AntiVirus 8.6

User Guide

ivanti

Endpoint Security

powered by HEAT

Notices

Version Information

Ivanti Endpoint Security: AntiVirus User Guide - Ivanti Endpoint Security: AntiVirus Version 8.6 -Published: Dec 2020

Document Number: 02_206_8.6_171251637

Copyright Information

Table of Contents

Chapter 1: AntiVirus Overview....9
The Virus and Malware Threat....9
Malware Categories....10
The Role of Ivanti AntiVirus....12
Ivanti AntiVirus Technologies....12
Ivanti AntiVirus Scan Types....13
Policy-based Malware Scanning....13
Scan Now Virus and Malware Scan....14
Comparison of Ivanti AntiVirus Scan Types....14

Chapter 2: Getting Started with AntiVirus....17
AntiVirus at a Glance....17
The Ivanti AntiVirus Workflow....18
Step 1: Install the AntiVirus Module Server Component....19
Step 2: Add the AntiVirus Module to Endpoints....20
Step 3: Verify AntiVirus Endpoint Component Installation Status....20
Step 4: Create an AntiVirus Group....21
Step 5: Run an Initial Virus and Malware Scan....22
Step 6: Review and Remediate Initial Scan Event Alerts....25
Step 7: Create AntiVirus Policies to Monitor Your Environment....25

Chapter 3: Using the Ivanti Endpoint Security Console....43
Common Functions....43
Common Conventions....44
The Navigation Menu....45
The Page Banner....52
List Pages....52
Toolbars....53
The Options Menu....53
Filters....54
Group By....58
Expanding and Collapsing Structures....59
Advancing Through Pages....60
Help....60
Exporting Data....61
The Home Page....61
The Dashboard....62
Dashboard Setting and Behavior Icons....80
Previewing and Printing the Dashboard....81
Editing the Dashboard....81
The System Alert Pane....82
License Expiration....84

Chapter 4: Configuring Notifications....87
The Email Notifications Page....88
Email Notification Page Buttons....88

The Email Notifications Table....89
Alert Settings....91
Working with Email Notifications....94
Configuring Alert Settings....94
Creating Email Notifications....96
Editing Email Notification Addresses....96
Deleting Email Notification Addresses....97
Exporting Email Notification Data....97
Testing Email Notifications....97
APNS Renewal Alerts....98
GSS Notifications....99

Chapter 5: Updating the AntiVirus Module....101
AntiVirus Engine and Definitions....101
Updating the AntiVirus Engine and Definitions Manually....102
Setting the Polling Frequency for AntiVirus Engine and Definition Updates....103
Setting an AntiVirus Content Storage Location....104
Delaying the Distribution of AntiVirus Definition File Updates to Endpoints....105
Checking the version of the AntiVirus Engine and Definition....107
The AntiVirus Tab....108

Chapter 6: Working with Antivirus Policies....109
About Antivirus Policies....109
Antivirus Policy Types....109
Real-time Monitoring Resultant Policies....112
Assigned and Inherited Policies....113
Archive Types Supported for Scanning....114
Viewing Antivirus Policies....115
The Central Antivirus Policies View....115
Antivirus Policies on Endpoints....118
Antivirus Policies on Groups....119
Creating Antivirus Policies....120
Creating a Recurring Virus and Malware Scan Policy....120
Creating a Real-time Monitoring Policy....129
Importing File, Folder and Process Exclusions....136
Exclusion Rules....138
Managing Antivirus Policies....140
Managing Antivirus Policies Centrally....141
Managing Antivirus Policies on the Endpoint....146
Managing Antivirus Policies on the Group....147

Chapter 7: Using Scan Now....149
About Scan Now....149
The Virus and Malware Scan Wizard....150
Using the Virus and Malware Scan Wizard....150
Running Scan Now on Selected Targets....156
Running Scan Now on an Endpoint....156
Running a Custom Scan Now on an Endpoint Using the Agent Control Panel....162
Running a Full Scan Now on an Endpoint Using The Agent Control Panel....163
Running Scan Now on a Group....164
Scan Now Task Status....169

Viewing Scan Now Tasks....170
Viewing the Last AntiVirus Scan Log on an Endpoint....170

Chapter 8: Viewing Virus Scan Results....173
About Virus Scan Results....173
Viewing Virus and Malware Event Alerts....173
The Virus and Malware Event Alerts Page....174
The Virus and Malware Event Alerts Page Toolbar....174
The Virus and Malware Event Alerts Page List....175
The Virus/Malware Details Page....176
Viewing the Virus/Malware Details Page....176
The Virus/Malware Details Page List....177
Endpoint Malware Details....178
Viewing Endpoint Malware Details....178
Endpoint Details Virus and Malware Tab....179
Group Malware Details....180
Viewing Group Malware Details....180
Group Virus and Malware Event Alerts View....181
Checking Virus Scan Status....182
Viewing the Virus/Malware Details Page....182
The Virus/Malware Details Page List....182

Chapter 9: Managing Quarantined Files....185
Understanding Quarantine....185
Viewing Files in Quarantine....187
Viewing Quarantined Files Using Centralized Quarantined....188
Viewing Quarantined Files Using the Agent Console....188
Restoring a File from Quarantine....189
Restoring a Quarantined File Using Centralized Quarantine....190
Restoring a Quarantined File Using the Agent Console....190
Deleting a File from Quarantine....191
Deleting a Quarantined File Using Centralized Quarantine....191
Deleting a Quarantined File Using the Agent Console....192
Deleting Files from Quarantine Automatically....192

Chapter 10: Reporting....195
About Antivirus Reports....195
The Antivirus Reports Page....196
Setting Parameters and Options....197
Generating an AntiVirus Definition Version Status Report....198
Generating an Endpoint/Groups with Infections by Date Report....198

Chapter 1

AntiVirus Overview

In this chapter:

- The Virus and Malware Threat
- The Role of Ivanti AntiVirus
- Ivanti AntiVirus Technologies
- Ivanti AntiVirus Scan Types

Viruses and malware are an ever-present danger in today's complex computing environment. There are many different types of malicious software, which can cause damage ranging from the trivial to the catastrophic. The threat is constantly evolving, with new viruses being identified on a daily basis.

The source of the threat is also changing. Previously, creators of malware were often misguided enthusiasts keen to prove how clever they were. Much of today's malware is created by people with a more sinister agenda, including cyber-criminals who want to access corporate and personal data for financial gain.

There are, however, well-defined technologies and strategies for dealing with the threat posed by viruses and malware. Ivanti AntiVirus provides a comprehensive solution to the malware problem.

The Virus and Malware Threat

Viruses and other forms of malicious software can infect an endpoint without the operator knowing. It is vital that they are removed as soon as possible.

A virus is a program that can copy itself and infect an endpoint, with potentially harmful results. A virus is a specific type of *malware* (malicious software). There are many other types of malware, however, including Trojans, worms, rootkits, and spyware. For a more detailed explanation of the main types of malware, see Malware Categories on page 10.

Note: The term *virus* is often used to describe other types of malware that are not true viruses. Likewise, the term *antivirus* is often used to describe systems that protect endpoints from malware in general, and not just from viruses. AntiVirus provides broad protection against all types of malware.

One of the main characteristics of malware is that it is designed to infiltrate systems without the operator's consent. Once it infiltrates, malware remains on the endpoint – an unwanted and potentially dangerous guest.

The effect that malware has on an endpoint or network depends very much on the intent of the person or group that created it. Some types of malware can be hugely destructive, deleting files and spreading

to other endpoints on the network. Other types can give unauthorized users access to the endpoint, enabling them to steal valuable information. Even when the effects are not so damaging, malware consumes system resources and reduces productivity. No matter how little damage a virus or malware *seems* to cause, it should be removed as soon as possible. There is always the possibility of it infecting another endpoint, or having a more damaging effect over time.

Malware Categories

Read about the main types of malicious software (malware) that can affect your endpoints and networks.

Malware Type	Description
Adware	*Adware* is a program that displays or downloads an advertisement, which would classify it simply as intrusive rather than destructive. Some adware programs also function as spyware as well.
Backdoor	A *backdoor* is a program that enables bypassing the normal authentication procedures to gain remote access to an endpoint. Some backdoors are implemented in a way which requires the endpoint user's intervention, like a *Trojan*. Other types of backdoor can be installed without any such intervention.
Backdoor Trojan	A *backdoor Trojan* combines aspects of two types of malware. The *backdoor* element does not damage the endpoint, but it sets it up for remote control and unauthorized use (which is, of course, very dangerous). The *Trojan* element indicates that it is installed unwittingly by the user. Some legitimate remote administration programs can be configured to act as backdoor Trojans. These programs should be identified as security risks.
Blended threat	A *blended threat* combines the characteristics of different types of malware, such as *worms*, *viruses*, and *Trojans*. It can also take advantage of specific server vulnerabilities. Blended threats can be quite dangerous because they use multiple techniques to spread through and damage a network.
Bot	A *bot* (short for *robot*) is a software agent that causes an endpoint to carry out an automated action, without the user's knowledge, and often for malicious purposes. For example, an endpoint could be used to target a Web server, inundating it with such a volume of requests that it cannot handle them and its normal service is disrupted, called a *denial-of-service* attack (DoS).
Botnet	A *botnet* is a network of endpoints that are infected with *bot* agents. Such networks can be harnessed to take part in *distributed denial-of-service* (DDoS) attacks, where multiple endpoints are used to send requests to overwhelm a Web server.

Malware Type	Description
Dropper	A *dropper* is a program that surreptitiously installs some type of malware, such as a virus or backdoor. A single-stage dropper contains the malware within itself, and prevents detection by virus scanners. A two-stage dropper first installs itself, then downloads the malware to the target machine.
Keylogger	A *keylogger* (keystroke logger) tracks the keys pressed by a user and transmits them covertly to a remote location.
Macro virus	A *macro virus* is malicious code written in a macro language such as that used in Microsoft Word or Excel. It is resident in a document or template file rather than an executable. The macro program runs when the document is opened, spreading the macro virus to other documents and templates. The macro virus also spreads when new documents are created with an infected template.
Malware	*Malware* (malicious software) is the catch-all term used to describe all types of software designed to infiltrate or damage files, endpoints, or networks.
Rootkit	A *rootkit* is software that can be used to modify the host operating system so as to conceal the existence of malicious programs. For example, it can modify the display of running processes to conceal malicious ones from the user, and hide files and registry entries. The term originally comes from UNIX computing – a rootkit was a set of tools used by someone who had gained *root* (administrator) access. While it may sometimes have a legitimate purpose, rootkits are now most often used to conceal malware. **Note:** Rootkit detection is only supported on endpoints running Windows versions from Vista onwards.
Spyware	*Spyware* is a type of malware that covertly collects information about endpoint users, including personal and business-related information and Internet browsing patterns.
Trojan	A *Trojan* (called after the Trojan horse of Greek legend) is a type of malware that conceals its purpose from the user, while posing as a useful or desirable program. Trojans are often downloaded from the Internet in the form of free or trial-version software. Once installed, some Trojans can cause severe damage to an endpoint such as deleting the file structure of the disk.
Virus	A *virus* is malicious code that infects an executable file (the host), and that spreads to other executables when the program is run. A virus can contain a payload that causes other, possibly malicious, actions. A virus needs human interaction to spread to other files and across networks.

Malware Type	Description
Worm	A *worm* is a self-replicating type of malware. Unlike a virus, it is self-contained – it does not need to infect a host file. What's more, it does not require any outside intervention to spread through a network. A worm causes harm to the network by consuming network bandwidth while it is propagating. Some worms carry a payload that can cause additional damage such as deleting or encrypting files, or sending unwanted emails.

The Role of Ivanti AntiVirus

Ivanti AntiVirus, an optional part of Ivanti Endpoint Security (Ivanti Endpoint Security), can be deployed to provide comprehensive protection against viruses and other malware.

Caution: It is not advisable to run Ivanti AntiVirus along with another antivirus product. Ivanti recommends you replace any existing antivirus product with Ivanti AntiVirus.

When Ivanti AntiVirus is enabled, its functionality is completely integrated into Ivanti Endpoint Security. New menu items and page views become available, enabling an administrator to quickly deploy the anti-malware functionality. For example, you can launch a virus and malware scan from the **Discover** menu in a similar way to which you launch a *Discover Applicable Updates* task.

The signature-based protection is essentially a *blacklisting* approach, in contrast to the *whitelisting* approach used by Ivanti Application Control. Combining these approaches in an integrated application provides a strong, layered defense that ensures maximum protection for the network and its endpoints.

Ivanti AntiVirus Technologies

Ivanti AntiVirus uses a signature-based approach to detect known malware.

Ivanti AntiVirus uses a conventional signature-matching technique to search for and identify known viruses and malware. This technique uses *signature files* which are constantly updated to take account of the latest malware threats. Up-to-date versions of these files are regularly downloaded to the Ivanti Endpoint Security Server and distributed to the network's endpoints where they are used in different types of scans to protect the network from attack.

Ivanti AntiVirus Scan Types

Ivanti AntiVirus malware scans can be initiated in two distinct ways. *Policy-based* scans run according to predefined policies, while *Scan Now* virus and malware scans are run directly by an administrator.

Policy-based scans	Policy-based scans run automatically according to a predefined settings. There are two types of policy-based scans: • Recurring virus and malware scans run according to a time schedule. • Real-time monitoring scans run whenever an endpoint performs an action on a file. For more information on these scan types, see Policy-based Malware Scanning on page 13.
Scan Now virus and malware scans	The Scan Now virus and malware scan is usually run a single time. It is run directly by an administrator when there is a perceived malware threat to an endpoint, a group of endpoints, or the entire network. It can be run immediately, or scheduled for later execution if desired. For more information, see Scan Now Virus and Malware Scan on page 14.

In practice, policy-based scans provide the main form of protection to the network. They run automatically and consistently, without human intervention. A set of well designed policies can provide excellent protection to the network. The Scan Now feature performs a useful complementary role, enabling the administrator to react directly to a specific threat or suspicious activity.

Policy-based Malware Scanning

Ivanti AntiVirus offers two types of policy-based malware scanning: recurring virus and malware scan, and real-time monitoring.

Recurring virus and malware scan	Scheduled to run on a regular basis, which can range in frequency from daily to weekly. The policy should specify a detailed scan that will be able to detect infected files that other policy types (such as real-time monitoring scans) might miss.

Real-time monitoring	Runs whenever an endpoint performs specified actions on a file. For example, the policy can specify that the file is scanned whenever it is read or executed. **Note:** Real-time monitoring is also known as *on-access scanning*, because the file has to be accessed before any other action is performed on it. An advantage of real-time monitoring is that it can detect viruses before they are triggered.

Scan Now Virus and Malware Scan

The *Scan Now* feature, sometimes called an *on-demand scan*, enables a virus and malware scan to be run immediately in response to a perceived threat, rather than waiting for a policy-based scan to run.

The **Scan Now - Virus and Malware Scan** option launches the ***Virus and Malware Scan Wizard***, a fast and convenient way to configure and run an antivirus scan. This wizard provides detailed control over scanning options and the endpoints or groups to be scanned. The wizard allows you to tailor the scan to precisely address the apparent virus or malware threat.

Note: The term *Scan Now* is also used in the context of a Discover Applicable Updates (DAU) task, which assists with the management and deployment of content items. A DAU task is not related to Ivanti AntiVirus functionality.

Comparison of Ivanti AntiVirus Scan Types

Though they use the same definition file, each Ivanti AntiVirus scan type provides its own unique depth and breadth of virus and malware protection.

The Real-time monitoring, Scan Now and Recurring virus and malware scan technologies provided with Ivanti AntiVirus work together to clean and quarantine suspicious files on endpoints.

Table 1:

	Automatic	On-Demand	
	Real-Time Monitoring	**Scan Now**	**Recurring Virus and Malware Scan**
Detection	Threats before they are triggered. Particularly efficient at detecting viruses.	"Sleeping" threats (for example, those which passed through real-time monitoring because a definition was not yet available). Particularly efficient at detecting malware.	

	Automatic	On-Demand	
	Real-Time Monitoring	**Scan Now**	**Recurring Virus and Malware Scan**
Endpoint Performance	Small but detectable impact. **Note:** Automatic scan performance can be improved during scan configuration by excluding as many safe files and paths as possible.	Significant impact. **Note:** On-Demand scan performance can be improved during scan configuration: • Set CPU utilization % to low, • Clear the Scan archives option, • Exclude as many safe files and paths as possible.	
Coverage	Only files on which an endpoint performs an action (e.g. read, write).	All files on an endpoint.	
Frequency	On-going	One-off, immediate or scheduled for later.	Runs on a regular basis, from daily to weekly for a specified period.

Ivanti recommends you run Real-time monitoring with a regular Recurring virus and malware scan (minimum weekly).

Chapter 2

Getting Started with AntiVirus

In this chapter:

- AntiVirus at a Glance
- The Ivanti AntiVirus Workflow

Learn the initial tasks you need to perform to start protecting your network from against all malware, including viruses, Trojans, rootkits, spyware and adware.

You will continue to perform these tasks, plus many others. Ivanti Endpoint Security contains many features and functions, and by learning the environment, you can secure your network quickly and efficiently.

Important: Before you roll out AntiVirus to endpoints in an environment, it is recommended that you work with your end users and other stakeholders, together with any IT security personnel, to start formulating a business policy regarding the usage of peripheral devices. Having a clear idea of what is to be achieved from the start will help shape the future steps you take with this product.

