true'
exec sp_dboption N'ReportServer', N'DB CHAINING', N'true'
exec sp_dboption N'ReportServerTempDB', N'DB CHAINING', N'true'
exec sp_dboption N'SafeGuard', N'DB CHAINING', N'true'
```

26. If you changed the computer name, Service account name, or Client account name, then you must perform the following steps.

a) Delete the previous Service account and Client account users from **each** database.

b) Add the new Service and Client account users to the following roles for each database.

- PLUS - EMSS Server and aspnet_ChangeNotification_ReceiveNotificationsOnlyAcccess
- PLUS_Reports - EMSS Server
- STAT_Guardian - Guardian_Admin
- UPCCommon - EMSS Server and aspnet_ChangeNotification_ReceiveNotificationsOnlyAcccess
- UPCExtended - EMSS Server and aspnet_ChangeNotification_ReceiveNotificationsOnlyAcccess
- ERS - EMSS Server
- ERS_Staging - EMSS Server

27. If you re-installed the Ivanti Endpoint Security server with a different user name than was used when originally installed, run the following SQL command.

```
UPDATE AccountContacts SET UserName = 'NewUserName' WHERE UserName = 'OldUserName'
```

28. If you re-installed the Ivanti Endpoint Security server with the content directory in a different location than the original installation, run the following SQL command.

    ```
     UPDATE SystemConfig SET SystemConfig_Value = 'NewStorageSystemPath' WHERE SystemConfig_Name =
    'Storage'
    ```

29. If you re-installed the Ivanti Endpoint Security server with a different installation directory than the original installation, run the following SQL command.

    ```
     UPDATE SystemConfig SET SystemConfig_Value = 'NewWebInstallPath' WHERE SystemConfig_Name =
    'InstallPath'
    ```

30. Restart the `World Wide Web Publishing Service`, `EDS LanPortal`, `EDS MessageBroker`, `EDS Server`, `Replication Service`, and `STATEngine` services.
31. Install the Ivanti Endpoint Security Agent from the ***Download Agent Installers*** page.

Creating an Automated Solution

A Maintenance Plan allows you to create an automated backup and schedule the backup to occur as frequently as your organizational needs dictate. Maintenance Plans allow you to define your back up options as well as which databases and transaction logs to include.

Note: If you have not already done so, you should change your Database Recovery Model to `FULL` before continuing. For additional information, refer to Changing the Database Recovery Model on page 391.

Creating a Maintenance Plan

You can automate a database maintenance plan for the SQL Server instances associated with Ivanti Endpoint Security.

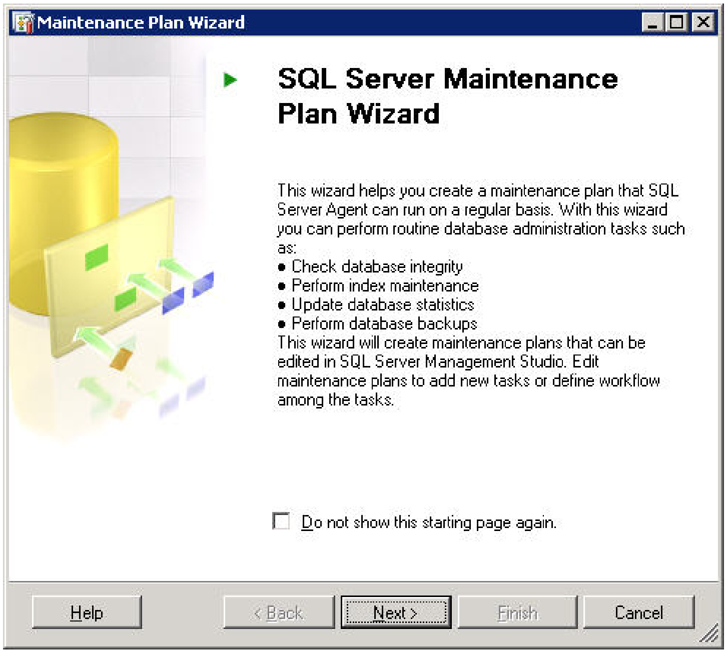
Prerequisites:

Prior to creating a Maintenance Plan you must upgrade your database server to ***Microsoft SQL Server 2008 Standard*** or ***Microsoft SQL Server 2008 Enterprise***, install SSIS (***SQL Server Integration Services***), and set the ***SQL Server Agent*** startup type to `Automatic`.

1. Open the ***Microsoft SQL Server Management Studio***.
2. Log into your database server.
3. In the directory tree, expand ***Server Name\SQL Instance*** **> Databases**.
4. Right-click on the **Maintenance Plans** folder.

5. Select **Maintenance Plan Wizard**.

   Step Result: The ***SQL Server Maintenance Plan Wizard*** opens.



SQL Server Maintenance Plan Wizard

This wizard helps you create a maintenance plan that SQL Server Agent can run on a regular basis. With this wizard you can perform routine database administration tasks such as:

- Check database integrity
- Perform index maintenance
- Update database statistics
- Perform database backups

This wizard will create maintenance plans that can be edited in SQL Server Management Studio. Edit maintenance plans to add new tasks or define workflow among the tasks.

□ Do not show this starting page again.

Figure 96: SQL Server Maintenance Plan Wizard

6. Click **Next**.

   Step Result: The ***Select a Target Server*** page opens.

7. Define the maintenance plan **Name**, **Description** [optional], target **Server**, and **Authentication** method.

8. Click **Next**.

   Step Result: The ***Select Maintenance Tasks*** page opens.

9. Select the following maintenance tasks:

   - **Check Database Integrity**
   - **Clean Up History** [optional]
   - **Back Up Database (Full)**
   - **Back Up Database (Transaction Log)**

10. Click **Next**.

    Step Result: The ***Select Maintenance Task Order*** page opens.

11. Set the tasks to execute in the following order:

- **Check Database Integrity**
- **Back Up Database (Full)**
- **Back Up Database (Transaction Log)**
- **Clean Up History** [optional]

12. Click **Next**.

Step Result: The ***Define Database Check Integrity Task*** page opens.

13. Click the **Database** drop-down.

a) Select the **These databases** option.

b) Select the `PLUS` database.

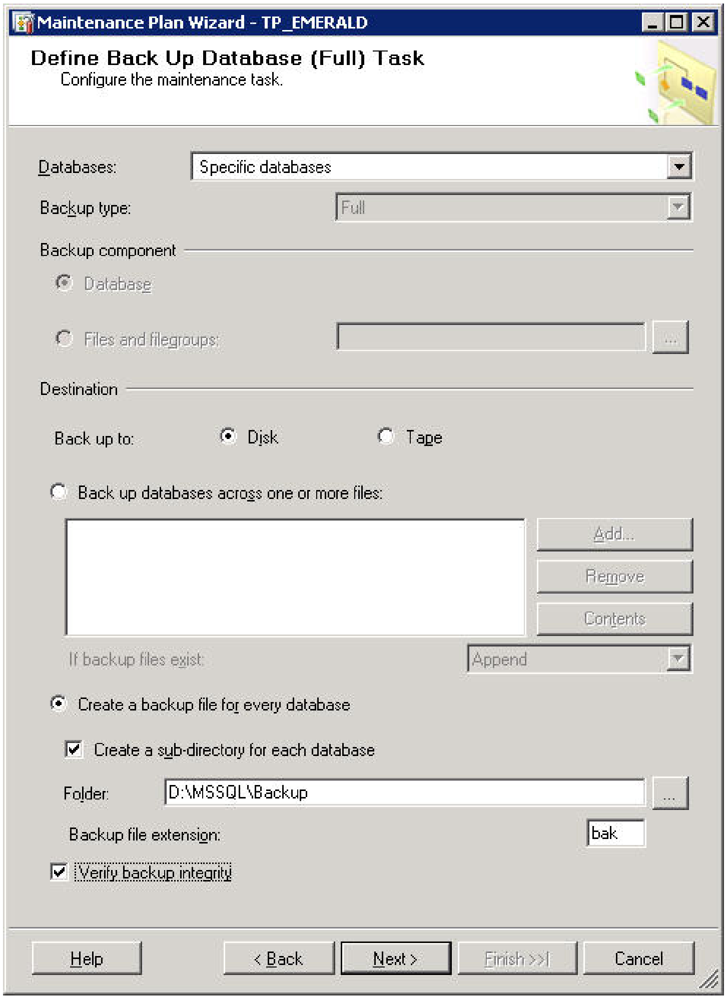
> **Tip:** You may choose all databases that require a database maintenance plan from the drop-down list.

c) Click **OK**.

14. Ensure that the **Include indexes** option is selected.

15. Click **Next**.

Step Result: The ***Define Back Up Database (Full) Task*** page opens.



Maintenance Plan Wizard - TP_EMERALD

Define Back Up Database (Full) Task
Configure the maintenance task.

Databases: Specific databases

Backup type: Full

Backup component

○ Database

○ Files and filegroups:

Destination

Back up to: ● Disk ○ Tape

○ Back up databases across one or more files:

If backup files exist: Append

● Create a backup file for every database

☑ Create a sub-directory for each database

Folder: D:\MSSQL\Backup

Backup file extension: bak

☑ Verify backup integrity

Figure 97: Define Back Up Database (Full) Task

16. Click the **Database** drop-down.

a) Select the **These databases** option.

b) Select the `PLUS` database.

> **Tip:** You may choose all databases that require a database maintenance plan from the drop-down list.

c) Click **OK**.

17. Define your Back up **Destination** settings.

a) Select either the **Disk** or **Tape** option.
b) Select to **Create a backup file** for every database.
c) Select to **Create a sub-directory** for each database.
d) Define your destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

e) Ensure the **Backup file extension** is set as `.bak` for the database backup.
f) Select **Verify backup integrity**.

18. Click **Next**.

Step Result: The ***Define Back Up Database (Transaction Log) Task*** page opens.

19. Click the **Database** drop-down.

a) Select the **These databases** option.
b) Select the `PLUS` database.

> **Tip:** You may choose all databases that require a database maintenance plan from the drop-down list.

c) Click **OK**.

20. Define your Back up **Destination** settings.

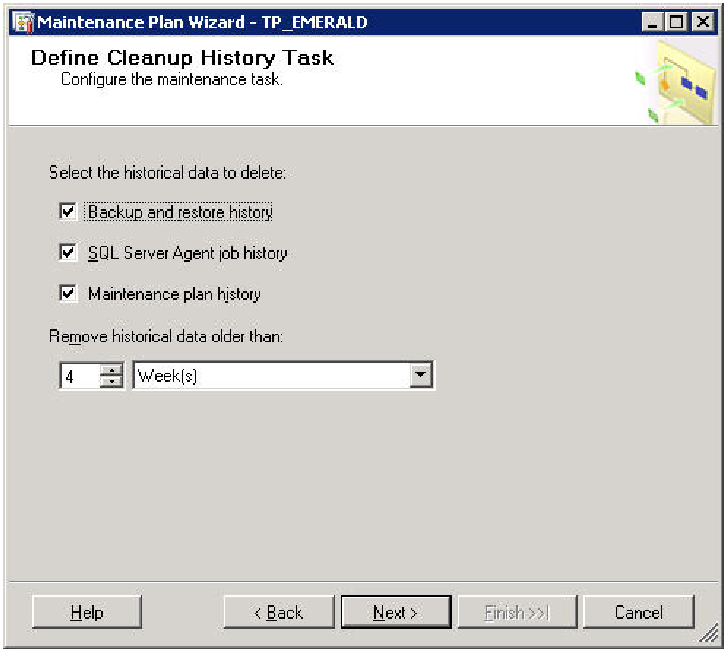
a) Select either the **Disk** or **Tape** option.
b) Select to **Create a backup file** for every database.
c) Select to **Create a sub-directory** for each database.
d) Define your destination **Folder**.