AntiVirus at a Glance

Learn the basic concepts, functions, and terminology you require to be proficient in the use of Ivanti AntiVirus.

Benefits

- Provides in-depth protection against malware resident on endpoints without compromising productivity.
- Ensures malware is cleaned from endpoints or blocks it from running.
- Speeds investigation and remediation of suspect endpoints through widgets, reports, and warnings.
- Maintains clean endpoints by ensuring that any detected malware is removed or quarantined and not allowed to remain on network assets.
- Automated, attendant-free operation through the automatic download of signatures/agent updates.
- Integrates with other Ivanti Endpoint Security product modules.

Key terms

Definition file	A collection of signatures used by AntiVirus to identify and capture viruses and other malware.
False positive	An antivirus scan result where a file is wrongly suspected to be infected by a virus or other malware. This term applies to environments with the AntiVirus module installed.
Malware	Malicious software developed for the purpose of causing harm to a computer system, such as viruses, Trojan horses, spyware, and malicious active content. This term applies to environments with the AntiVirus module installed.
Quarantine	A secure folder that holds files suspected of containing a virus or other suspicious code. An Administrator can review the contents to decide what items are safe (for example, false positives) or should be deleted. This term applies to environments with the AntiVirus module installed.
Spyware	Software that obtains information from a user's computer without their knowledge or consent. This term applies to environments with the AntiVirus module installed.
Zero-day exploit	A software vulnerability that security researchers and software developers are not yet aware of. They pose a higher risk to users than other vulnerabilities of penetrating a system undetected and unnoticed. This term applies to environments with the AntiVirus module installed.

The Ivanti AntiVirus Workflow

Learn the sequence of specific tasks you need to perform to create your first AntiVirus policy.

Install the AntiVirus module server component. This component is installed after the initial Ivanti Endpoint Security installation.

Note: If you purchased an AntiVirus license during your initial Ivanti Endpoint Security purchase, AntiVirus is installed during the initial Ivanti Endpoint Security installation by default.

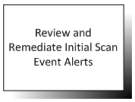
For more information, see Step 1: Install the AntiVirus Module Server Component on page 19.

Add the AntiVirus module endpoint component to agents you want to support AntiVirus functions. Each agent you add the endpoint component to consumes an AntiVirus license. For more information, see Step 2: Add the AntiVirus Module to Endpoints on page 20.

Use the endpoint or group management pages to ensure all the endpoints you specified have installed the AntiVirus module. For more information, see Step 3: Verify AntiVirus Endpoint Component Installation Status on page 20.

Create a new group (or multiple groups) to enable the collectively manage endpoints using the AntiVirus module For more information, see Step 4: Create an AntiVirus Group on page 21.

Perform a thorough or full system scan to ensure your environment is free of active threats. For more information, see Step 5: Run an Initial Virus and Malware Scan on page 22.



Upon completion of the initial scan, details about malware detected are displayed on the Virus and Malware Events Alerts page for review and remediation purposes. For more information, see Step 6: Review and Remediate Initial Scan Event Alerts on page 25.

Use the scheduled (periodic) and/or real-time (continuous) scan capabilities to provide on-going, in-depth protection against malware. For more information, see Step 7: Create AntiVirus Policies to Monitor Your Environment on page 25.

Step 1: Install the AntiVirus Module Server Component

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

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

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

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

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

   Step Result: The ***Install/Update Components*** dialog opens.

4. Click **Next** to dismiss the **Database backup recommended** notification.

   Ivanti recommends backing up your database before installing a module.

5. Click **Install**.

   Step Result: A dialog opens, notifying you that installing the module may cause users currently logged in to lose their work.

6. Click **OK**.

   Step Result: The installation begins.

7. Click **Finish**.

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

Result: The AntiVirus server module is installed.

After Completing This Task:
Continue to Step 2: Add the AntiVirus Module to Endpoints on page 20.

Step 2: Add the AntiVirus Module to Endpoints

After installing the AntiVirus server module, you must add the AntiVirus module to your managed network endpoints.

Prerequisites:

- Complete Step 1: Install the AntiVirus Module Server Component on page 19.
- Ivanti Endpoint Security Agent must be installed on target endpoints.
- Antivirus software from any other vendors should be uninstalled from target endpoints.
- Target endpoints must have a minimum of 2 GB of free disk space for the creation of temporary files during AntiVirus engine and definitions file updates.

The endpoint component is added from the ***Endpoints*** page.

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

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

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

   Step Result: The ***Add/Remove Modules*** dialog opens.

4. Select the **AntiVirus** check box for all endpoints you want to install the component on.
5. Click **OK**.

Result: The AntiVirus module is added to the selected endpoints and Windows Security Center recognizes Ivanti AntiVirus as the antivirus program on each.

After Completing This Task:
Continue to Step 3: Verify AntiVirus Endpoint Component Installation Status on page 20.

Step 3: Verify AntiVirus Endpoint Component Installation Status

Use the endpoint or group management pages to ensure all the endpoints you specified have installed the AntiVirus module.

Server

Prerequisites:

Complete Step 2: Add the AntiVirus Module to Endpoints on page 20.

1. Access the agents from the group or endpoint level:

Option	Description
Groups view	1. From the navigation menu, select **Manage** > **Groups**. 2. From the **Browser** tree, select the group that contains endpoints with the AntiVirus module installed.
Endpoints view	From the navigation menu, select **Manage** > **Endpoints**.

2. On the **All** tab, ensure the value for an endpoint's AV Installed column is `Yes`.

After Completing This Task:
Add the AntiVirus module to endpoints you require.

Endpoint

1. Right-click on the **Agent Control Panel** icon in the Windows system tray and select **Agent Control Panel**.

   Step Result: The ***Agent Control Panel*** displays.

2. Ensure **AntiVirus** appears among the menu options on the left menu bar.

After Completing This Task:
Continue to Step 4: Create an AntiVirus Group on page 21.

Step 4: Create an AntiVirus Group

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

Prerequisites:

Complete Step 3: Verify AntiVirus Endpoint Component Installation Status on page 20.

Tip: If groups already exist and suit your AntiVirus purposes, group creation is not necessary. You can use those groups instead. However, AntiVirus adds new group settings. If you use preexisting groups for AntiVirus, edit the group settings to leverage new features.

1. From the navigation menu, select **Manage** > **Groups**.

2. From the **Browser** tree, select **Custom Groups**.

   Groups are arranged within a directory 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.
   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.
   c) Click **Save**.

Result: The group is created.

After Completing This Task:
Continue to Step 5: Run an Initial Virus and Malware Scan on page 22.

Step 5: Run an Initial Virus and Malware Scan

Use the ***Scan Now - Virus and Malware Scan Wizard*** to perform a thorough or full system scan to ensure your environment is free of active threats.

Prerequisites:

Complete Step 4: Create an AntiVirus Group on page 21.

The first virus and malware scan you run should utilize all the of the protection mechanisms provided by the AntiVirus module. By default, the ***Scan Now - Virus and Malware Scan Wizard*** is configured to perform the most thorough scan possible:

- Attempts to clean then quarantine then delete any viruses it detects.
- Scans boot sectors and automatically repairs them.
- Scans archive files such as .zip, .cab, and .rar.
- Scans memory.
- Detailed logging level (includes results summary, name, time, and status for each scanned file)

Note: Be prepared for the scan to last a considerable duration.

1. Select **Discover** > **Scan Now – Virus and Malware Scan**. If you are on the ***Virus and Malware Event Alerts*** page, click **Scan Now**.

   Step Result: The ***Virus and Malware Scan Wizard*** opens to the ***Scan Name and Scheduling*** page.

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

   Note: By default, new virus scans are named `New Virus and Malware Scan`, followed by the server's date and time, which is formatted according to your browser's locale setting.

3. Schedule the scan using one of the following methods:

Method	Steps
To schedule an immediate scan:	Select the **Run scan immediately** option.
To schedule a later scan:	1. Select the **Run scan at** option. 2. Type the start date in the **Start date** field. You can also select the start date by clicking the **Calendar** icon. 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon. **Note:** The purpose of the deferred scan feature is to enable you to schedule the scan at a time that will not adversely affect network or endpoint performance.

4. Click **Next**.

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

5. Build a list of targets (endpoints) for the virus scan, using either or both of the following methods:

Method	Steps
To define targets using individual endpoints:	1. From the **Target type** list, select **Endpoints**. 2. In the search field, type an endpoint name in one of the following formats: *endpointname* or *domain\endpointname*. Alternatively, you can type an IP address. **Tip:** You can type a partial name or IP address to search for a range of endpoints. 3. Click the **Search** icon. One or more endpoints are displayed in the area under the search field. 4. Select the check box for the endpoint you want to scan. 5. Click **Add to Target List**.
To define targets using endpoint groups:	1. From the **Target type** list, select **Endpoint Groups**. 2. In the tree control, select one or more endpoint groups. 3. Click **Add to Target List**. **Note:** You can exclude an endpoint or subgroup from a group that is to be scanned. Select the endpoint/subgroup in the tree control and click **Exclude from Target List**.

Note: You must add at least one endpoint or group for **Next** to become available. If you change your mind about anything you have added to the target list, you can remove it from the list by selecting its check box and clicking **Remove**.

Step Result: One or more endpoints are assigned to the scan.

6. Click **Finish**.

Step Result: The ***Virus and Malware Scan Wizard*** closes. The scan begins, either immediately or at the scheduled time. After the scan completes, the ***Virus and Malware Scan Results*** page displays details of any malware that has been detected.

Result: The scan begins, either immediately or at the scheduled time. After the scan completes, **Review** > **Virus and Malware Event Alerts** lists the malware that has been detected. Any files with known threats will be cleaned, deleted, or quarantined.

After Completing This Task:
Continue to Step 6: Review and Remediate Initial Scan Event Alerts on page 25.

Step 6: Review and Remediate Initial Scan Event Alerts

Details about malware detected during the initial scan are displayed on the Virus and Malware Events Alerts page.

Prerequisites:

Complete Step 5: Run an Initial Virus and Malware Scan on page 22.

The page provides a centralized view of all the *Event Alerts* generated during the scan, each of which include the name of the malware detected and the endpoints affected. You can then (if necessary) take further action to remove any remaining malware threat to the network.

1. Select **Review** > **Virus and Malware Event Alerts**.

   Step Result: The ***Virus and Malware Event Alerts*** page opens.

2. Review the results.

   Tip: You can use the **Group By** row, available above the list, to sort list items into groups based on column headers. This feature (along with the filters above the toolbar) is useful when you need to examine a large number of event alerts.

After Completing This Task:

You can use Scan Now to launch the ***Virus and Malware Scan Wizard***, configuring it to perform specific actions that will reduce the threat to the network. See Using the Virus and Malware Scan Wizard on page 150 for more information.

Complete Step 5: Run an Initial Virus and Malware Scan on page 22.

Step 7: Create AntiVirus Policies to Monitor Your Environment

Use the scheduled (periodic) and/or real-time (continuous) scan capabilities to provide on-going, in-depth protection against malware.

Prerequisites:

Step 6: Review and Remediate Initial Scan Event Alerts on page 25

The Ivanti Endpoint Security agents that detect and remediate malware threats on endpoints need to be assigned a properly configured antivirus policy. Policies define such features as when the endpoints will be scanned for threats, where on endpoints to search for threats, and the actions to be taken when threats are discovered.

The AntiVirus module enables you to create two types of antivirus policies: *Recurring Virus and Malware Scan* and *Real-time Monitoring Policy*.

Recurring Virus and Malware Scan
Runs a scan on a regular, scheduled basis. It typically analyzes all the files on an endpoint (except those specifically excluded from the scan). It can take an appreciable amount of time to run if there are a large number of files to be scanned.

1. Select **Manage** > **Antivirus Policies**.

   Step Result: The ***Antivirus Policies*** page opens.

2. From the ***Manage*** > ***AntiVirus Policies*** toolbar, select **Create** > **Recurring Virus and Malware Scan**.

   Step Result: The ***Recurring Virus and Malware Scan Policy Wizard*** opens at the ***Name and Schedule Policy*** page.

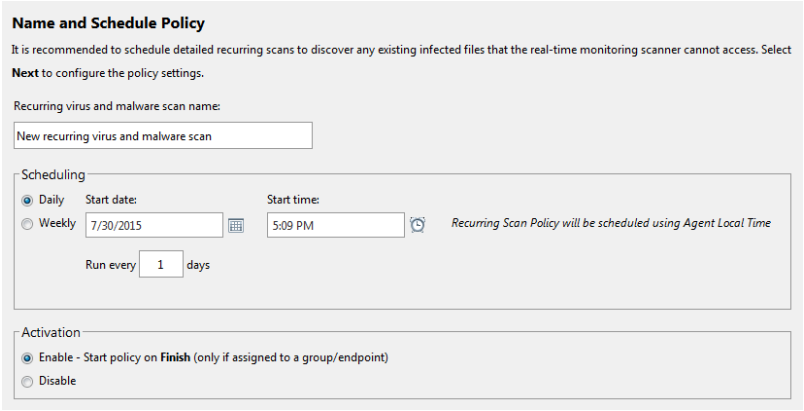


Figure 1: Recurring Virus and Malware Scan Policy Wizard

3. Type a new name in the **Recurring virus and malware scan name** field. Make the name descriptive, conveying the role of this recurring policy.

Note: The name must be unique, otherwise a warning will be displayed.

4. Select and configure a **Scheduling** option:

Important: If an endpoint's internal clock changes (for example, due to Daylight Savings Time or time-zone differences while travelling) a recurring scan scheduled to take place during the time skipped will not occur.

Ensure you or the endpoint user run a Scan Now immediately after a time change to maintain continuous protection.

Method	Steps
Daily	1. Select the **Daily** option. 2. Type the start date in the **Start date** field. You can also select the start date by clicking the **Calender** icon. 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon. 4. Type a value in the **Run every x days** field.
Weekly	1. Select the **Weekly** option. 2. Type the start date in the **Start date** field. You can also select the start date by clicking the **Calender** icon. 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon. 4. Type a value in the **Run every x weeks on:** field. **Note:** Leave the value at 1 if you want the scan to run at least once a week. 5. Select one or more of the daily check boxes to run the scan on those days.

5. Select an **Activation** option.

Setting	Result
Enable - Start policy on Finish (only if assigned to a group/endpoint)	The policy is created and activated when you click **Finish** and the wizard closes. **Note:** The policy must be assigned to at least one endpoint or group.

Setting	Result
Disable	The policy is created but not activated when you click **Finish** and the wizard closes. You may activate it at a later time.

6. Click **Next** to set the scanning options.

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

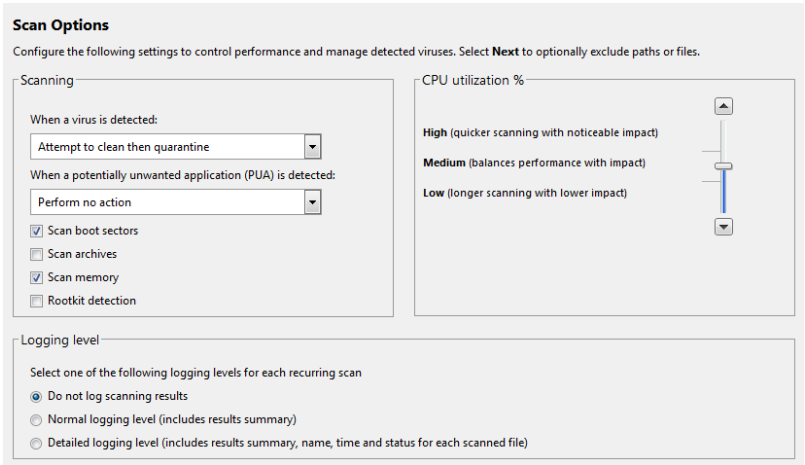


Figure 2: Recurring Virus and Malware Scan Wizard - Scan Options

Note: If you click **Finish** at this point, a basic policy is created, but is not assigned to any endpoints. You can configure the policy further and assign it to endpoints later.

7. From the drop-down list, select the action that occurs when a virus is detected.

Setting	Result
Perform no action	Does nothing with the infected file, but sends an alert to the server.
Attempt to clean then quarantine	Attempts to clean the infected file. If this is not possible, the file is quarantined. An alert is sent to the server. **Note:** This option is the default selection.
Attempt to clean then delete	Attempts to clean the infected file. If this is not possible, the file is deleted. An alert is sent to the server.

Setting	Result
Attempt to clean then quarantine then delete	Attempts to clean the infected file. If this is not possible, the file is quarantined. If it is not possible to quarantine it, it is deleted. An alert is sent to the server.

Note:

- To *clean* an infected file means to completely remove the malicious code so that the file is safe to use. It is not always possible to remove the malicious code, however. When this happens, you can either delete the file or *quarantine* it. To quarantine means to move it to a safe place on the endpoint where it can be kept for further examination.

  In certain cases (such as when the malware is a Trojan) the entire file is malicious. Such a file cannot be cleaned, so the only options are to quarantine or delete it.
- Virus detection actions are not used for memory scans.

8. From the drop-down list, select the action to be taken when a potentially unwanted application (PUA) is detected:

Setting	Result
Perform no action	The system ignores the potentially unwanted application. **Note:** This option is the default selection.
Send alert only	An alert is sent to the server only.
Alert and action (treat as malware)	An alert is sent to the server and the file is cleaned, quarantined, or deleted, according to the action you selected in the **When a virus is detected** drop down.