> **Note:** For performance reasons, it is recommended that you create your database backup in a directory that is not on the same physical drive as your database.

e) Ensure the **Backup file extension** is set as `.trn` for the transaction backup file.
f) Select **Verify backup integrity**.

21. Click **Next**.

Step Result: If the **Clean Up History** option was selected, the ***Define Cleanup History Task*** page opens. Otherwise the ***Select Plan Properties*** page will open.



Maintenance Plan Wizard - TP_EMERALD

Define Cleanup History Task

Configure the maintenance task.

Select the historical data to delete:

☑ Backup and restore history

☑ SQL Server Agent job history

☑ Maintenance plan history

Remove historical data older than:

4 Week(s)

Figure 98: Define Cleanup History Task

22. If the **Clean Up History** option was selected, define the ***Cleanup History Task*** options.

a) Ensure that **Backup and restore history** is selected.

b) Ensure that **SQL Server Agent job history** is selected.

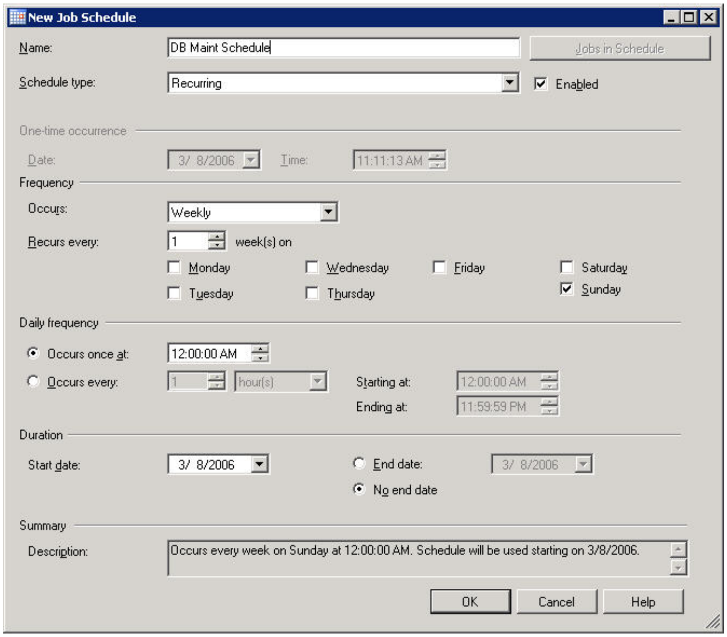
c) Ensure that **Maintenance plan history** is selected.

d) Define the **Remove historical data older than** setting as appropriate for your organization.

e) Click **Next**.

Step Result: The ***Select Plan Properties*** page will open.

23.[Optional] Click **Change** to open the ***New Job Schedule*** page and define the maintenance plan schedule.



New Job Schedule

Name: DB Maint Schedule

Schedule type: Recurring ☑ Enabled

One-time occurrence

Date: 3/ 8/2006 Time: 11:11:13 AM

Frequency

Occurs: Weekly

Recurs every: 1 week(s) on

□ Monday □ Wednesday □ Friday □ Saturday

□ Tuesday □ Thursday ☑ Sunday

Daily frequency

● Occurs once at: 12:00:00 AM

○ Occurs every: 1 hour(s) Starting at: 12:00:00 AM

Ending at: 11:59:59 PM

Duration

Start date: 3/ 8/2006 ○ End date: 3/ 8/2006

● No end date

Summary

Description: Occurs every week on Sunday at 12:00:00 AM. Schedule will be used starting on 3/8/2006.

Figure 99: New Job Schedule

a) Enter a **Name** for the schedule.
b) Select a **Schedule** type.
c) Ensure that **Enabled** is selected.
d) Define the **Occurrence** frequency (**Daily**, **Weekly**, or **Monthly**) and options.
e) Define the **Daily frequency**.
f) Define the **Duration**.
g) Click **OK**.

Step Result: The changes are saved and the ***New Job Schedule*** page closes.

24. Click **Next**.

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

25. Set your desired reporting options.

26. Click **Next**.

Step Result: The ***Complete the Wizard*** page opens.

27. Click **Finish** to complete the wizard.

28. Repeat steps 13 through 27 for the following databases:

Table 160: Database Names

Database Name	Product
`STAT_Guardian`	Ivanti Endpoint Security
`UPCCommon`	Ivanti Endpoint Security
`UPCExtended`	Ivanti Endpoint Security
`PLUS_Reports`	Ivanti Enterprise Reporting Client
`ERS`	Ivanti Enterprise Reporting
`ERS_Staging`	Ivanti Enterprise Reporting
`ReportServer` (1)	Microsoft SQL Server Reporting Services
`ReportServerTempDB` (1)	Microsoft SQL Server Reporting Services
`SafeGuard` (2)	powered by Sophos®

(1) Subscription features available in Microsoft SQL Server Reporting Services can be implemented in Ivanti Enterprise Reporting. By default, the database names are `ReportServer` and `ReportServerTempDB`.

(2) Data protection capabilities in is enhanced with a full disk encryption add-on from Sophos. The installation of results in a `Safeguard` database.

After Completing This Task:
You must now establish a backup procedure which will archive all of your backup files and the contents of the `UpdateStorage` directory on a regular basis. This can be done through the use of any file backup utility.