9. Set the **Scanning** options:

Setting	Result
Scan boot sectors	The virus scan will be more thorough if you scan boot sectors in addition to program and data files. **Note:** If malware is detected in a boot sector, the action taken depends on the virus detection option selected: • **Perform no action** - the boot sector is left as it is and an alert is sent to the ***Virus and Malware Event Alerts*** page. • **Clean/Delete/Quarantine** - the boot sector is automatically repaired.

Setting	Result
Scan archives	The virus scan will be more thorough if you scan archive files such as `.zip` and `.cab` files. **Note:** • Scanning archives will result in longer scan durations. • Infected .rar files can be quarantined and deleted, but can't be cleaned. See Archive Types Supported for Scanning on page 114
Scan memory	Viruses and other malware can reside in memory as well as on the disk(s). The virus scan will be more thorough if you scan memory for such viruses and malware. **Note:** Virus detection actions and exclusions are not applied to memory scans.
Rootkit detection	A rootkit, similar to a hack tool, enables attackers to gain administrator access to a system. They hide the attacker's presence and give them full control of a server or client endpoint without being noticed. **Note:** Rootkit detection is only supported on endpoints running Windows versions from Vista onwards.

10. Set the ***CPU utilization %*** threshold to control the level of impact the scan is to have on endpoint performance:

Setting	Result
High	Quicker scanning but may noticeably impact endpoint performance.
Medium	Balances scan speed with endpoint performance impact (default option).
Low	Slower scanning but has the lowest impact on endpoint performance.

11. Set the logging options:

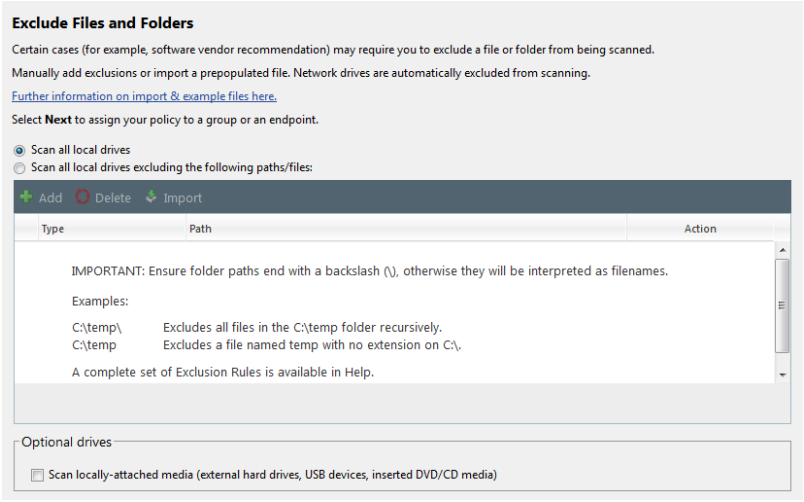
Note: As logging information is kept on the endpoint, the option you choose will not affect the loggings sent to the server.

Setting	Result
Do not log scanning results	No scan log is generated.
Normal logging level (includes results summary)	A standard scan log is generated.
Detailed logging level (includes results summary, name, time and status for each scanned file)	A detailed scan log is generated. **Caution:** Logging detailed virus scan results typically generates large amounts of data, especially when recurring scans run frequently.

12. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created, but not assigned to any endpoints. You can assign it to endpoints at a later time.

Step Result: The ***Exclude Files and Folders*** page opens.



This page enables you to exclude specified files and paths from the scan. You may want to do this because:

- You have some applications whose manufacturers recommend be excluded from virus scans.
- You have folders containing large amounts of data that you consider relatively safe, such as graphics files. Excluding them from the scan saves time.
- You have files that cause known "false positives" during a scan.

Caution: Excluding files or paths from the scan always involves some degree of risk.

13. Exclude files and folders, using one of the following methods:

Tip: Masks and system variables can be used in exclusions. See Exclusion Rules on page 138.

Note: More information on excluding files and folders from Ivanti AntiVirus malware scans, including recommended exclusions, can be found in Ivanti Community Article 58945.

Method	Steps
Manually exclude specific files and folders from the scan.	1. Click **Add**. A blank entry is added to the exclusions list. 2. Select an exclusion type from the **Type** field. The types are File and Folder. 3. Enter the path to the item you want to exclude in the **Path** field. 4. Click  to add the exclusion to the list. Repeat this procedure for all files and folders you want to exclude from the scan. **Note:** Click **Remove** () to remove items from the exclusion list.
Import an XML file containing a formatted list of file and folder exclusions.	See Importing File, Folder and Process Exclusions on page 136.

14. Configure the **Optional drives** settings:

Setting	Result
Scan locally-attached media	All storage media (including external hard drives, USB devices, and DVD/CD media) are included in the scan.

15. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created, but not assigned to any endpoints. You can assign it to endpoints at a later time.

Step Result: The **Assign virus and malware scan policy to groups and/or endpoints** page opens.

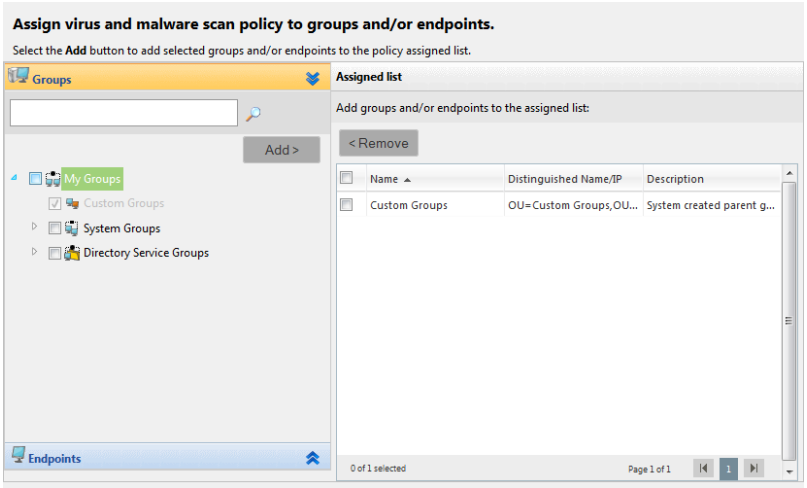


Figure 3: Assign Policy to Groups or Endpoints

16. Build a list of targets (endpoints), using either or both of the following methods:

Important: Recurring scans will not run on an endpoint that is shutdown or hibernating at the scheduled scan time.

Method	Steps
To define targets using groups:	1. If the **Groups** section is not open, click its up arrow to open it. 2. Select one or more endpoint groups by selecting their check boxes. 3. Click **Add**. This adds the group(s) to the **Assigned** list.

Method	Steps
To define targets using endpoints:	**1.** If the **Endpoints** section is not open, click its up arrow to open it. **2.** In the search field, do one of the following: • Type an endpoint name (to search for a specific endpoint) • Type part of an endpoint name (to search for similarly named endpoints) • Leave it blank (to search for all available endpoints) **3.** Click the **Search** icon. Depending on what you typed, one or more endpoints will appear in the **Name** column, with their respective IP addresses. **4.** Select the check box for each endpoint you want to assign. **5.** Click **Add**. This adds the endpoint(s) to the **Assigned** list.

Note: You can remove targets from the **Assigned** list by selecting the applicable check boxes and clicking **Remove**.

17. Click **Finish**.

Step Result: The ***Virus and Malware Scan Policy Wizard*** closes. The newly created policy is displayed in the ***Antivirus Policies*** page.

Real-Time Monitoring Policy

Runs a scan when an endpoint accesses a file to carry out an action such as a read or a write. It continuously checks files in the background for malware before it gets a chance to cause damage.

1. Select **Manage** > **Antivirus Policies**.

Step Result: The ***Antivirus Policies*** page opens.

2. Click **Create** > **Real-time Monitoring Policy**.

   Step Result: The ***Real-time Monitoring Policy Wizard*** opens.

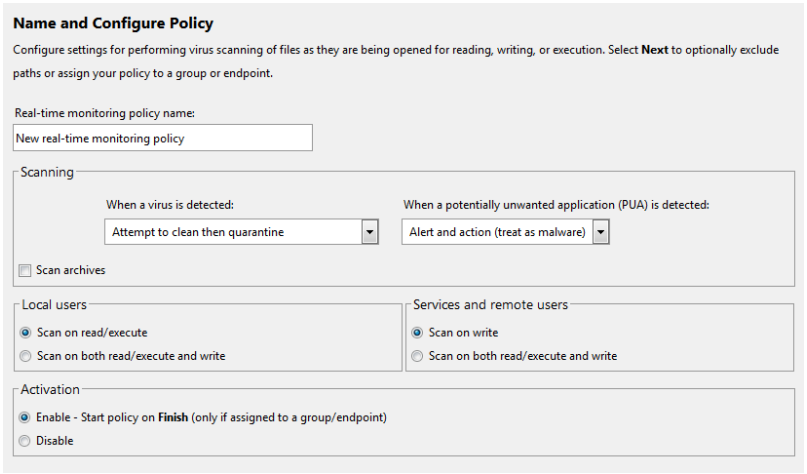


Figure 4: Real-time Monitoring Policy Wizard

3. Type a new name in the **Real-time monitoring policy name** field. Make the name descriptive, conveying the role of this real-time monitoring policy.

   Note: The name must be unique. If it is not, a warning will be displayed.

4. From the drop-down list, select the action that occurs when a virus is detected.

Setting	Result
Perform no action	Does nothing with the infected file, but sends an alert to the server.
Attempt to clean then quarantine	Attempts to clean the infected file. If this is not possible, the file is quarantined. An alert is sent to the server. **Note:** This option is the default selection.
Attempt to clean then delete	Attempts to clean the infected file. If this is not possible, the file is deleted. An alert is sent to the server.

Setting	Result
Attempt to clean then quarantine then delete	Attempts to clean the infected file. If this is not possible, the file is quarantined. If it is not possible to quarantine it, it is deleted. An alert is sent to the server.

Note:

- To *clean* an infected file means to completely remove the malicious code so that the file is safe to use. It is not always possible to remove the malicious code, however. When this happens, you can either delete the file or *quarantine* it. To quarantine means to move it to a safe place on the endpoint where it can be kept for further examination.

  In certain cases (such as when the malware is a Trojan) the entire file is malicious. Such a file cannot be cleaned, so the only options are to quarantine or delete it.
- Virus detection actions are not used for memory scans.

5. From the drop-down list, select the action to be taken when a potentially unwanted application (PUA) is detected:

Setting	Result
Perform no action	The system ignores the potentially unwanted application. **Note:** This option is the default selection.
Send alert only	An alert is sent to the server only.
Alert and action (treat as malware)	An alert is sent to the server and the file is cleaned, quarantined, or deleted, according to the action you selected in the **When a virus is detected** drop down.

6. [Optional] Select the **Scan archives** check box to scan compressed files like: .zip, .rar, and .cab

Note:

- Scanning the contents of archive files will impact endpoint performance.
- Infected .rar files can be quarantined or deleted, but can't be cleaned.

See Archive Types Supported for Scanning on page 114

7. Configure the **Local users** setting. This applies when the endpoint is being used as a workstation, with a logged-on user.

Setting	Result
Scan on read/execute	Scans files before they are used.

Setting	Result
Scan on both read/execute and write	Scans files that are opened for write. New or changed files are scanned on close.

Note: With **Scan on read/execute** selected, it is possible that an infected file can be downloaded from the Internet and saved to disk. With **Scan on both read/execute and write** selected, the scanner will detect and (if possible) remove the malware before writing the file to disk.

8. Configure the **Services and remote users** setting. This applies when the endpoint is being used as a server. If someone physically logs on to the server, the **Local users** setting applies.

Setting	Result
Scan on write	Scans files that are saved to disk.
Scan on both read/execute and write	Scans files that are being read or executed, as well as those being saved to disk. **Note:** This is not the default option, as it increases scanning time. But if the server becomes infected, this is the option to select.

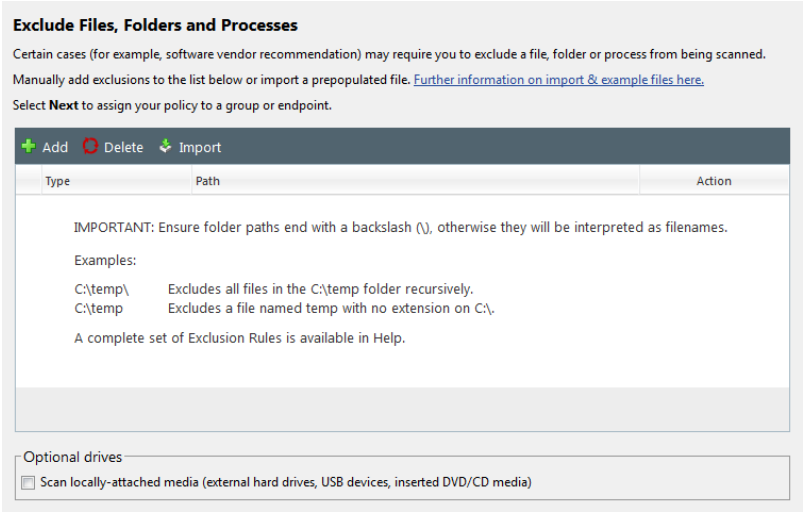
9. Select an **Activation** option.

Setting	Result
Enable - Start policy on Finish (only if assigned to a group/endpoint)	The policy is created and activated when you click **Finish** and the wizard closes. **Note:** The policy must be assigned to at least one endpoint or group.
Disable	The policy is created but not activated when you click **Finish** and the wizard closes. You may activate it at a later time.

10. Click **Next**.

Note: If you click **Finish** at this point, a basic policy is created, but is not assigned to any endpoints. You can configure the policy further and assign it to endpoints later.

Step Result: The ***Exclude Files, Folders and Processes*** page opens.



This page enables you to exclude specified files and paths from the scan. You may want to do this because:

- You have some applications whose manufacturers recommend be excluded from virus scans.
- You have folders containing large amounts of data that you consider relatively safe, such as graphics files. Excluding them from the scan saves time.
- You have files that cause known "false positives" during a scan.

Caution: Excluding files or paths from the scan always involves some degree of risk.

11. Exclude files, folders or processes, using one of the following methods:

Tip: Masks and system variables can be used in exclusions. See Exclusion Rules on page 138.

Note: More information on excluding files and folders from Ivanti AntiVirus malware scans, including recommended exclusions, can be found in Ivanti Community Article 58945.

Method	Steps
Manually exclude specific files, folders and processes.	1. Click **Add**. A blank entry is added to the exclusions list. 2. Select an exclusion type from the **Type** field. File, Folder, or Process. 3. Enter the path to the item you want to exclude in the **Path** field. 4. Click  to add the exclusion to the list. Repeat this procedure for all files, folders and processes you want to exclude from the scan. **Note:** Click **Remove** () to remove items from the exclusion list.
Import an XML file containing a formatted list of file, folder and and process exclusions.	See Importing File, Folder and Process Exclusions on page 136.

12. Configure the **Optional drives** settings:

Setting	Result
Scan locally-attached media	All storage media (including external hard drives, USB devices, and DVD/CD media) are included in the scan.

13. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created, but not assigned to any endpoints. You can assign it to endpoints at a later time.

Step Result: The ***Assign real-time monitoring policy to groups and/or endpoints*** page opens.

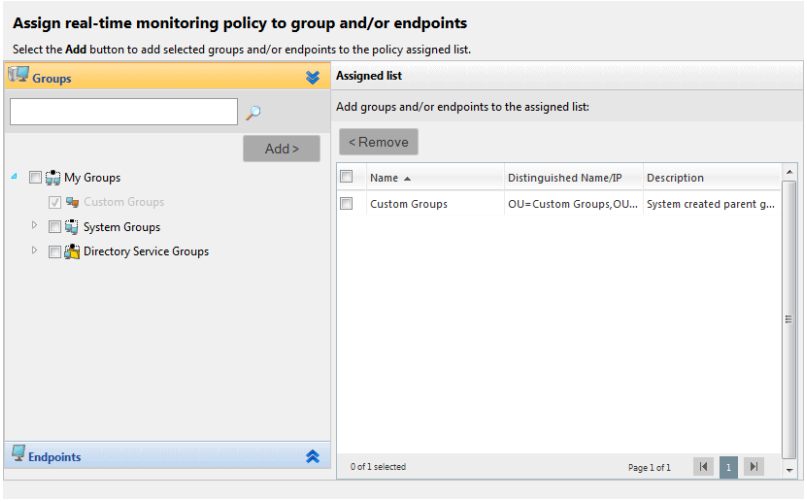


Figure 5: Assign Real-time Monitoring Policy Page

14. Build a list of targets (endpoints), using either or both of the following methods:

Important: Recurring scans will not run on an endpoint that is shutdown or hibernating at the scheduled scan time.

Method	Steps
To define targets using groups:	1. If the **Groups** section is not open, click its up arrow to open it. 2. Select one or more endpoint groups by selecting their check boxes. 3. Click **Add**. This adds the group(s) to the **Assigned** list.

Method	Steps
To define targets using endpoints:	**1.** If the **Endpoints** section is not open, click its up arrow to open it. **2.** In the search field, do one of the following: • Type an endpoint name (to search for a specific endpoint) • Type part of an endpoint name (to search for similarly named endpoints) • Leave it blank (to search for all available endpoints) **3.** Click the **Search** icon. Depending on what you typed, one or more endpoints will appear in the **Name** column, with their respective IP addresses. **4.** Select the check box for each endpoint you want to assign. **5.** Click **Add**. This adds the endpoint(s) to the **Assigned** list.

Note: You can remove targets from the **Assigned** list by selecting the applicable check boxes and clicking **Remove**.

15. Click **Finish**.

Step Result: The ***Real-time Monitoring Policy Wizard*** closes. The newly created policy is displayed in the ***Antivirus Policies*** page.

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***.

Ivanti Endpoint Security performs the following functions:

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

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

Common Functions

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

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

Common Conventions

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

Table 2: Common User Interface Conventions

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

Tip: Most pages support right-click.

The Navigation Menu

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

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

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

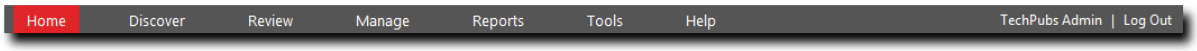


Figure 6: Navigation Menu

Table 3: Navigation Menus

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

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

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

Table 4: Discover Menu Items

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

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

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

Table 5: Review Menu Items

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

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

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

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

Table 6: Manage Menu Items

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

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

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

Table 7: Reports Menu Items

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

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

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

Table 8: Tools Menu Items

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

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

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

Table 9: Help Menu Items

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

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

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

The Page Banner

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

Figure 7: Page Banner

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

List Pages

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

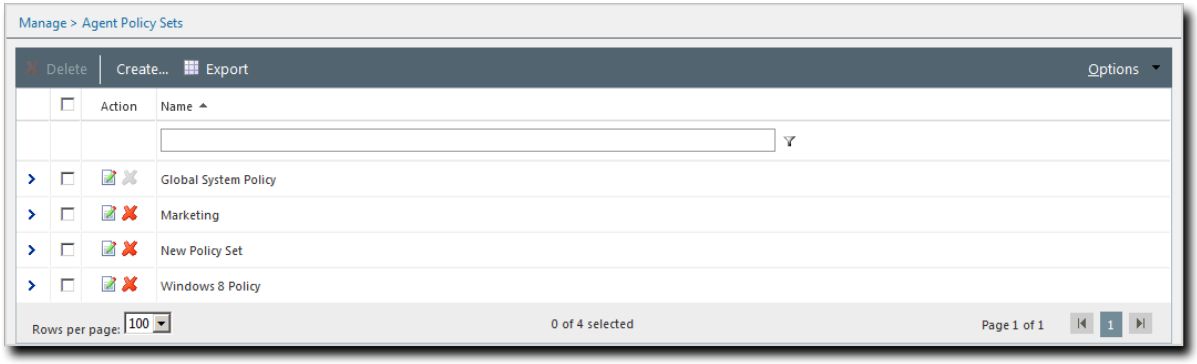


Figure 8: List Page

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.

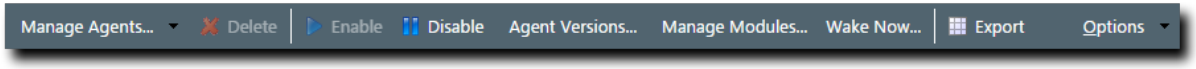


Figure 9: Toolbar

- 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 10: 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 54.
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 56
Show Group By Row[2]	Toggles the **Show Group By Row** on and off. For additional information, refer to Group By on page 58.
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.

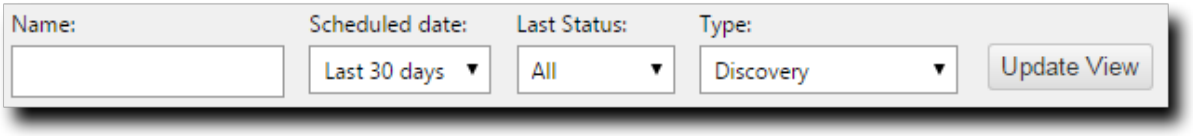


Figure 10: Filters

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 11: 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.

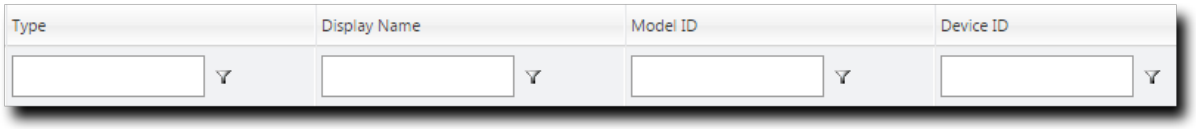


Figure 11: Filter Row

- 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 12: 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 52.
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 13: Data Filtering Types

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

Type	Description
NotIsNull	Returns results that have a value.

Note:

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

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

Using a Custom Date Range Filter

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

Prerequisites:

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

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

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

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

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

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

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

Group By

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

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

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

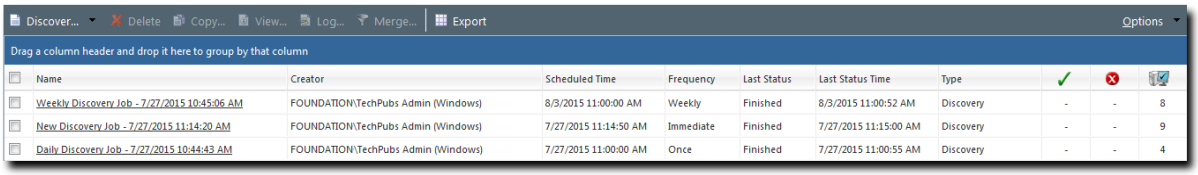


Figure 12: Group By Row

Expanding and Collapsing Structures

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

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

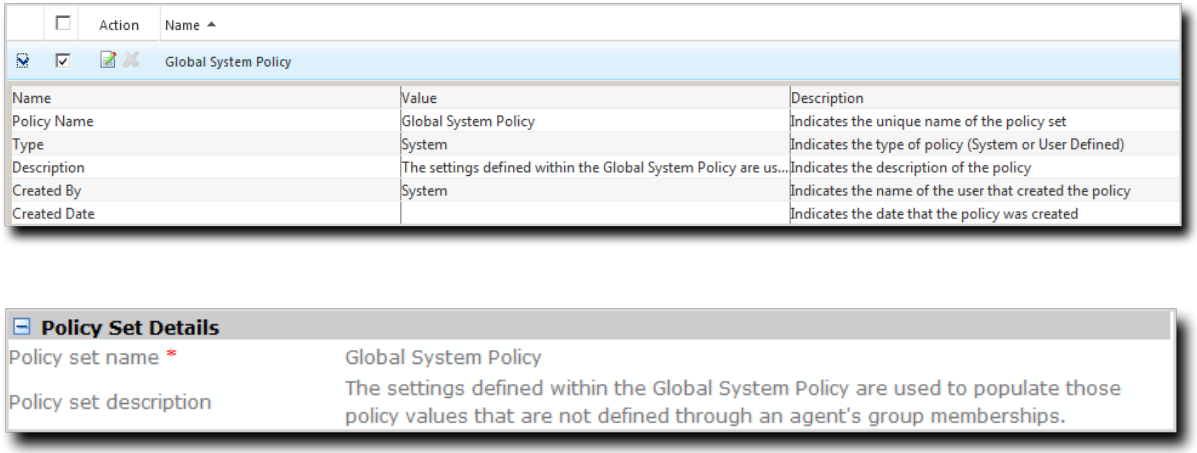


Figure 13: Expandable Structure Examples

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.

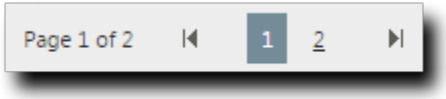


Figure 14: Pagination Feature

Table 14: Pagination Feature Functions

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

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

Help

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

Accessing Help differs according to context.

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

Use the following features to navigate through Help:

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

Exporting Data

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

You can export data from a variety of pages.

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

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

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

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

The Home Page

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

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

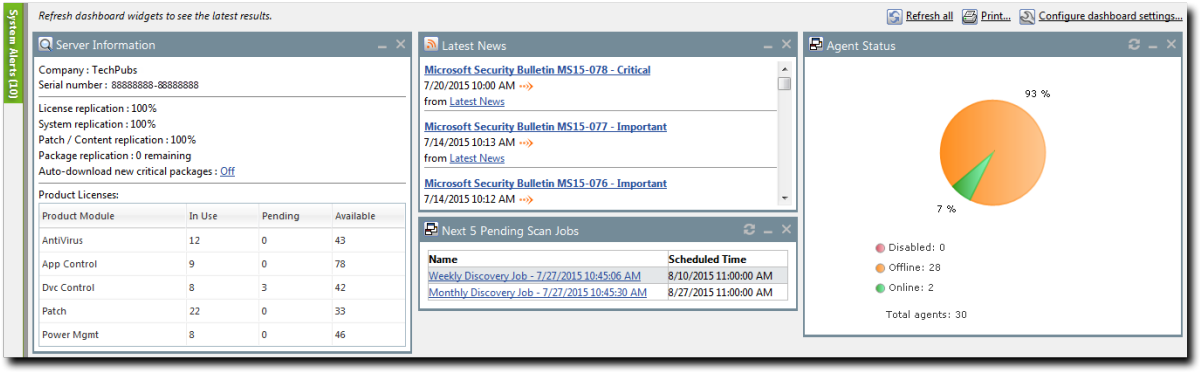


Figure 15: The Home Page

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 63
- The Agent Status Widget on page 63
- The Applicable Content Updates Widget on page 63
- The Discovery Scan Results: Agents Widget on page 67
- The Critical Patch Status by Endpoint Widget on page 66
- The Endpoints with Unresolved Updates Widget on page 67
- The Incomplete Deployments Widget on page 68
- The Last 5 Completed Scan Jobs Widget on page 68
- The Latest News Widget on page 69
- The Mobile Endpoint Last Check In Widget on page 69
- The Mobile Endpoint Status Widget on page 70
- The Mobile Endpoints with Policy Widget on page 70
- The Mandatory Baseline Compliance Widget on page 69
- The Next 5 Pending Scan Jobs Widget on page 71
- The Offline Patch Endpoints Widget on page 71
- The Patch Agent Module Status Widget on page 72
- The Scheduled Deployments Widget on page 72
- The Server Information Widget on page 73
- The Time Since Last DAU Scan Widget on page 74
- The Un-remediated Critical Vulnerabilities Widget on page 74
- The Endpoints with Unresolved AV Alerts Widget on page 75
- The Top 10 Infected Endpoints Widget on page 76
- The Top 10 Virus/Malware Threats Widget on page 77
- The Estimated Energy Savings: Daily Widget on page 77
- The Estimated Energy Savings: Weekly Widget on page 78
- The Estimated Energy Savings: Monthly Widget on page 79
- The Device Control Denied Actions Widget on page 79
- The Devices Connected to Endpoints Widget on page 80

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 15: 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 16: Agent Status Widget Fields

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

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

The Applicable Content Updates Widget

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

Table 17: Applicable Content Updates Widget Graph Bars

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

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

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

Table 18: Applicable Content Updates Widget Fields

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

Note:

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

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

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

Table 20: Critical Patch Status By Endpoint Bars

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

The following table describes the widget fields.

Table 21: Critical Patch Status By Endpoint Fields

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

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

Note:

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

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

Table 22: Discovery Scan Results: Agents Widget Fields

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

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

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

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

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

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

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

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

Note:

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

The Incomplete Deployments Widget

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

Table 23: Incomplete Deployment Widget Fields

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

The Last 5 Completed Scan Jobs Widget

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

Table 24: Last 5 Completed Scan Jobs Widget Columns

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

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

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

Click a link to view additional details about an announcement.

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

Table 25: Mandatory Baseline Compliance Widget Fields

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

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

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

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

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

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

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

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

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

This table describes each widget bar.

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

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

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

Table 26: Next 5 Pending Scan Jobs Widget Columns

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

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

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

Table 27: Offline Agents Widget Fields

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

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

The Patch Agent Module Status Widget

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

Table 28: Patch Agent Module Status Widget Fields

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

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

The Scheduled Deployments Widget

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

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

Table 29: Scheduled Deployments Widget Graph Bars

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

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

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

Table 30: Scheduled Deployments Widget Field

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

The Server Information Widget

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

Table 31: Server Information Widget Fields

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

Table 32: Product Licenses Table Columns

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

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

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

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

Table 33: Time Since Last Agent Scan Widget Fields

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

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

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

Table 34: Un-remediated Critical Vulnerabilities Widget Graph

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

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

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

Table 35: Un-remediated Critical Vulnerabilities Widget Fields

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

Note:

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

The Endpoints with Unresolved AV Alerts Widget

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

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

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

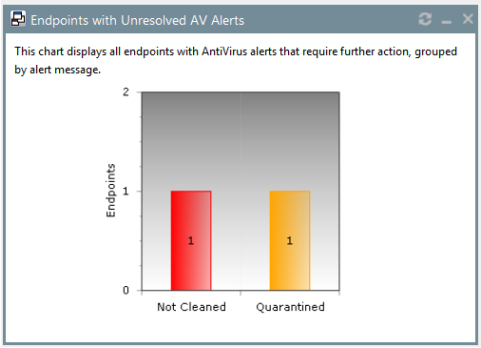


Figure 17: Endpoints with Unresolved AV Alerts Widget

The following table describes each graph bar.

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

The Top 10 Infected Endpoints Widget

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

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

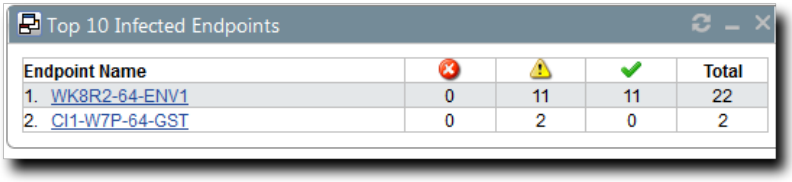


Figure 18: Top 10 Infected Endpoints Widget

The following table describes each column in the widget.

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

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

The Top 10 Virus/Malware Threats Widget

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

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

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

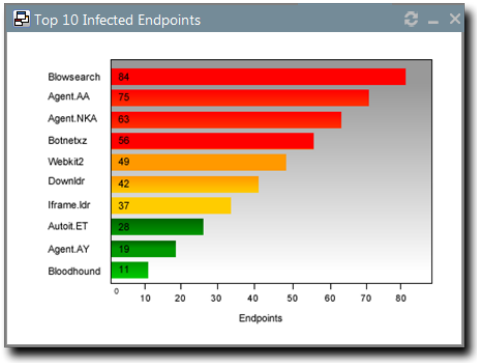


Figure 19: Top 10 Virus/Malware Threats

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

The Estimated Energy Savings: Daily Widget

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

Table 36: Estimated Energy Savings: Daily Widget Fields

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

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

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

Table 37: Estimated Energy Savings: Weekly Widget Fields

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

The Estimated Energy Savings: Monthly Widget

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

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

Table 38: Estimated Energy Savings: Monthly Widget Fields

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

The Device Control Denied Actions Widget

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

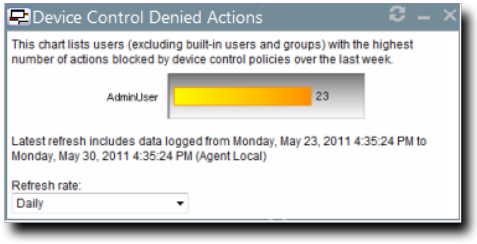


Figure 20: Device Control Denied Actions Widget

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

The Devices Connected to Endpoints Widget

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

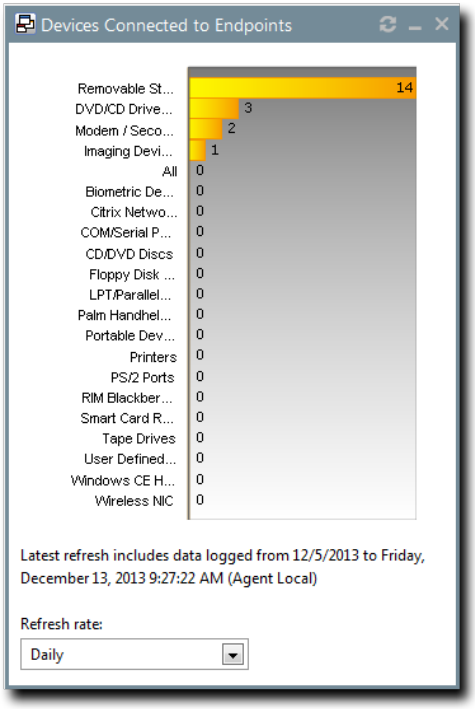


Figure 21: Devices Connected to Endpoints Widget

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

Dashboard Setting and Behavior Icons

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

The following table describes each icon action.

Table 39: Widget Setting and Behavior Icons

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

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

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

Previewing and Printing the Dashboard

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

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

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

Editing the Dashboard

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

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

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

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

   Highly prioritized widgets are more prominently placed.