Appendix E

Installation Manager Reference

In this appendix:

- Configuring Windows Firewall for Installation Manager
- Updating Ivanti Installation Manager

Within Ivanti Endpoint Security, you can use Installation Manager to install Ivanti Endpoint Security components.

Occasionally, after upgrading Ivanti Endpoint Security, you may be asked to update Installation Manager after opening it.

Configuring Windows Firewall for Installation Manager

Allow Installation Manager to communicate through a Windows Firewall on the Ivanti Endpoint Security (Ivanti Endpoint Security) server.

Prerequisites:

- Install Ivanti Endpoint Security.
- An active Firewall is present on the Ivanti Endpoint Security server.

Create a port exception through the Firewall for Ivanti Installation Manager and Ivanti Installation Manager Update.

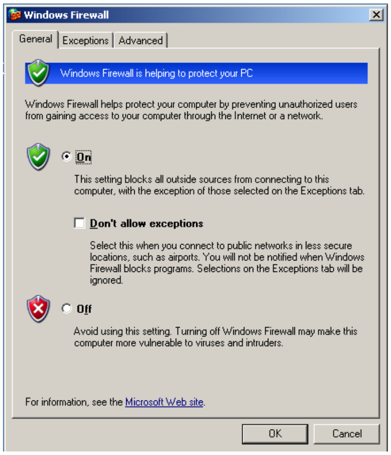
Note: The following steps were created for Windows 2003. When creating a port exception for Windows 2008, steps may differ slightly.

1. Create a port exception through the Firewall.

   a) Click **Start** > **Run**.

b) In the **Open** field, type `firewall.cpl`.

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



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

For information, see the Microsoft Web site.

Figure 100: Windows Firewall Dialog

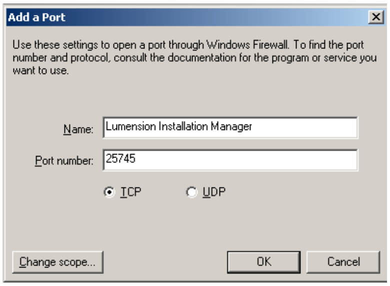
c) Click the ***Exceptions*** tab.

d) Click **Add Port**.

Step Result: The ***Add a Port*** dialog opens.

e) In the **Name** field, type `HEAT Installation Manager`.

f) In the **Port number** field, type `25745`.



Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: Lumension Installation Manager

Port number: 25745

● TCP ○ UDP

Figure 101: Add a Port

g) Ensure **TCP** option is selected.

h) Click **OK**.

Step Result: The ***Add a Port*** dialog closes.

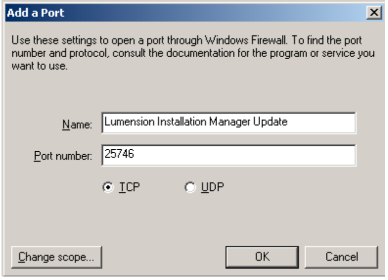
2. Create a port exception through the Firewall for Ivanti Installation Manager Update.

a) Click **Add Port**.

Step Result: The ***Add a Port*** dialog opens.

b) In the **Name** field, type `HEAT Installation Manager Update`.

c) In the port field, type `25746`.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: Lumension Installation Manager Update

Port number: 25746

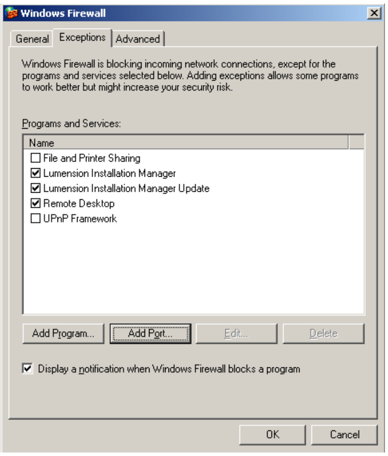
● TCP ○ UDP

Figure 102: Add a Port

d) Ensure **TCP** option is selected.

e) Click **OK**.

Step Result: The ***Add a Port*** dialog closes.



Windows Firewall

Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name

- □ File and Printer Sharing
- ☑ Lumension Installation Manager
- ☑ Lumension Installation Manager Update
- ☑ Remote Desktop
- □ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

Figure 103: Windows Firewall Dialog

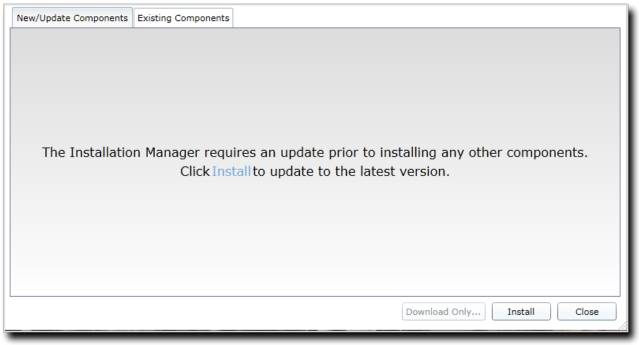
3. Click **OK**.

Step Result: Closes the ***Windows Firewall*** dialog.

Result: The Ivanti Installation Manager can communicate through a Windows Firewall on the Ivanti Endpoint Security server.

Updating Ivanti Installation Manager

Ivanti Installation Manager is updated periodically. Install the new version to take advantage of higher performance or added features.



The Installation Manager requires an update prior to installing any other components. Click Install to update to the latest version.

Figure 104: New/Update Components Tab

Ivanti Installation Manager updates are downloaded and applied by Ivanti Endpoint Security, or you can install them manually as any other component. For additional information, refer to Installing or Updating Components on page 299. Ivanti recommends installing updates immediately.