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

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

The System Alert Pane

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

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

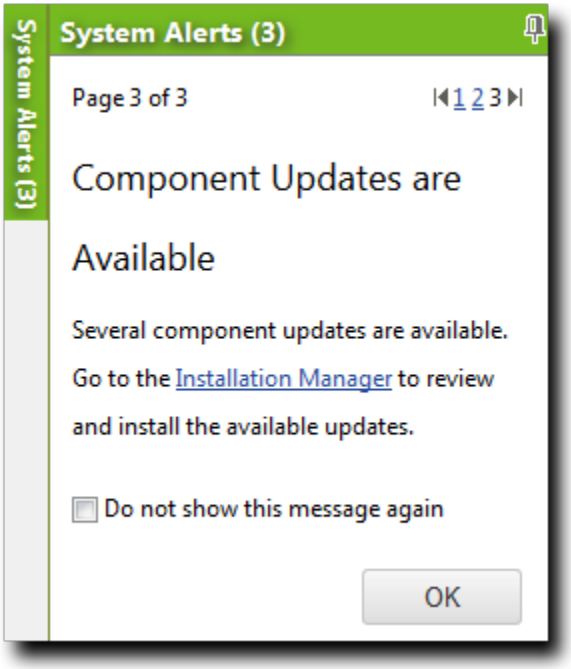


Figure 22: The System Alert Pane

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

Table 40: 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 60.
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 41: License Expiration Scenario and Events

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

Table 42: License Expiration Scenario and Events for Mobile Endpoints

Scenario	Event

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

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

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

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

Chapter 4

Configuring Notifications

In this chapter:

- The Email Notifications Page
- Working with Email Notifications
- APNS Renewal Alerts
- GSS Notifications

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 88.
- 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 99.
- APNS Renewal Alerts. These system alerts inform you of upcoming Apple Push Notification Service certificate expiration, so that you can renew it before communication iOS devices is disabled. For more information, see APNS Renewal Alerts on page 98

The Email Notifications Page

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

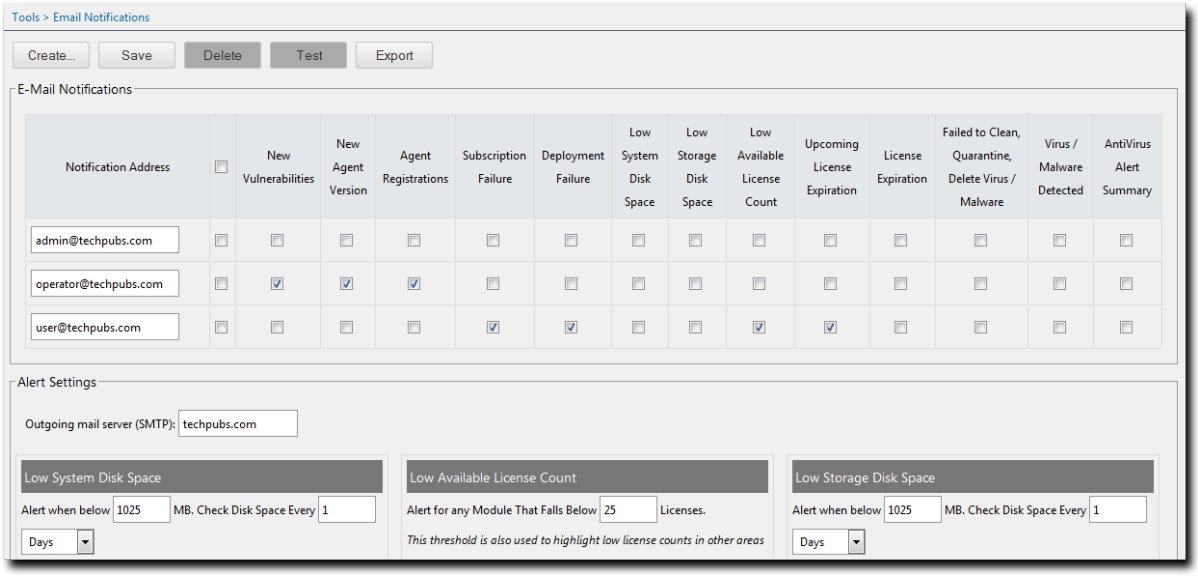


Figure 23: Email Notifications Page

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 43: Email Notification Page Buttons

Button	Function
Create...	Creates a new item to **Email Notifications**. For additional information, refer to Creating Email Notifications on page 96.
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 97.
Test	Sends a test email to selected email addresses. For additional information, refer to Testing Email Notifications on page 97.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 61. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

The Email Notifications Table

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

Installation of the Patch and Remediation modules adds new notifications:

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

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

Installation of the AntiVirus modules adds new notifications:

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

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

Table 44: E-Mail Notification Table

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

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

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

Alert Settings

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

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

Table 45: Alert Settings Options

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

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

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

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

Working with Email Notifications

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

- Configuring Alert Settings on page 94
- Creating Email Notifications on page 96
- Editing Email Notification Addresses on page 96
- Deleting Email Notification Addresses on page 97
- Testing Email Notifications on page 97

Configuring Alert Settings

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10. Click **Save**.

Result: Your alert setting values are saved.

Creating Email Notifications

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

Prerequisites:

Complete Configuring Alert Settings on page 94.

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 61.

Testing Email Notifications

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

Prerequisites:

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

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

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

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

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

3. Click **Test**.

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

APNS Renewal Alerts

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

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

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

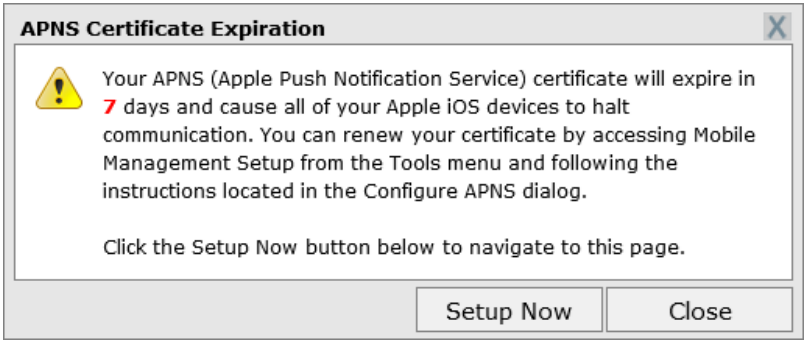


Figure 24: APNS Certificate Expiration Alert

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

Figure 25: Mobile Management Setup Page Alert

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

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

GSS Notifications

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

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

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

Chapter 5

Updating the AntiVirus Module

In this chapter:

- AntiVirus Engine and Definitions
- Updating the AntiVirus Engine and Definitions Manually
- Setting the Polling Frequency for AntiVirus Engine and Definition Updates
- Setting an AntiVirus Content Storage Location
- Delaying the Distribution of AntiVirus Definition File Updates to Endpoints
- Checking the version of the AntiVirus Engine and Definition
- The AntiVirus Tab

During a license period the Ivanti Endpoint Security subscription service ensures the AntiVirus module engine and definitions database are regularly updated in order for the detection and removal of threats to properly occur.

The AntiVirus module engine is the mechanism that scans objects to uncover malicious software, by referencing a definition database containing all known viruses and malware. Updates are retrieved by the Ivanti Endpoint Security server from a storage location, on-demand or according to predefined intervals, then automatically passed to endpoints.

Running a current engine that uses the latest definitions can prevent the outbreak and spread of even the most recently identified threats.

AntiVirus Engine and Definitions

Proactive threat protection is maintained through engine upgrades and definition updates, which are downloaded as file sets directly from the Global Subscription Service (GSS) or a specified storage location.

The detection and removal of threats on endpoints is powered by the AntiVirus module's engine. Periodic upgrades to it provide such enhancements as detection capability improvements, performance optimizations, and memory footprint reductions. The engine detects viruses and malware by comparing files on endpoints against code samples (signatures) of known virus and malware components, called *definitions*. Ivanti updates its definitions database several times daily. There are separate definitions for 32-bit and 64-bit systems.

After retrieving an engine upgrade or definitions update, the server notifies licensed agents immediately: online agents begin downloading immediately, offline agents when they reconnect with the server. The download to agents can be delayed in Agent Policy Sets.

You must have: a valid AntiVirus subscription, offered in durations of one to five years, to enable the Ivanti Endpoint Security server to distribute new content to endpoints.

Important:

- An expired AntiVirus subscription service provides you with no protection against new viruses and malware threats that arise after the date of the last definitions update. Ensure you are aware of your subscription expiration date and renew a minimum of six months beforehand.
- Endpoints hosting agents must have a minimum of 1 GB of free disk space for the creation of temporary files during engine and definitions file updates.

Using a current engine and up-to-date definitions guarantees you the highest level of protection.

Updating the AntiVirus Engine and Definitions Manually

Though AntiVirus automatically updates the engine and definitions according to intervals determined by the Polling Frequency, you can perform an immediate update manually from the ***AntiVirus*** tab in the ***Subscription Service Configuration*** page.

Prerequisites:

- You must have a valid AntiVirus subscription.
- Ensure at least one AntiVirus content storage location is set. See Setting an AntiVirus Content Storage Location on page 104.
- Endpoints hosting agents must have a minimum of 1 GB of free disk space for the creation of temporary files during an update.

1. Select **Tools** > **Subscription Updates**.

   Step Result: The ***Subscription Updates*** page opens.

2. Click the **Configure** button.

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

3. Select the **AntiVirus** tab.

   Step Result: Subscription information and configuration options are displayed.

   Tip: The date and time the system last checked the Global Subscription Service for engine and definition file updates is displayed in the ***AntiVirus communication settings*** section (Last Checked GSS).

4. In the ***AntiVirus engine & definition versions (Server)*** section, click **Download now**.

   Step Result: A dialog appears, prompting you to confirm the action.

5. Click **OK**.

Result: The server checks the Storage Location for a new AntiVirus engine and definitions update. Information about the update attempt will appear on the ***Tools > Subscription Service*** page under the ***Subscription Service History*** section as Type `AntiVirus / Content (32-bit)` and `AntiVirus / Content (64-bit)`.

Immediately after retrieving an update, the server sends a notification about the file's presence and licensed agents begin to download it: online agents at once, offline agents when they reconnect with the server. Distribution to agents will be postponed if they are part of a Group assigned an Agent Policy Set with a Definition Distribution Delay. If a scan is in-progress on an endpoint, the new definitions file will be used immediately to complete the scan. Files in quarantine will be automatically scanned using the new definitions file.

Note: Network bandwidth usage per endpoint can substantially increase during the engine and definition download.

Tip: `DefUpdate.log` on endpoints in `<INSTALL_DIR>\LMAgent\logs\AV` keeps a running record (version number and date/time) of all the definitions files an endpoint installs.

Setting the Polling Frequency for AntiVirus Engine and Definition Updates

You can define the interval at which Ivanti Endpoint Security automatically checks the Global Subscription Service (GSS) for AntiVirus related updates. The default interval is every 1 hour.

Prerequisites:

- You must have a valid AntiVirus subscription.
- Ensure at least one AntiVirus content storage location is set.
- Endpoints hosting agents must have a minimum of 1 GB of free disk space for the creation of temporary files during an update.

The types of polling frequencies available are:

- Every specified number of hours, ranging from a minimum of 0.5 hours to a maximum of 24 hours (restricted to the most optimal polling frequencies). The default interval is 1 hour.
- Daily at a specified time.

Important: Too frequent polling wastes CPU resources through repeated checks for updates that are not yet available. Too infrequent polling can delay the download of important updates and make your environment vulnerable to new viruses or malware.

1. Select **Tools** > **Subscription Updates**.

   Step Result: The ***Subscription Updates*** page opens.

2. Click the **Configure** button.

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

3. Select the **AntiVirus** tab.

   Step Result: Subscription information and configuration options are displayed.

4. In the ***AntiVirus engine & definition download settings (GSS to Server)*** section, set the interval at which the system is to check for updates:

Option	Description
Run Every	Select an interval in hours from the list. Update checks will occur every number of hours specified.
Daily at	Enter a time (server time) or click the **Time View** () icon to select from a list. Update checks will occur once a day at the time specified.

5. Click **Apply**.

   Step Result: A message appears to confirm that the setting you selected is saved.

Result: The polling frequency has been changed, and the interval to the next AntiVirus engine and definitions update check begins.

Tip: `DefUpdate.log` on endpoints in `<INSTALL_DIR>\LMAgent\logs\AV` keeps a running record (version number and date/time) of all the definition files an endpoint installs.

Setting an AntiVirus Content Storage Location

You must specify at least one location (URL with filename and extension) where Ivanti Endpoint Security is to check for and download AntiVirus engine and definition file updates.

Prerequisites:

You must have a valid AntiVirus subscription.

By default the system is configured to check the Ivanti Global Subscription Service (GSS) location http://cache.lumension.com/avcontent.

You can specify a local server in isolated environments with limited or no Internet access.

1. Select **Tools** > **Subscription Updates**.

   Step Result: The ***Subscription Updates*** page opens.

2. Click the **Configure** button.

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

3. Select the **AntiVirus** tab.

   Step Result: Subscription information and configuration options are displayed.

4. Under the ***AntiVirus content storage location*** section, enter a URL with filename in the ***AntiVirus / Content location (URL)*** field.
5. Click **Test Link...** to verify that the URL you entered works correctly.

   Step Result: A dialog opens informing you about the validity of the URL.

6. Click **Add**.

   Step Result: The URL is added to the list.

7. Click **Apply**.

   Step Result: A message appears to confirm that the URL you entered was saved.

Result: The storage location is added to the list and will be checked during the next scheduled or immediate update attempt.

Delaying the Distribution of AntiVirus Definition File Updates to Endpoints

You can control when Ivanti Endpoint Security agents download a new AntiVirus definitions file by setting a time delay interval in an Agent Policy Set.

Prerequisites:

- An Agent Policy Set must exist (use the Global Policy Set to apply the Distribution Delay to all endpoints). See ***Creating an Agent Policy Set*** in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .
- Endpoints you want to delay definitions file distribution to must be part of a Group assigned the Agent Policy Set you edit. See ***Assigning an Agent Policy Set to a Group*** in the Ivanti Endpoint Security User Guide (https://help.ivanti.com/) .

Use a distribution delay to make time to test a new definitions file in a test environment before distributing it to endpoints (for example, to check for false positives that can negatively affect system functionality). In cases where a resultant policy is created through the merging of multiple assigned Agent Policy Sets, the shortest delay is used.

Important: Delaying the distribution of important updates can make your environment vulnerable to new viruses or malware.

The Definitions Distribution Delay option works together with the AntiVirus/Content polling frequency option, which determines how frequently or when the Ivanti Endpoint Security server is to check for definitions updates on the Global Subscription Service. As the Polling Frequency determines when the latest definitions are downloaded to the Ivanti Endpoint Security server, by combining it with the **AntiVirus** Distribution Delay you can postpone sending the latest set of definitions to endpoints up to the Polling Frequency value minus 1 hour.

For example, if the Polling Frequency is set to 4 hours, it means Ivanti Endpoint Security will download a new set of definitions every 4 hours and you have the possibility to delay the distribution of those definitions for 0, 1, 2 or 3 hours.

Note: Ensure that the distribution delay is always set to less than the Polling Frequency. If the delay is set to be equal to or greater than the Polling Frequency, the delay will be reduced to 1 hour less than the Polling Frequency. For example, if the Polling Frequency is 4 hours and the administrator sets the AntiVirus distribution delay to 8 hours, the actual delay applied will be 3 hours

1. 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. Under the ***AV Engine & Definition Distribution Settings*** section in the ***Delay AV definition distribution by*** field, type the time interval (in hours, up to 23 hours) that the Ivanti Endpoint Security Agent is to delay requesting a new AntiVirus definitions file from the Application Server. The default value of `0` disables the option.
4. Click **Save**.

Result: Endpoints assigned the agent policy set will have new updates made available to them for download according to the configured delay interval. For example, if you set a value of 5 hours, an endpoint can download a new AntiVirus definition file 5 hours after it is received by the Application Server.

After Completing This Task:
Now you can:

- Check the version of the AntiVirus definition file on both the server and agents. See Checking the version of the AntiVirus Engine and Definition on page 107.
- Set the Polling Frequency for AntiVirus engine and definition file updates. See Setting the Polling Frequency for AntiVirus Engine and Definition Updates on page 103.
- Manually update the AntiVirus engine and definition files. See Updating the AntiVirus Engine and Definitions Manually on page 102.

Checking the version of the AntiVirus Engine and Definition

To ensure that Real-time, Recurring, and Scan Now scans are providing endpoints with the highest level of protection from malicious software, you must have the latest version of AntiVirus engine and definition on both the server and agents.

Agents download the engine and definitions file, used by the AntiVirus module to accurately detect, identify, and efficiently remove threats on endpoints, from the Ivanti Endpoint Security Server upon receiving notification that a newer version was retrieved from the Global Subscription Service (GSS) or a specified location. There are seperate files for 32-bit and 64-bit systems. The server polls for engine upgrades and definition updates at regular intervals (by default, every 1 hour).

1. To check the version of the AntiVirus engine and definition file on the server:
   a) Select **Tools** > **Subscription Updates**.

      Step Result: The ***Subscription Updates*** page opens.

   b) Click the **Configure** button.

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

   c) Select the **AntiVirus** tab.

      Step Result: The version information is displayed in the ***AntiVirus engine & definition versions (Server)*** section.

2. To check the version of the AntiVirus engine and definition file on an agent:
   a) Select **Manage** > **Endpoints**.

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

b) Select the **AntiVirus** tab.

Step Result: The version is displayed in the ***AV Definition Version*** column (each row refers to a specific endpoint). You can apply the **Last AV Definition Update** filter to only display versions of a particular type (`Current`, `Out of date`, `Error`).

Tip: Generating an AntiVirus Definition Version Status Report enables reviewing the current versions for an entire network or specific endpoints and groups.

After Completing This Task:
If the version of the AntiVirus definitions is older on the endpoint than on the server, marked with a **Warning** icon , you should wait for the agent to download the latest definitions and then run a Scan Now (see Using Scan Now on page 149). If the problem persists, possible issues include:

- Endpoint is offline.
- Agent AntiVirus license has expired.
- Network configuration problems.
- Network outages.

The AntiVirus Tab

Use this tab to configure default AntiVirus settings.

Enable the automatic deletion of files from Quarantine.	Select and enter the quarantine age of files to be automatically deleted. 1 to 60 days from the date a file was quarantined can be entered. Default: 30 days. **Important:** Detected threats that have been quarantined can safely be left in quarantine as they are no longer any danger to endpoints. If you need to free up endpoint storage space, wait at least 30 days before deleting quarantined files to ensure they are not false positives. Removing such files can lead to installed applications or the operating system malfunctioning.

Chapter 6

Working with Antivirus Policies

In this chapter:

- About Antivirus Policies
- Viewing Antivirus Policies
- Creating Antivirus Policies
- Managing Antivirus Policies

Implementing effective antivirus policies is key to protecting the network from malware.

Ivanti AntiVirus provides two policy types to implement such protection:

- Recurring Virus and Malware Scan
- Real-time Monitoring Policy

About Antivirus Policies

Antivirus policies define a set of actions that are carried out automatically to protect the network and its endpoints from viruses and other malware.

In practice, antivirus policies provide the main form of protection to the network because they perform malware scanning automatically and consistently. A good set of antivirus policies can provide comprehensive protection to the network without significantly affecting its performance.

Ivanti AntiVirus provides two types of antivirus policy, the *Recurring Virus and Malware Scan* and the *Real-time Monitoring Policy*. You can create as many of each policy type as you want; the effect of assigning multiple Real-time Monitoring Policies to a group or endpoint is a *resultant policy*.

Ivanti Endpoint Security allows you to organize endpoints and groups in a hierarchical fashion, and antivirus policies can be assigned and inherited accordingly.

Antivirus Policy Types

Two types of complementary antivirus policies can be created to automatically inspect files for malware: *Recurring Virus and Malware Scan* and *Real-time Monitoring Policy*.

Real-time Monitoring Policy	Scans files for malware when read, executed or written by an endpoint (also known as *on-access* or *background* scanning).

Recurring Virus and Malware Scan	Scans all files on an endpoint for malware on a regular, scheduled basis (daily or weekly). Duration is typically long due to the large amount of files targeted, but can be noticeably reduced through various configuration options (for example, the careful exclusion of specific files and folders).

About Recurring Virus and Malware Scan Policies

A recurring virus and malware scan policy runs a scan on selected endpoints or groups at regularly scheduled times.

The frequency of a recurring scan can range from daily to weekly. When configuring a recurring scan, you should make it thorough enough to provide comprehensive protection to the network.

A recurring virus and malware scan policy is defined by the following settings:

Table 46: Recurring Virus and Malware Scan Settings

Setting	Description
Scheduling	Specifies frequency of scan: • Daily • Weekly
Virus detection actions	Specifies the action taken when malware is detected: • Perform no action • Attempt to clean then quarantine (default) • Attempt to clean then delete • Attempt to clean then quarantine then delete
Scan boot sectors	Scans boot sectors in addition to program and data files.
Scan archives	Scans archive files such as `.zip` and `.cab` files. **Note:** Infected .rar files can be quarantined and deleted, but can't be cleaned.
Scan memory	Scans memory in addition to local storage (hard drive).
Logging level	Determines the level of detail that is recorded in log files. *Detailed* includes a results summary, name, time and status for each scanned file, while *Normal* includes only a results summary.
Exclude path/filename	Excludes specified paths or files from the scan.
Optional drives	Scans locally attached storage media such as external hard drives and USB devices.

You create a recurring scan policy with the ***Recurring Virus and Malware Scan Policy Wizard***. The wizard provides detailed configuration options that enable you to specify a high level of protection,

without impacting network performance. See Creating a Recurring Virus and Malware Scan Policy on page 120 for more information on policy settings and how to use this wizard.

About Real-time Monitoring Policies

Real-time monitoring is an ongoing scanning process that monitors file activities on an endpoint. With a real-time monitoring policy you can set the scanning options, determine excluded files or paths, and assign it to endpoints and groups.

A real-time monitoring policy is defined by the following settings:

Table 47: Real-time Monitoring Policy Settings

Setting	Description
Virus detection actions	Specifies the action taken when malware is detected: • Perform no action • Attempt to clean then quarantine (default) • Attempt to clean then delete • Attempt to clean then quarantine then delete
Local user	Applies when the endpoint is being used as a workstation. • Scan on read/execute • Scan on both read/execute and write
Services and remote users	Applies when the endpoint is being used as a server. • Scan on write • Scan on both read/execute and write
Exclude path/filename	Excludes specified paths or files from the scan.
Optional drives	Scans locally attached storage media such as external hard drives and USB devices.

You create a real-time monitoring policy with the ***Real-time Monitoring Policy Wizard***. The wizard provides detailed configurations options that enable you to specify a high level of protection for the endpoint without affecting its performance unduly. See Creating a Real-time Monitoring Policy on page 129 for more information on policy setting and how to use this wizard.

Real-time Monitoring Resultant Policies

If two or more Real-time Monitoring Policies are assigned to an endpoint or group, their settings are combined to create a *resultant policy*.

When combining policies to produce a resultant policy, the system will choose settings that optimize the endpoint's security. Results are described in the *AntiVirus Real-time Monitoring Resultant Policy* section of the ***Information*** tab (endpoints) or ***Information*** view (groups).

Example:

Two Real-time Monitoring Policies with different settings are assigned to an endpoint:

Table 48:

Settings	Real-time Monitoring Policy 1	Real-time Monitoring Policy 2	Resultant Policy
When a virus is detected	Attempt to clean then quarantine	Attempt to clean then quarantine then delete	Attempt to clean then quarantine then delete
Local user	Scan on both read/execute and write	Scan on both read/execute and write	Scan on both read/execute and write
Services and remote users	Scan on write	Scan on write	Scan on write
Activation	Enable - Start policy on Finish (only if assigned to a group/ endpoint)	Enable - Start policy on Finish (only if assigned to a group/ endpoint)	Enable - Start policy on Finish (only if assigned to a group/ endpoint)
Exclude path/ filename	c:\temp\	(none)	c:\temp\
Optional drives	Do not scan locally attached storage media such as external hard drives and USB devices.	Scan locally attached storage media such as external hard drives and USB devices.	Scan locally attached storage media such as external hard drives and USB devices.

Assigned and Inherited Policies

Antivirus policies may be assigned to a group or an endpoint, or inherited from a group.

In Ivanti AntiVirus a group may contain endpoints or other groups. There is a parent-child relationship between a group and what it contains. When an antivirus policy is assigned to a group, it is *inherited* by that group's children, whether they are endpoints or other groups.

You can view an endpoint's antivirus policies on the ***Antivirus Policies*** tab of the ***Details*** page. Assigned policies can be selected and their **Source** property is set to "Assigned". Inherited policies are grayed-out (not selectable) and their **Source** property is set to **Inherited**.

Similarly, a group's antivirus policies are displayed on the **Antivirus Policies** view of the ***Groups*** page. Assigned policies can be selected and their **Source** property is set to **Assigned**. Inherited policies are grayed-out (not selectable) and their **Source** property is set to **Inherited**.

Archive Types Supported for Scanning

Ivanti AntiVirus can scan the contents of many archive types when the Scan Archives option is set during scan confiiguration.

- 7-ZIP
- ACE
- ALZ
- ARJ
- debug scripts
- BZIP2
- CAB
- CHM files
- cpio
- Doc files
- SIS
- gzip
- IMP
- INNO installer
- Instyler
- ISO disk images
- LHA
- MSO
- NSIS installer
- objects
- Windows/MAC OS X process scanner
- Batch file compiler
- RAR
- Windows Registry
- rpm
- SFX installers
- SWF flash
- Tar
- TeleDisk image
- TNEF
- Universal Image Format
- UUDecoder
- VISE installer
- WISE installer
- IE cookies extractor
- InstallShield
- ZIP
- Z

Viewing Antivirus Policies

You can view all antivirus policies on the ***Antivirus Policies*** page. You can view the antivirus policies assigned to individual endpoints on their ***Details*** pages, and those assigned to groups on their ***Groups*** pages.

The ***Antivirus Policies*** page displays all existing antivirus policies. It has a list format that displays basic policy information such as name, type, assignment details, and status. You can see more detailed information on the policy by expanding it.

If you go to a ***Groups*** page or the ***Details*** page of an endpoint, you can see the antivirus policies that have been assigned to it. An endpoint or group can have more than one policy assigned to it. For example, policies could be assigned to both an endpoint and to a group of which it is a member.

When two or more Real-time Monitoring Policies are assigned to an endpoint, they are combined in such a way as to produce a *resultant policy*, a combination of policy details that optimizes the endpoint's security.

The Central Antivirus Policies View

The ***Antivirus Policies*** page provides a centralized view of current antivirus policies.

On this page you can view the list of antivirus policies and examine their details. You can also create new policies, and manage antivirus policies across the network.

Viewing the Antivirus Policies Page

You can view and manage antivirus policies centrally on the ***Antivirus Policies*** page.

Select **Manage** > **Antivirus Policies**.

Step Result: The ***Antivirus Policies*** page opens.

Result: Now you can view all the Real-time Monitoring and Recurring Virus and Malware Scan policies configured in the system. Refine the list by using the filters provided or expand a row to see detailed policy information.

The Antivirus Policies Page

The ***Antivirus Policies*** page enables you to create, edit, and manage antivirus policies.

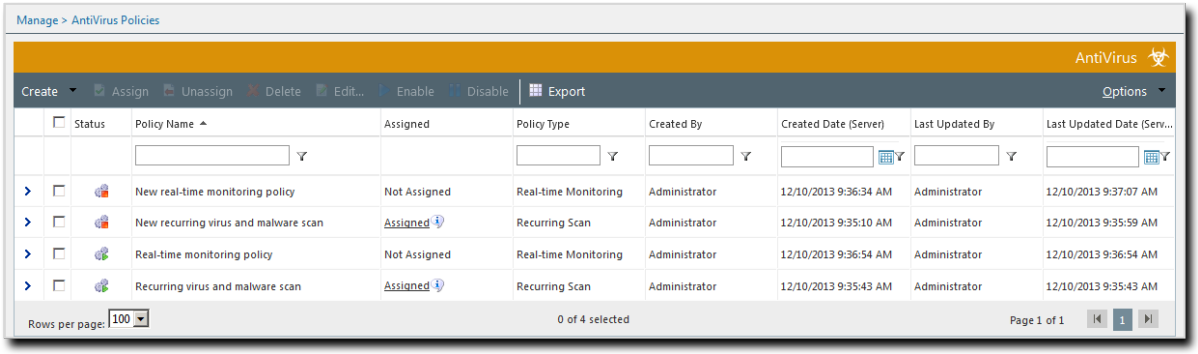


Figure 26: Antivirus Policies Page

The ***Antivirus Policies*** page has:

- A toolbar for creating and managing antivirus policies
- A list displaying the existing antivirus policies

The Antivirus Policies Page Toolbar

The ***Antivirus Policies*** page toolbar enables you to create, edit, and manage antivirus policies.

Table 49: Antivirus Policies Toolbar Buttons

Button	Function
Create	Enables you to create a *Recurring Virus and Malware Scan* policy (see Creating a Recurring Virus and Malware Scan Policy on page 120) or a *Real-time Monitoring Policy* (see Creating a Real-time Monitoring Policy on page 129).
Assign	Assigns the selected policy to one or more endpoints or groups.
Unassign	Unassigns the selected policy from one or more endpoints or groups.
Delete	Deletes the selected policy.
Edit	Opens a wizard to edit the selected policy.
Enable	Enables the selected policy.
Disable	Disables the selected policy.
Export	Exports the selected policy to a comma separated value (`.csv`) file. See Exporting Data on page 61 for more information.

Button	Function
Options	Features options to set page views, filter data, and enable clipboard copy. See The Options Menu on page 53 for more information.

Note: All toolbar buttons except **Create** and **Options** are disabled until at least one policy is selected.

For more information on creating and managing antivirus policies, see the following:

- Creating Antivirus Policies on page 120.
- Managing Antivirus Policies on page 140.

The Antivirus Policies Page List

The ***Antivirus Policies*** page list provides information on existing antivirus policies. Selecting a policy enables it to be edited and managed.

Table 50: Antivirus Policies List Columns

Column	Description
Status	An icon representing whether the policy is enabled or disabled.
Policy Name	The name given by the policy creator.
Assigned	Defines whether the policy is assigned to at least one endpoint or group. If a policy is assigned: • The **Assigned** hyperlink opens the wizard that created the policy at the ***Assignments*** page. • The **Information** icon lists the groups or endpoints the policy is assigned to.
Policy Type	• Recurring Virus and Malware Scan • Real-time Monitoring Policy
Created By	The creator of the policy.
Created Date (Server)	The date the policy was created in server time.
Last Updated By	The last user to update the policy.
Last Updated Date (Server)	The date and time the policy was last updated in server time.

Viewing Policy Details

On the ***Antivirus Policies*** page, you can expand a policy entry to view the policy details.

1. Select **Manage** > **Antivirus Policies**.

   Step Result: The ***Antivirus Policies*** page opens, displaying a list of existing policies.

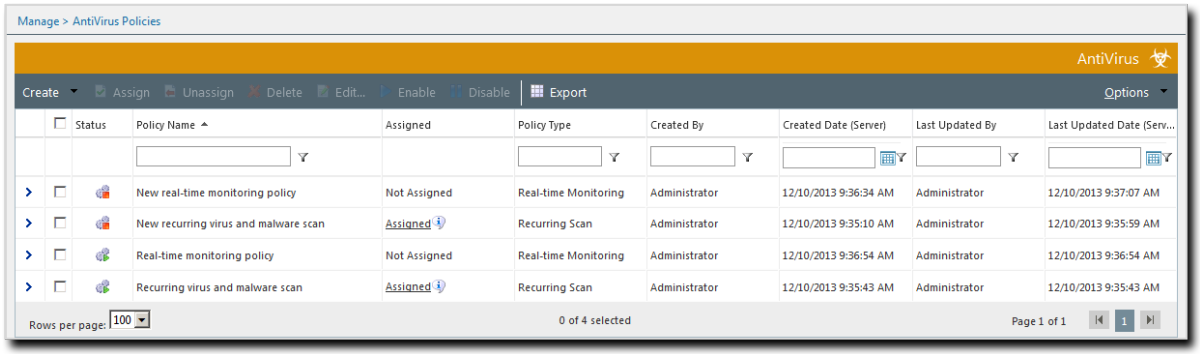


Figure 27: Antivirus Policies Page

2. To view the details of a policy, click the arrow at the side of the that policy's entry.

   Step Result: The policy expands, listing the name, value, and description of each of its components.

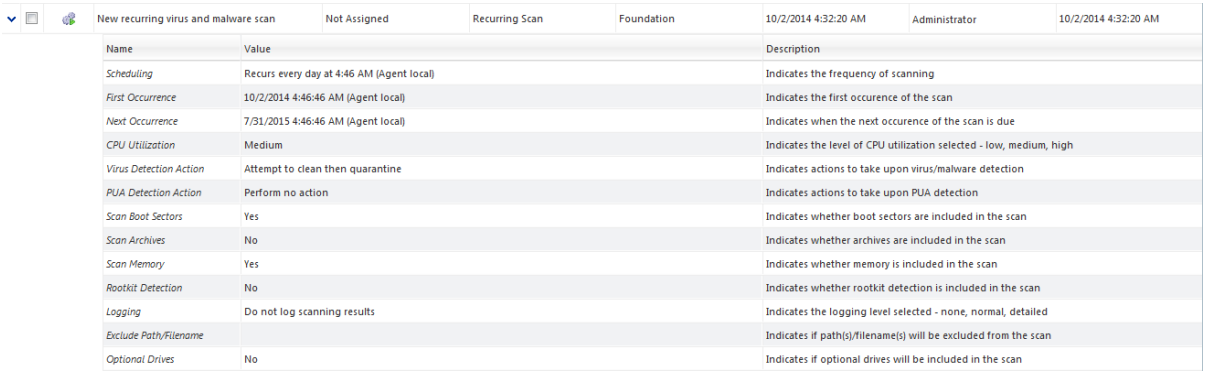


Figure 28: Policy Details

3. When you have finished viewing the policy details, click the arrow again to collapse the detailed listing.

Tip: You can have more than one policy expanded at the same time. This is useful for comparing the details of two policies.

Antivirus Policies on Endpoints

You can view and manage the antivirus policies for a specific endpoint on its ***Details*** page.

This page has two tabs that relate to antivirus policies:

Information **tab**	Displays details of the antivirus policies and the resultant Real-time Monitoring policies that apply to the endpoint.

***Antivirus Policies* tab**	Lists the antivirus policies that apply to the endpoint, and enables you to manage them.

Viewing Endpoint Antivirus Policies
You can view the antivirus policies assigned to and inherited by an endpoint on the ***Antivirus Policies*** tab of its ***Details*** page.

1. Select **Manage** > **Endpoints**.
2. Select an endpoint by clicking on its link.

   Step Result: The endpoint's ***Details*** page opens.
3. Select the ***Antivirus Policies*** tab.

Result: Now you can view all the Real-time Monitoring and Recurring Virus and Malware Scan policies assigned to and inherited by the endpoint. Refine the list by using the filters provided or expand a row to see detailed policy information.

Tip: The name, type, and source of each endpoint antivirus policy is also available in the **Antivirus Policies** section on the Information tab.

After Completing This Task:
View the resultant policies created through the merger of Real-time Monitoring Policy sets in the ***AntiVirus Real-time Monitoring Resultant Policy*** section of the ***Information*** tab.