Note: If you are upgrading to Ivanti Endpoint Security 8.6 using the Ivanti Installation Manager, you may be asked to reboot the server to continue the update process.

Appendix F

Upgrading Agents on Endpoints

Upgrading an agent on an endpoint installs an updated version of the agent on the endpoint.

Versions of the Ivanti Endpoint Security Agent 7.3 and later can be upgraded using the Ivanti Endpoint Security Web console. During upgrades, the agent data and configuration are maintained. For additional information, refer to one of the following topics:

- To upgrade agents based on a complete list of endpoints in the system, refer to Upgrading Endpoints on page 173.
- To upgrade agents based on individual endpoints Upgrading the Agent on a Single Endpoint on page 187.
- To upgrade agents based on groups, refer to Defining the Endpoint Agent Version (Groups Page) on page 215.

Appendix G

Glossary

In this appendix:

- Glossary

This glossary defines terms related to Ivanti Endpoint Security. Some terms apply to information technology in general, while others are specific to Ivanti Endpoint Security.

Glossary

This glossary contains list of terms related to Ivanti Endpoint Security, as well as their definitions.

A

AAA Architecture	In client/server networking, an architecture that combines three necessary elements of security, to make them available on one server and able to work with each other in a coordinated manner.
access control list (ACL)	A database file that stores information regarding entities that may request access to a network, as well as the rights and privileges to be granted upon request.
accessible endpoints	A feature that associates an individual endpoint with a particular role. This feature allows you to limit a user’s permissions to specific endpoints. For example, you can limit a user with administrative rights to administration of a single endpoint.
accessible endpoint groups	A feature that associates an individual group with a particular role. This feature allows you to limit a user's permissions to specific groups. For example, you can limit a user with administrative rights to administration of a single group.
access rights	System privileges that determine whether or not a user can access an individual feature or page. There is an access right for each system page and function. Access rights for a user are determined by selecting rights for a user role, and then assigning that user role to the applicable user.

accounting

In network security architectures, records what users do once they are granted access to a network, or in the case of denied access, it can report how many failed attempts, and even details of the attempts.

Active Directory

Microsoft's trademarked system that centralizes the management of networked resources by making each item on a network, including most applications, objects in a relational database and then enabling the administrator to manage those objects through one management center.

active directory synchronization

The process by which the Application Control module synchronizes with a network active directory. This process crawls targeted active directories for users, user groups, endpoints, endpoint containers, and other data stored in the active directory.

Active Server Page

An HTML page that contains embedded server side scripting that is processed on a Microsoft Web Server before the page is sent to the user.

ActiveX

A technology, built on Microsoft's Component Object Model (COM), that enables software components, regardless of the language used to create them, to interact with one another in a networked environment.

Active Template Library

A Microsoft program library for use when creating ASP code and other ActiveX program components to run in a browser window.

Address Resolution Protocol

An OSI layer-3 protocol used to find an endpoint's MAC address using its IP address.

agent

A software routine that resides in background memory on a computer or other device and waits to perform an action when a specified event occurs.

Agent Management Job

Jobs that let you install agents upon endpoints within your network remotely. The first function of this job is to discover the targeted endpoints as in a *Discovery Scan Job*. The second function of this job is to install agents upon endpoints discovered during the first function. These jobs access the targeted endpoints by providing credentials specified during job configuration.

Agent Policies

The agent rules for communicating with the server. These rules include: communication interval, deployment notification options, discovery agent mode, hours of operation, logging level, and reboot notification options. Agent policies are assigned to groups, but any group that has not been explicitly assigned an agent policy will use the default system policy, as defined within the Ivanti Endpoint Security server.

agent policy conflict resolution

A series of protocols that determine which setting takes priority when a group or endpoint is assigned two or more agent policy sets with policies that conflict.

Agent Policy Sets

The combined selected agent policies as defined by the user. After their definition, these sets are then assigned to groups.

asset

An endpoint, along with all the hardware and software that is installed on that endpoint. Each endpoint, individual hardware device, and individual software application is considered an asset.

authentication

The process of identifying a user, typically through the use of credentials such as a user name and password, as the originator of a message or as the end point of a channel. High level authentication can use such other tokens as the originating IP address, or an encryption key, providing evidence of the authenticity of the request.

Authenticode

A technology based on information technology security industry standards that provides a method for developers to digitally sign their code. When code is signed, the company signing the code takes responsibility for the code and guarantees that the code is safe and free from viruses.

authorization vs. authentication

Whereas authentication is the process of verifying that a user is who they say they are, like having two forms of ID from different places, or dating paint and frame wood to verify authenticity of a painting, authorization is verifying the level of access available to that user, such as aisle and row seating stamped on a concert ticket, or possessing a back-stage pass.

authorization

The process of determining what level of access to grant a user to a system or software application function based upon their log in credentials.

B

browser

Software that allows the user to find, view, hear, and interact with material on a corporate Intranet or the World Wide Web.

C

child hierarchy

The entire group hierarchy belows a specific group within the group hierarchy. Child groups have only one parent. Nesting child groups within parent groups creates an inheritance, which lets you apply one agent policy set to a parent and its children.

client	In computer networks, a client is any user, computer, node, server, or system that is requesting files from or access to some other system, regardless of whether it also acts as a server.
code signing	The process of digitally signing programs for verification purposes.
components	The components that form Ivanti Endpoint Security. components come in two types: platform components and module components. Platform components form a basis for module components to operate. Module components are the individual security solutions used to prevent network security breaches.
Component Object Model (COM)	Microsoft's programming architecture in the Windows family of operating systems that enables software components to communicate between processes and fit easily into object-oriented program design. The family of COM technology includes COM+, Distributed COM (DCOM) and ActiveX.
context	Pertaining to Microsoft Active Directory, context refers to the exact container position in the directory tree, thus allowing for the location of resources in a tree, by use of relative rather than fully qualified identifiers.
Control Panel applet	An application designed to be run within Microsoft Windows Control Panel. Ivanti's Control Panel applet allows easy interaction with the Ivanti Endpoint Security agent.
Coordinated Universal Time (UTC)	An international standard that allows for synchronization of events across many geographic zones. On a Ivanti Endpoint Security server, UTC might be chosen instead of local time if a scheduled event is desired to run at the same time at all sites, dependent also upon deployment constraints.
credentials	An object or objects presented along with a request for admission to a network or server that is used to validate the authorization of the presenter. Usually a credential is a combined user name and password, but can also consist of IP address, MAC address or an encryption key to verify that the request comes form an authorization location.
cross-platform	Portable or applicable to more than one operating system.

D

decryption	The process of converting ciphered text back to plain text after it travels across a public access medium. A previously determined key is used once the text arrives at its destination to convert the ciphered message back to clear text.

decryption key

A string of seemingly random bits of data used with cryptographic algorithms to create or verify digital signatures and unscramble cipher text back to its original clear text. Keys can be public or private and keeping at least one key private provides high security. Keys at least 128 bits long are considered more secure by modern standards, as many shorter ones have been cracked by modern computing technology.

discovery methods

The methods used to designate targets (endpoints and devices) during discovery scan jobs. Endpoints and devices can be discovered using a single IP address, an IP address range, a single computer name, network neighborhood, or active directory.

discovery options

A series of queries and scans that collect information about targets defined for detection during discovery scan jobs. These options (which include Verify with PING, ICMP Discovery, Port Scan Discovery, SNMP Discovery, Windows Version Discovery, Resolve DNS Names, Resolve MAC Addresses, and Resolve NetBIOS Names) identify whether an endpoint is present, and, if one is, what its address and operating system information are.

Discovery Scan Job

A network-based scan run from the Ivanti Endpoint Security server that discovers assets in your network (endpoints, routers, switches, printers, and so on) by using user-specified IP addresses or asset names and/or domains. These jobs also discover additional information about assets (operating system, address information, and so on) through port scans, information queries, and address mask requests.

Distributed Component Object Model (DCOM)

An extension of the Component Object Model (COM) that extends COM’s capabilities across network boundaries, allowing objects to communicate across a network. COM, unlike DCOM, is designed for interprocess communication on the same node or computer.

domain

On a local or wide area network, a domain is a set of network resources and services available to a group of users. Domains act as containers that can be identified by a name and address, which can then provide authorized users access to any elements they contain. Domains can also share resources with each other as trust is extended by administrators to those other domains.

Domain Name System (DNS)

The system used to name computers and especially servers for easier location. A domain name is a meaningful and human-readable name associated with an IP address. Domain names most often take on the format of domainname.com and the most common ones are associated with WWW locations.

Dynamic Host Configuration Protocol (DHCP)	A protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization’s network by establishing a range of IP addresses to be assigned automatically and indexed. Without DHCP, managers would have to manually assign and keep track of each host IP address on the network.
dynamic-link library file (DLL file)	A file that has linked and compiled one or more functions used by a separate process, which can be loaded into the memory space of that process when the program is started or running.

E

encryption	The process of converting clear, readable text to ciphered text before it travels on network media, so that it can only be read or understood by a recipient with the proper decryption key. Some of the most secure encryption methods include RSA, AES, IKE, MDS, SSL, and SHA-1.
encryption key	A string of ciphered bits used with cryptographic algorithms to create or verify digital signatures and scramble clear text to protect it from being intercepted and read while traveling across public networking media. Keys can be public or private, and keeping at least one key private provides high security. Keys at least 128-bits long are considered more secure by modern standards, as many shorter ones have been compromised by modern computing technology.
Endpoint	In a client/server network architecture, an endpoint is any node that is a destination of two-way communication, whether requesting or responding. Additionally, in regard to the Ivanti Endpoint Security, the term endpoint is synonymous with any computer in your network that can have an agent installed.

F

File Transfer Protocol (FTP)	A protocol that uses simple, clear text. Thus, it is a non-secure protocol used to exchange files between computers on a network or the internet.
firewall	A firewall is a set of related programs located at a network gateway server that protects the resources of a private network from unauthorized access.

fully qualified domain name (FQDN)	The domain name is a unique identifier for any resource located within a domain or network. A FQDN is the full name of any network entity starting with its hostname and ending with the exact domain name in which it resides. Example: johnq.accounting.acme.com

G

Global Subscription Service (GSS)	The central repository where security content is stored for retrieval by the Ivanti Endpoint Security server. The GSS also serves as the Ivanti Endpoint Security licensing server.
globally unique identifier (GUI)	A 128-bit number generated by Windows operating systems or one of its applications, which is assigned to any object in a two-way communication, be it user, application, or component. The algorithm used to generate GUIDs combines a few unique settings, such as IP Address, MAC Address, and clock date and time to create an even more unique identifier.
Group	A targeted collection of computers created and named for the purpose of deploying distribution packages, defining agent policies, setting Mandatory Baselines, or reporting. Groups provide a simple way to manage computers that have similar requirements rather than managing each computer separately.

H

hostname	The name given to identify each node of a network. The hostname usually describes either the user that operates the node, its position in a building, or its function. Hostname is intended to be more human friendly than numeric IP Addresses.
HTML	The accepted publishing language of the World Wide Web. It is a universally accepted standard for displaying links, images, and text in a format that computers around the world can read. There are currently many advantages in HTML that allow for an increasing number of different types of objects to be added to and displayed in a browser page.
HTTP	The set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
HTTPS	A Web protocol built into most browsers that encrypts and decrypts user page requests as well as the pages that are returned via HTTP over SSL by the Web server.