Antivirus Policies on Groups

You can view and manage the antivirus policies for a specific group on the ***Groups*** page.

The ***Groups*** page has two views that relate to antivirus policies:

- The **Information** view displays details of the antivirus policies and the resultant Real-Time Monitoring policies that apply to the group.
- The **Antivirus Policies** view lists the antivirus policies that apply to the group, and enables you to manage these policies and create new ones.

Viewing Group Antivirus Policies
You can view the antivirus policies assigned to and inherited by a group on the Antivirus Policies view of the ***Groups*** page.

1. Select **Manage** > **Groups**.
2. From the **Browser**, select a group.

3. Select the **Antivirus Policies** view.

Result: Now you can view all the Real-time Monitoring and Recurring Virus and Malware Scan policies assigned to and inherited by the group. Refine the list by using the filters provided or expand a row to see detailed policy information.

> **Tip:** The name, type, and source of each group antivirus policy is also available in the **Antivirus Policies** section on the Information view.

After Completing This Task:
View the resultant policies created through the merger of Real-time Monitoring Policy sets in the ***AntiVirus Real-time Monitoring Resultant Policy*** section of the ***Information*** tab.

Creating Antivirus Policies

Ivanti AntiVirus provides two wizards for creating antivirus policies, the ***Recurring Virus and Malware Scan Wizard*** and the ***Real-time Monitoring Policy Wizard***.

You can launch either of these wizards using the **Create** control on the following pages:

- The ***Antivirus Policies*** page.
- The ***Antivirus Policies*** tab of an endpoint's ***Details*** page.
- The **Antivirus Policies** view of a group's page.

The process of using each wizard follows a general pattern:

1. Name the policy
2. Configure basic scanning options
3. Configure additional scanning options
4. Configure exclusions or inclusions
5. Assign to endpoints or groups

Only the first two steps are required to create a basic antivirus policy. After it has been created you can edit the policy to configure additional options and exclusions/inclusions, and assign it to endpoints or groups.

Creating a Recurring Virus and Malware Scan Policy

The ***Recurring Virus and Malware Scan Policy Wizard*** enables you to schedule a recurring scan, set scanning options, and build a list of target endpoints.

A recurring scan runs on a regular, scheduled basis. It typically scans all the files on an endpoint (apart from those that are specifically excluded from the scan). A recurring scan can take an appreciable amount of time to run if there are a large number of files to be scanned.

1. Select **Manage** > **Antivirus Policies**.

   Step Result: The ***Antivirus Policies*** page opens.

2. From the ***Manage*** > ***AntiVirus Policies*** toolbar, select **Create** > **Recurring Virus and Malware Scan**.

   Step Result: The ***Recurring Virus and Malware Scan Policy Wizard*** opens at the ***Name and Schedule Policy*** page.

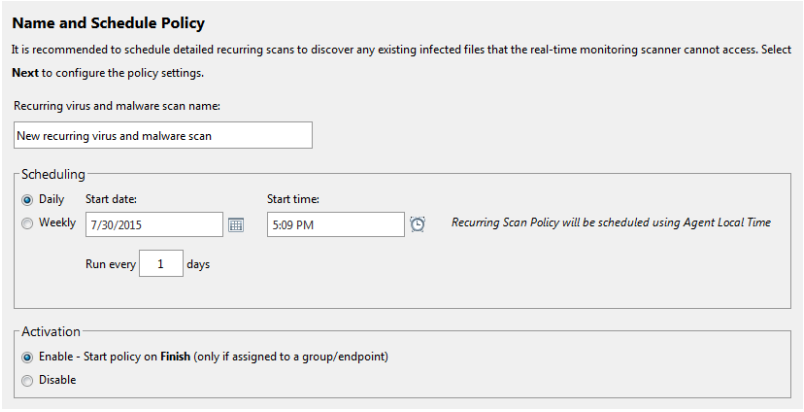


Figure 29: Recurring Virus and Malware Scan Policy Wizard

3. Type a new name in the **Recurring virus and malware scan name** field. Make the name descriptive, conveying the role of this recurring policy.

Note: The name must be unique, otherwise a warning will be displayed.

4. Select and configure a **Scheduling** option:

Important: If an endpoint's internal clock changes (for example, due to Daylight Savings Time or time-zone differences while travelling) a recurring scan scheduled to take place during the time skipped will not occur.

Ensure you or the endpoint user run a Scan Now immediately after a time change to maintain continuous protection.

Method	Steps
Daily	1. Select the **Daily** option. 2. Type the start date in the **Start date** field. You can also select the start date by clicking the **Calender** icon. 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon. 4. Type a value in the **Run every x days** field.

Method	Steps
Weekly	1. Select the **Weekly** option. 2. Type the start date in the **Start date** field. You can also select the start date by clicking the **Calender** icon. 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon. 4. Type a value in the **Run every x weeks on:** field. **Note:** Leave the value at 1 if you want the scan to run at least once a week. 5. Select one or more of the daily check boxes to run the scan on those days.

5. Select an **Activation** option.

Setting	Result
Enable - Start policy on Finish (only if assigned to a group/endpoint)	The policy is created and activated when you click **Finish** and the wizard closes. **Note:** The policy must be assigned to at least one endpoint or group.
Disable	The policy is created but not activated when you click **Finish** and the wizard closes. You may activate it at a later time.

6. Click **Next** to set the scanning options.

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

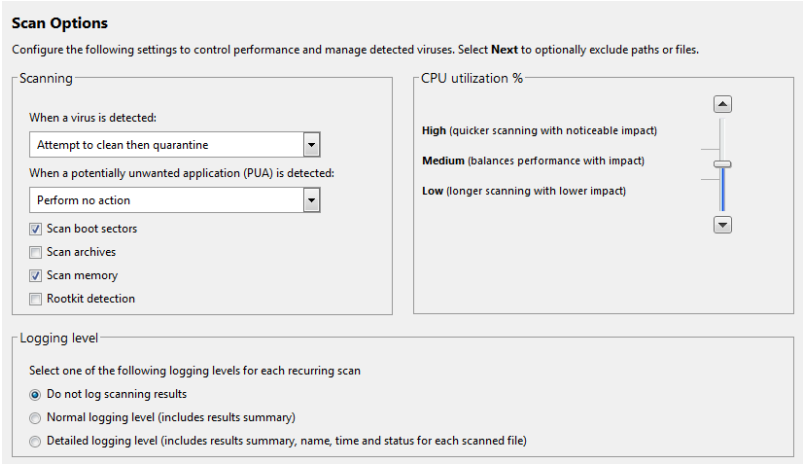


Figure 30: Recurring Virus and Malware Scan Wizard - Scan Options

> **Note:** If you click **Finish** at this point, a basic policy is created, but is not assigned to any endpoints. You can configure the policy further and assign it to endpoints later.

7. From the drop-down list, select the action that occurs when a virus is detected.

Setting	Result
Perform no action	Does nothing with the infected file, but sends an alert to the server.
Attempt to clean then quarantine	Attempts to clean the infected file. If this is not possible, the file is quarantined. An alert is sent to the server. **Note:** This option is the default selection.
Attempt to clean then delete	Attempts to clean the infected file. If this is not possible, the file is deleted. An alert is sent to the server.

Setting	Result
Attempt to clean then quarantine then delete	Attempts to clean the infected file. If this is not possible, the file is quarantined. If it is not possible to quarantine it, it is deleted. An alert is sent to the server.

Note:

- To *clean* an infected file means to completely remove the malicious code so that the file is safe to use. It is not always possible to remove the malicious code, however. When this happens, you can either delete the file or *quarantine* it. To quarantine means to move it to a safe place on the endpoint where it can be kept for further examination.

  In certain cases (such as when the malware is a Trojan) the entire file is malicious. Such a file cannot be cleaned, so the only options are to quarantine or delete it.
- Virus detection actions are not used for memory scans.

8. From the drop-down list, select the action to be taken when a potentially unwanted application (PUA) is detected:

Setting	Result
Perform no action	The system ignores the potentially unwanted application. **Note:** This option is the default selection.
Send alert only	An alert is sent to the server only.
Alert and action (treat as malware)	An alert is sent to the server and the file is cleaned, quarantined, or deleted, according to the action you selected in the **When a virus is detected** drop down.

9. Set the **Scanning** options:

Setting	Result
Scan boot sectors	The virus scan will be more thorough if you scan boot sectors in addition to program and data files. **Note:** If malware is detected in a boot sector, the action taken depends on the virus detection option selected: • **Perform no action** - the boot sector is left as it is and an alert is sent to the ***Virus and Malware Event Alerts*** page. • **Clean/Delete/Quarantine** - the boot sector is automatically repaired.

Setting	Result
Scan archives	The virus scan will be more thorough if you scan archive files such as `.zip` and `.cab` files. **Note:** • Scanning archives will result in longer scan durations. • Infected .rar files can be quarantined and deleted, but can't be cleaned. See Archive Types Supported for Scanning on page 114
Scan memory	Viruses and other malware can reside in memory as well as on the disk(s). The virus scan will be more thorough if you scan memory for such viruses and malware. **Note:** Virus detection actions and exclusions are not applied to memory scans.
Rootkit detection	A rootkit, similar to a hack tool, enables attackers to gain administrator access to a system. They hide the attacker's presence and give them full control of a server or client endpoint without being noticed. **Note:** Rootkit detection is only supported on endpoints running Windows versions from Vista onwards.

10. Set the ***CPU utilization %*** threshold to control the level of impact the scan is to have on endpoint performance:

Setting	Result
High	Quicker scanning but may noticeably impact endpoint performance.
Medium	Balances scan speed with endpoint performance impact (default option).
Low	Slower scanning but has the lowest impact on endpoint performance.

11. Set the logging options:

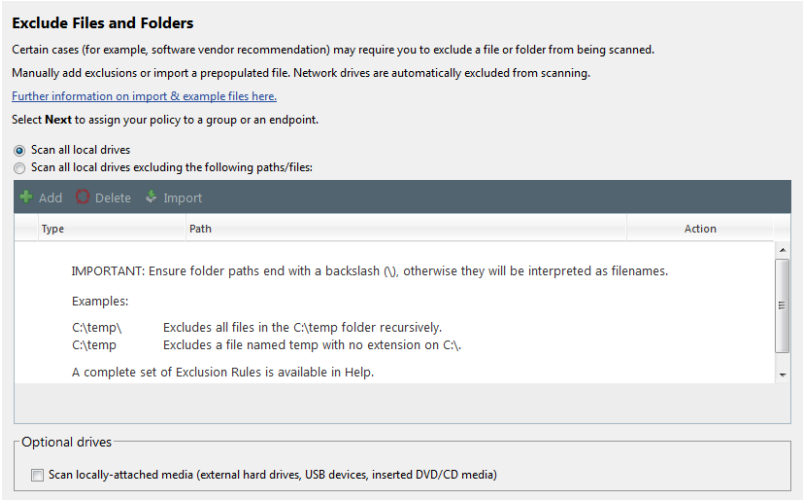
Note: As logging information is kept on the endpoint, the option you choose will not affect the loggings sent to the server.

Setting	Result
Do not log scanning results	No scan log is generated.
Normal logging level (includes results summary)	A standard scan log is generated.
Detailed logging level (includes results summary, name, time and status for each scanned file)	A detailed scan log is generated. **Caution:** Logging detailed virus scan results typically generates large amounts of data, especially when recurring scans run frequently.

12. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created, but not assigned to any endpoints. You can assign it to endpoints at a later time.

Step Result: The ***Exclude Files and Folders*** page opens.



This page enables you to exclude specified files and paths from the scan. You may want to do this because:

- You have some applications whose manufacturers recommend be excluded from virus scans.
- You have folders containing large amounts of data that you consider relatively safe, such as graphics files. Excluding them from the scan saves time.
- You have files that cause known "false positives" during a scan.

Caution: Excluding files or paths from the scan always involves some degree of risk.

13. Exclude files and folders, using one of the following methods:

Tip: Masks and system variables can be used in exclusions. See Exclusion Rules on page 138.

Note: More information on excluding files and folders from Ivanti AntiVirus malware scans, including recommended exclusions, can be found in Ivanti Community Article 58945.

Method	Steps
Manually exclude specific files and folders from the scan.	1. Click **Add**. A blank entry is added to the exclusions list. 2. Select an exclusion type from the **Type** field. The types are File and Folder. 3. Enter the path to the item you want to exclude in the **Path** field. 4. Click  to add the exclusion to the list. Repeat this procedure for all files and folders you want to exclude from the scan. **Note:** Click **Remove** () to remove items from the exclusion list.
Import an XML file containing a formatted list of file and folder exclusions.	See Importing File, Folder and Process Exclusions on page 136.

14. Configure the **Optional drives** settings:

Setting	Result
Scan locally-attached media	All storage media (including external hard drives, USB devices, and DVD/CD media) are included in the scan.

15. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created, but not assigned to any endpoints. You can assign it to endpoints at a later time.

Step Result: The **Assign virus and malware scan policy to groups and/or endpoints** page opens.

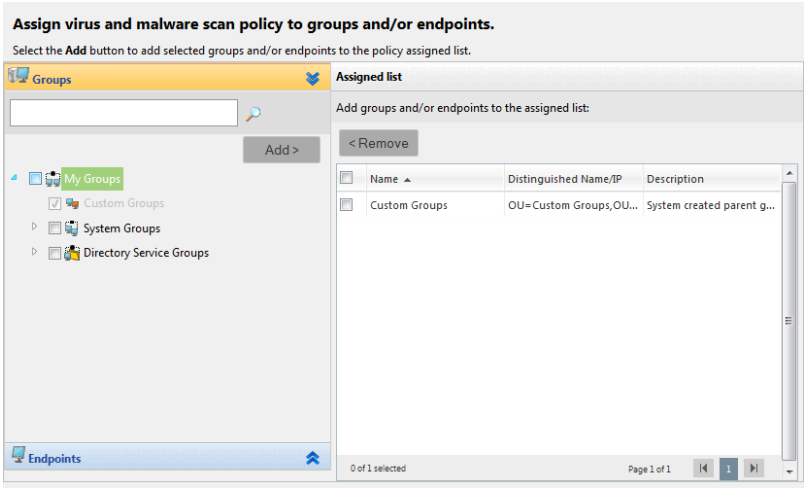


Figure 31: Assign Policy to Groups or Endpoints

16. Build a list of targets (endpoints), using either or both of the following methods:

Important: Recurring scans will not run on an endpoint that is shutdown or hibernating at the scheduled scan time.

Method	Steps
To define targets using groups:	1. If the **Groups** section is not open, click its up arrow to open it. 2. Select one or more endpoint groups by selecting their check boxes. 3. Click **Add**. This adds the group(s) to the **Assigned** list.

Method	Steps
To define targets using endpoints:	**1.** If the **Endpoints** section is not open, click its up arrow to open it. **2.** In the search field, do one of the following: • Type an endpoint name (to search for a specific endpoint) • Type part of an endpoint name (to search for similarly named endpoints) • Leave it blank (to search for all available endpoints) **3.** Click the **Search** icon. Depending on what you typed, one or more endpoints will appear in the **Name** column, with their respective IP addresses. **4.** Select the check box for each endpoint you want to assign. **5.** Click **Add**. This adds the endpoint(s) to the **Assigned** list.

Note: You can remove targets from the **Assigned** list by selecting the applicable check boxes and clicking **Remove**.

17. Click **Finish**.

Step Result: The ***Virus and Malware Scan Policy Wizard*** closes. The newly created policy is displayed in the ***Antivirus Policies*** page.

Result: You have created a recurring Recurring Virus and Malware Scan Policy.

Creating a Real-time Monitoring Policy

The ***Real-time Monitoring Policy Wizard*** enables you to set real-time scanning options, include or exclude files or paths, and build a list of target endpoints.

A Real-time scan runs when an endpoint accesses a file to perform an action, such as a read or write. This scan type runs continuously in the background to catch malware before it can infect systems.

1. Select **Manage** > **Antivirus Policies**.

Step Result: The ***Antivirus Policies*** page opens.

2. Click **Create** > **Real-time Monitoring Policy**.

   Step Result: The ***Real-time Monitoring Policy Wizard*** opens.

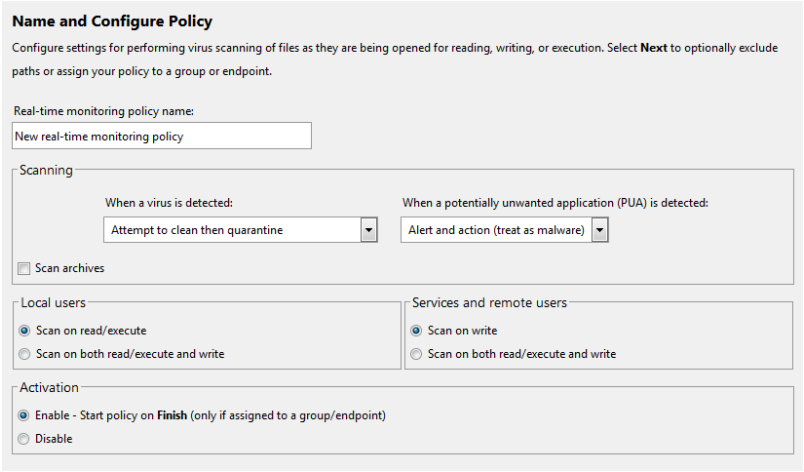


Figure 32: Real-time Monitoring Policy Wizard

3. Type a new name in the **Real-time monitoring policy name** field. Make the name descriptive, conveying the role of this real-time monitoring policy.