hyperlink

Generally a different color from the surrounding text, a hyperlink is a coded reference to another location in the document, or to a URL or network address, usually written in a form of HTML code or JAVA, and is most prevalent on Web pages.

I

Internet Assigned Numbers Authority (IANA)

An administrative organization that assigns internet host addresses and other numeric constants used in Internet protocols.

IP (Internet Protocol)

The best known and main protocol in a suite of protocols known as TCP/IP that carry all traffic on the internet currently. IP is a connectionless protocol, meaning it does not wait for confirmation that it was received before sending the next packet. It is designed for long distance carriage of packets of data, as was originally the plan with Arpanet, which later became the internet.

IP address

The 32-bit (4 dotted divisions of eight binary digits) numeric identifier for any device on a network that distinguishes it from other devices and allows for routers and switches to group devices and their communication packets. The 32-bit dotted format is soon to be replaced by IPv6, which will expand the number of available IP addresses to keep pace with the enormous growth of the internet in recent years. Example: IP address 192.168.0.1 would be read by a router as 11000000.10101000.00000000.00000001.

J

JAVA

A programming language invented by Sun Microsystems. It can be used as a general purpose application programming language with built-in networking libraries. It can also be used to write small applications called applets.

JAVA Runtime Environment (JRE)

Created by Sun Microsystems, it is the core set of files necessary to execute JAVA written programs in any OS environment. JAVA is used because it is cross-platform, which is increasingly necessary in the current Web-based world.

L

library

A collection of precompiled routines, sometimes called modules, that are stored in object format for reuse by a program.

Lightweight Directory Access Protocol (LDAP)	A software protocol that enables the use of Directory Services to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet.
localhost	The default name describing the computer address also known as the loopback address of the computer. On Web servers, this loopback can be used to test the default Web page. To access this page, type http://127.0.0.1 or http://localhost.
localprofile.txt	An XML file found in the `%Installation Directory%\HEAT Software\EMSSAgent\live\patch\`, this file is maintained by the Ivanti Endpoint Security agent and contains information on computer's name, services, software, hardware, operating system, and support pack level. The refresh inventory data system task uses the information in this file to populate computer inventory data on the Ivanti Endpoint Security server.
Ivanti Content Wizard	Ivanti Content Wizard (HCW). An addition to Ivanti Endpoint Security that provides the ability to define custom detection reports, deployment packages, signatures, and fingerprints. It has an easy-to-use graphical interface that illustrates all associated subcomponents of the patch in a single view.
Ivanti Endpoint Security	An application that serves as a platform for other applications that protect your network from security risks. These applications, called *modules*, use different approaches to protect your endpoint. Ivanti Endpoint Security is composed of a server component and an agent component. The server component is installed on a server within your network. The agent component is installed on network endpoints you want to protect from security risks. Ivanti Endpoint Security is accessed via a Web UI.
Ivanti Endpoint Security administrator	Any user who is assigned any of the access rights that control the functionality of the Ivanti Endpoint Security server or its deployments is considered a Ivanti Endpoint Security administrator.
Ivanti Endpoint Security Agent	The Ivanti Endpoint Security agent is a service that runs on each node and queries the Ivanti Endpoint Security server to receive any deployments that become ready. The behavior of the agent is defined by the agent's policies, whether it is using the default agent policies of the Ivanti Endpoint Security server or the group's agent policies.

Ivanti Endpoint Security Server

The central system in Ivanti Endpoint Security that manages content retrieval, vulnerability detection, and package deployment to all registered computers on the network. As a sophisticated, automated central repository of the most current security content available for a network, it maintains communication with the Ivanti Endpoint Security agent on nodes, across many key networking platforms, on the network, and detects any vulnerabilities with the help of the agent on each node.

Ivanti Endpoint Security user

Any user who has access to authenticate in to the Ivanti Endpoint Security server is considered a Ivanti Endpoint Security user.

M

MAC address

A 12-digit hexadecimal address that is burned into network cards and networking devices to allow for unique reference.

macro

Within Ivanti Endpoint Security, a macro is an environment variable that represents a filename, directory path, or a series of commands, actions, or keystrokes that can only be executed by the Ivanti Endpoint Security agent.

Microsoft SQL Desktop Edition (MSDE)

An enabling technology that provides local data storage and is completely compatible with the SQL Server version 7.0 code base. This technology transforms Microsoft Access from a simple file-server database application into an extremely powerful and highly scalable client-server solution for any size organization.

Module Components

Individual security solutions used to prevent various types of security breaches within your network. Each module plugs in to the Ivanti Endpoint Security platform and can be purchased individually. Some module components come installed with the Ivanti Endpoint Security platform and require no additional licensing.

Module Sub Components

The two parts that form a module component. Each module component consists of a server sub component and an endpoint subcomponent. These subcomponents work together to form a module's functionality.

MSI installer

Designed for Windows networks that use the Windows software installer mechanism. The MSI installer can be edited to include the Ivanti Endpoint Security server name and serial number. In this way, the agent can be deployed through the use of group policy agents.

N

NetWare	Networking OS that has played a major role in the development of Local Area Networking over the past few decades, being an early Network OS to use the Directory Services concept.
Novell Directory Services (NDS)	The relational database that contains all the resources on a Novell network, and provides security, and access for all resources.

O

Open Software Description (OSD)	Creates a standard way to describe software components, their versions, underlying structure and relationships to other components. OSD is the standard language used when performing automatic software distributions and updates over the Internet.
Operating System Pack (OSP)	Contains all vulnerability detection information needed by an agent for a given operating system. It is generated by the DS and is passed to the agent during the DAU task. When a vulnerability replication executes, it checks to see if any operating systems received new data and it will automatically schedule the DS to regenerate the OS Packs for those operating systems.

P

parent hierarchy	Refers to the entire group hierarchy above a specific group within the group hierarchy.
Platform components	The essential components needed for Ivanti Endpoint Security operation. These components include the Ivanti Endpoint Security Web console, the Ivanti Endpoint Security database, and the Ivanti Installation Manager.
policy server	In a network designed with protections against unauthorized admission, it is where the rules and policies are stored that are the standards by which admission decisions are made. Rules can then be enforced by routers or some other form of firewall protection.
port number	The port number is carried in internet transport protocols to identify which service or program is to receive an incoming packet. Certain port numbers are permanently assigned to particular protocols by the IANA. For example, e-mail uses port 25 and Web services use port 80.

proxy server	In an enterprise that uses one of the Internet protocols, a proxy server is a server that acts as an intermediary between a client and an Internet server. The proxy server allows an enterprise to ensure security and administrative control.

Q

Q-chain (QChain.exe)	The utility Microsoft provides to chain hotfixes on Microsoft Windows NT, 2000, 2003, 2008, XP, or Vista.

R

Reflective Memory Injection	A technique for excuting external code within an authorized process, bypassing an endpoint's whitelist enforcement mechanism. This is sometimes (though not always) the result of a malware attack.
Refresh Inventory Data (RID)	Prevents certain log files from getting too large. RID is handled differently on the various platforms; some delete the files when they reach a certain size, while others will trim the file, leaving the most recent data but shrinking the file size.
registry	The registry serves as a central data repository for system and application-specific configuration data on a Windows machine. A registry contains keys, which are like directories in a Windows file system. Each key can contain values (the registry equivalent of a data file) or nested subkeys (the registry equivalent of a nested folder). Just as with files or folders, you can identify a registry key by building a full path to it.
replication	The process whereby the Ivanti Endpoint Security server receives daily scheduled updates of patches from the GSS. The schedule replication time of day can be manually overridden daily by clicking **Update Now**.
report	Records that document activity and information pertaining to your network environment. Within the Ivanti Endpoint Security server, you can generate reports for virtually every function that the server and agent performs: endpoint inventory, the results of discovery scan jobs, the status of a deployment, and so on.
Reverse Address Resolution Protocol (RARP)	Literally, the reverse of Address Resolution Protocol, RARP resolves an IP address from a given hardware, or MAC address.
rules	Statements of conditions that must be met or parameters that will determine an action to be taken. Rules can be positive or negative, but usually are stated simply and clearly such as "if member of group ADMIN, run superuser.bat."

S

Secure File Transfer Protocol (SFTP)	A secure version of FTP, SFTP is designed to provide some encryption capabilities for file transfer over a network. Functionally similar to FTP, SFTP instead uses SSH to transfer files, so it cannot be used with a standard FTP client.
Secure Sockets Layer (SSL)	A security protocol that provides data encryption, message integrity, and client/server authentication for the transmission of private information and documents over the internet. SSL is available with either 40-bit or 128-bit encryption. However, 40-bit has been compromised in recent years, making 128-bit the lowest level anyone should go for secure encryption.
server	A server is a computer or software application that provides data to client computers or software applications. A single computer running multiple software applications can simultaneously perform the function of multiple servers, multiple clients, or any combination thereof.
source group	Groups that automatically assigned managed endpoints to associated custom groups.
SQL Server	A trademark for a Microsoft database server that uses SQL. SQL Server is a popular database management system for Windows NT environments.
structured query language (SQL)	A database language used by administrators of relational databases to query, update, and mange data. It enables the administrator to use clear syntax that is descriptive of whatever action is wanted.
SSL Certificate	An electronic certificate consisting of a set of keys, one public, one private, exchanged between a Web server and a requesting client. A session is created, and a unique session key ensures a high level of encryption of any sensitive data passed between the client and server, preventing interception or unauthorized use of that data by any other entity.

T

TCP/IP (Transmission Control Protocol/Internet Protocol)	The main suite of communications protocols used to connect hosts on the Internet, and now the prevalent LAN protocol even when other protocols are available.
transaction log	A Web server file that records a history of actions such as data changes. This log is used to roll the Web server back to a stable condition should the database be found in an inconsistent state.

trust	In domains, a trust relationship will allow members of one domain, when properly logged in and authenticated, to access services available on another domain.

U

URL (Universal Resource Locater)	The address that is the formal access name for a network or Internet resource. It usually begins with the protocol identifier, such as http or ftp. Thus, http://www.yahoo.com is a URL for the domain yahoo.com.
user	A profile used to access the Ivanti Endpoint Security server. These profiles include credentials (a user name and password) and an assigned role that determines the user's access rights within the system.
User Datagram Protocol (UDP)	A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses *Internet Protocol*. It is one of the most common connection based protocols in use on the internet, the other being TCP.
user name	The unique name used to gain access to a computer and/or network. User names and passwords are required in multi-user systems.

V

VeriSign certificate	A VeriSign certificate is issued by VeriSign, Inc. to verify a company’s identity and enables the company to digitally sign programs and prove the authenticity of a Web site address.

W - Z

Web server	A program that publishes content using the HTTP protocol so that it can be viewed using any type of compliant browser from any location on the connected Intranet or Internet.
widget	A graph or chart displayed on the Ivanti Endpoint Security ***Home*** page that depicts Ivanti Endpoint Security and Ivanti Endpoint Security module activities.
World Wide Web (WWW)	A commonly used name for the Internet, the WWW is a Web of connected Domains of local computers, which can share information with authorized users whom connect from anywhere else on the Web. Due to the exponential growth in recent years, a good way to check on current standards is to visit the World Wide Web Consortium (http://www.w3.org).

XML (extensible markup language)	A flexible way to create common information formats and share both the format and the data on the World Wide Web, Intranets, and elsewhere.