   Note: The name must be unique. If it is not, a warning will be displayed.

4. From the drop-down list, select the action that occurs when a virus is detected.

Setting	Result
Perform no action	Does nothing with the infected file, but sends an alert to the server.
Attempt to clean then quarantine	Attempts to clean the infected file. If this is not possible, the file is quarantined. An alert is sent to the server. **Note:** This option is the default selection.
Attempt to clean then delete	Attempts to clean the infected file. If this is not possible, the file is deleted. An alert is sent to the server.

Setting	Result
Attempt to clean then quarantine then delete	Attempts to clean the infected file. If this is not possible, the file is quarantined. If it is not possible to quarantine it, it is deleted. An alert is sent to the server.

Note:

- To *clean* an infected file means to completely remove the malicious code so that the file is safe to use. It is not always possible to remove the malicious code, however. When this happens, you can either delete the file or *quarantine* it. To quarantine means to move it to a safe place on the endpoint where it can be kept for further examination.

  In certain cases (such as when the malware is a Trojan) the entire file is malicious. Such a file cannot be cleaned, so the only options are to quarantine or delete it.
- Virus detection actions are not used for memory scans.

5. From the drop-down list, select the action to be taken when a potentially unwanted application (PUA) is detected:

Setting	Result
Perform no action	The system ignores the potentially unwanted application. **Note:** This option is the default selection.
Send alert only	An alert is sent to the server only.
Alert and action (treat as malware)	An alert is sent to the server and the file is cleaned, quarantined, or deleted, according to the action you selected in the **When a virus is detected** drop down.

6. [Optional] Select the **Scan archives** check box to scan compressed files like: .zip, .rar, and .cab

Note:

- Scanning the contents of archive files will impact endpoint performance.
- Infected .rar files can be quarantined or deleted, but can't be cleaned.

See Archive Types Supported for Scanning on page 114

7. Configure the **Local users** setting. This applies when the endpoint is being used as a workstation, with a logged-on user.

Setting	Result
Scan on read/execute	Scans files before they are used.

Setting	Result
Scan on both read/execute and write	Scans files that are opened for write. New or changed files are scanned on close.

Note: With **Scan on read/execute** selected, it is possible that an infected file can be downloaded from the Internet and saved to disk. With **Scan on both read/execute and write** selected, the scanner will detect and (if possible) remove the malware before writing the file to disk.

8. Configure the **Services and remote users** setting. This applies when the endpoint is being used as a server. If someone physically logs on to the server, the **Local users** setting applies.

Setting	Result
Scan on write	Scans files that are saved to disk.
Scan on both read/execute and write	Scans files that are being read or executed, as well as those being saved to disk. **Note:** This is not the default option, as it increases scanning time. But if the server becomes infected, this is the option to select.

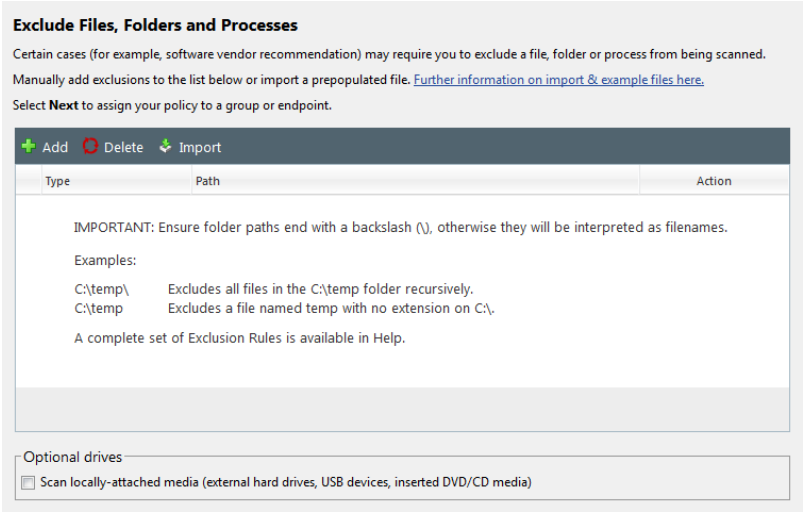
9. Select an **Activation** option.

Setting	Result
Enable - Start policy on Finish (only if assigned to a group/endpoint)	The policy is created and activated when you click **Finish** and the wizard closes. **Note:** The policy must be assigned to at least one endpoint or group.
Disable	The policy is created but not activated when you click **Finish** and the wizard closes. You may activate it at a later time.

10. Click **Next**.

Note: If you click **Finish** at this point, a basic policy is created, but is not assigned to any endpoints. You can configure the policy further and assign it to endpoints later.

Step Result: The ***Exclude Files, Folders and Processes*** page opens.



This page enables you to exclude specified files and paths from the scan. You may want to do this because:

- You have some applications whose manufacturers recommend be excluded from virus scans.
- You have folders containing large amounts of data that you consider relatively safe, such as graphics files. Excluding them from the scan saves time.
- You have files that cause known "false positives" during a scan.

Caution: Excluding files or paths from the scan always involves some degree of risk.

11. Exclude files, folders or processes, using one of the following methods:

Tip: Masks and system variables can be used in exclusions. See Exclusion Rules on page 138.

Note: More information on excluding files and folders from Ivanti AntiVirus malware scans, including recommended exclusions, can be found in Ivanti Community Article 58945.

Method	Steps
Manually exclude specific files, folders and processes.	1. Click **Add**. A blank entry is added to the exclusions list. 2. Select an exclusion type from the **Type** field. File, Folder, or Process. 3. Enter the path to the item you want to exclude in the **Path** field. 4. Click  to add the exclusion to the list. Repeat this procedure for all files, folders and processes you want to exclude from the scan. **Note:** Click **Remove** () to remove items from the exclusion list.
Import an XML file containing a formatted list of file, folder and and process exclusions.	See Importing File, Folder and Process Exclusions on page 136.

12. Configure the **Optional drives** settings:

Setting	Result
Scan locally-attached media	All storage media (including external hard drives, USB devices, and DVD/CD media) are included in the scan.

13. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created, but not assigned to any endpoints. You can assign it to endpoints at a later time.

Step Result: The ***Assign real-time monitoring policy to groups and/or endpoints*** page opens.

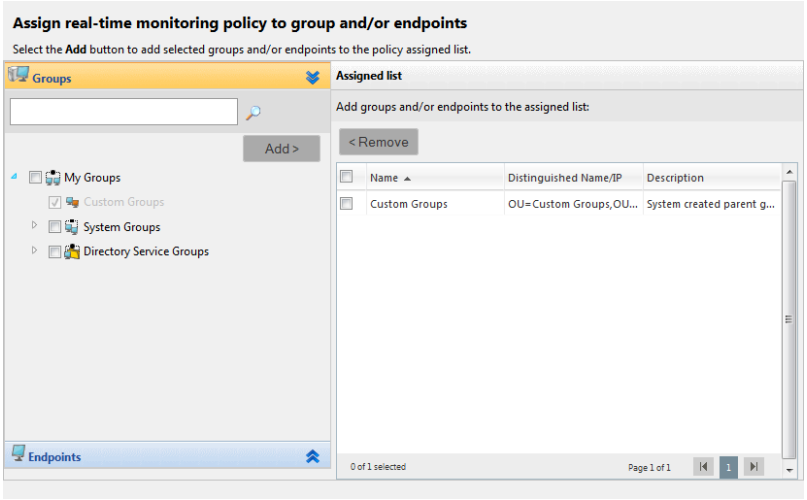


Figure 33: Assign Real-time Monitoring Policy Page

14. Build a list of targets (endpoints), using either or both of the following methods:

Important: Recurring scans will not run on an endpoint that is shutdown or hibernating at the scheduled scan time.

Method	Steps
To define targets using groups:	1. If the **Groups** section is not open, click its up arrow to open it. 2. Select one or more endpoint groups by selecting their check boxes. 3. Click **Add**. This adds the group(s) to the **Assigned** list.

Method	Steps
To define targets using endpoints:	**1.** If the **Endpoints** section is not open, click its up arrow to open it. **2.** In the search field, do one of the following: • Type an endpoint name (to search for a specific endpoint) • Type part of an endpoint name (to search for similarly named endpoints) • Leave it blank (to search for all available endpoints) **3.** Click the **Search** icon. Depending on what you typed, one or more endpoints will appear in the **Name** column, with their respective IP addresses. **4.** Select the check box for each endpoint you want to assign. **5.** Click **Add**. This adds the endpoint(s) to the **Assigned** list.

Note: You can remove targets from the **Assigned** list by selecting the applicable check boxes and clicking **Remove**.

15. Click **Finish**.

Step Result: The ***Real-time Monitoring Policy Wizard*** closes. The newly created policy is displayed in the ***Antivirus Policies*** page.

Importing File, Folder and Process Exclusions

You can facilitate the exclusion of a large number of files, folders, and processes (Real-time Monitoring Policy only) from an antivirus scan through the import of a formatted XML file.

Prerequisites:

- You must be in the process of configuring a *Real-time Monitoring Policy*, *Recurring Virus and Malware Scan Policy* or *Scan Now*.
- You must have created an import XML file. See `<install_dir>/AntiVirus/Controls/Components/ExcludeFileImport/NonDomainExcludes.xml` for an example.

Scan performance can be improved and false positives prevented by skipping certain files and paths during scans. The **Exclude Files and Paths** page on the policy and Scan Now wizards enables you to exclude specific files and paths, according to the exclusion rules that apply.

Note: Recommended file and folder excludes are listed in Ivanti Community Article 58945.

As an alternative to manually entering exclusions, you can import an XML file containing a list in a specific format:

```
<?xml version="1.0"?>
                <excludes>
                <exclude path=""/>
                <pexclude path=""/>
                </excludes>
```

Where:

<exclude path=""/>	File and folder exclusion paths.
<pexclude path=""/>	Process exclusion paths (Real-time Monitoring Policies only)

Tip: Scan durations can be reduced by avoiding exclusions for software not installed on endpoints.

Keep the exclusion file up to date, especially if you install new software in your environment.

Caution: Do not exclude files or folders unless their contents are known to be threat-free.

Note: Exclusions are not applied to memory scans (when the **Scan Memory** option is selected during scan configuration).

1. From the ***Exclude Files or Paths*** wizard page, click the **Import** button.

   Step Result: The Import Exclusion list from File dialog opens.

2. Click **Browse**, select the file, and click **OK**.

   Step Result: The XML file imports and you will be made aware of any file and path duplicates detected.

Result: You have added a list of exclusions to an antivirus policy or Scan Now configuration.

After Completing This Task:
Continue configuring a *Real-time Monitoring Policy*, *Recurring Virus and Malware Scan Policy* or *Scan Now*.

Exclusion Rules

Use wildcards (masks) and system variables to precisely choose files and paths to exclude from antivirus policies and a Scan Now.

Caution: Do not exclude files or folders unless their contents are known to be threat-free.

Important: Wildcard character * is not accepted in filenames (`test00*.log`) but can be used for:

- Drives (`*\temp`)
- Paths (`c:\temp\*\`) but only once in a single exclusion

Drive and path wildcards can also be used together in a single exclusion (`*\temp\*\test\`).

DOS 8.3 short names (`ALONGF~1.TXT`) are not accepted.

Note: Exclusions are not applied to memory scans (when the **Scan Memory** option is selected during scan configuration).

Files without paths

***.exe**	All files with extension EXE.
file.*	All files named `file` with any extension.
file	All files named `file` with no extension.
file.exe	All `text.exe` files.

Absolute file paths

Note: Folder paths must end with a path separator (\).

c:\temp	All files in the `c:\temp` folder recursively.
***\temp**	All files in the `temp` folder on all drives recursively.
c:\temp*.* or c:\temp*	All files in the `c:\temp` folder but not recursively.
c:\temp	The file named `temp` with no extension on `c:\`.
c:\temp\test	The file named `test` in the `c:\temp` folder.
c:\temp*.exe	All files with the extension EXE in the `c:\temp` folder.
c:\temp\test.doc	The `test.doc` file in the `c:\temp` folder.

Environment variable directories

%WINDIR%\ or %WINDIR%/ or %WINDIR%	All files in the Windows folder recursively.

%WINDIR%*	All files in the Windows folder but not recursively.
%WINDIR%*\temp	All files in a subfolder named `temp` recursively within any folder in the Windows folder.

Note: System account environment variables with multiple values are not supported. For example: `%path%`

Wildcard Usage

Exclusions can contain the "*" single asterisk wildcard (mask) character in specific combinations, with a maximum of two per exclusion.

Caution: Improper wildcard usage can exclude incorrect files and directories.

Full directory

Restriction:

- Cannot be used with a file exclusion (`c:\directory1\*\file.exe` is invalid)
- Cannot be used in an exclusion that uses a filename wildcard (`*\directory1\*.exe` and `c:\directory1\*\*.exe` are invalid)
- Use of multiple directory wildcards in a single exclusion is not permitted (`c:\*\*\directory3\` is invalid)
- For exclusions without a specific file or filename with wildcard, a trailing backslash must be present or the exclusion will be treated as a file exclusion.

Valid	Invalid
`c:\*\directory1\directory2\`	`c:\directory1\directory*\`
`c:\directory1\*\directory3\`	`c:\directory1\*\directory3\*\directory5\`
`%system_variable%\*\directory1\`	`c:\*\*\directory3\`

Full filename and extension

Restriction: Cannot be used in conjunction with full directory wildcards (`c:\directory1\*\*.exe` is invalid).

Valid	Invalid
`*.exe`	`*file.exe`
`abc.*`	`file*.exe`
`c:\directory1\*.exe`	`c:\directory1\*file.exe`
`c:\directory1\file.*`	`c:\directory1\file*.exe`

Valid	Invalid
`%system_variable%\directory1\*.exe`	`c:\*\file.exe`
	`%system_variable%\directory1\*\*.exe`

Drives and System Variables

Restriction: Cannot be used with a file exclusion (`*\directory1\file.exe` is invalid)

Valid	Invalid
`*\directory1\directory2\`	`*\directory1\*.exe`
`*\*\directory2\`	`*\directory1\file.*`
`*\%system_variable%\directory1\*\`	`*\directory1\file.exe`

Managing Antivirus Policies

After you have created one or more antivirus policies, you can perform policy management functions. You can manage antivirus policies centrally on the ***Antivirus Policies*** page, or on an endpoint's ***Details*** page or a group's page.

When you select a policy on the ***Antivirus Policies*** page the following functions are available:

- Assigning a policy
- Unassigning a policy
- Deleting a policy
- Editing a policy
- Enabling a policy
- Disabling a policy
- Exporting policy details

When you select a policy on an endpoint's ***Details*** page or a group's page, a more limited set of functions are available:

- Assigning a policy
- Unassigning a policy
- Exporting policy details

Note: You cannot delete, edit, enable, or disable a policy at group or endpoint level because these actions could have an undesired effect if the policy also applies to other endpoints or groups.

Managing Antivirus Policies Centrally

You can manage antivirus policies centrally on the ***Antivirus Policies*** page.

The ***Antivirus Policies*** page lists all existing antivirus policies and enables you to perform a wide range of management functions on them. From here, you can assign the policies to endpoints and groups. You can also un-assign, delete, and edit them, as well as enabling and disabling them.

Assigning a Policy

Use the ***AntiVirus Policies*** page to assign an existing policy to one or more endpoints or groups.

1. Select **Manage** > **AntiVirus Policies**.

   Step Result: The ***AntiVirus Policies*** page opens.

2. Select a policy to assign.

   Note:

   - You can only select and assign one policy at a time.
   - A policy can be assigned multiple times to different endpoints or groups.

   Step Result: The **Assign** button becomes available.

3. Click **Assign**.

   Step Result: Depending on the type of policy selected, the relevant policy wizard opens at the ***Assign virus and malware scan policy to groups and/or endpoints*** page.

4. Build a list of targets (endpoints), using either or both of the following methods:

Important: Recurring scans will not run on an endpoint that is shutdown or hibernating at the scheduled scan time.

Method	Steps
To define targets using groups:	1. If the **Groups** section is not open, click its up arrow to open it. 2. Select one or more endpoint groups by selecting their check boxes. 3. Click **Add**. This adds the group(s) to the **Assigned** list.

Method	Steps
To define targets using endpoints:	**1.** If the **Endpoints** section is not open, click its up arrow to open it. **2.** In the search field, do one of the following: • Type an endpoint name (to search for a specific endpoint) • Type part of an endpoint name (to search for similarly named endpoints) • Leave it blank (to search for all available endpoints) **3.** Click the **Search** icon. Depending on what you typed, one or more endpoints will appear in the **Name** column, with their respective IP addresses. **4.** Select the check box for each endpoint you want to assign. **5.** Click **Add**. This adds the endpoint(s) to the **Assigned** list.

Note: You can remove targets from the **Assigned** list by selecting the applicable check boxes and clicking **Remove**.

5. Click **Finish**.

Result: The policy has been assigned to one or more endpoints or groups.

Note: The **Assigned** column entry for that policy now contains:

- An **Assigned** link, which opens the policy wizard at the ***Assign virus and malware scan policy to groups and/or endpoints*** page. This enables you to change the endpoints or groups that the policy is assigned to.
- An **Information** icon, which displays a list of the endpoints or groups that the policy is assigned to.

Unassigning a Policy

On the ***Antivirus Policies*** page you can unassign policies that are currently assigned to endpoints or groups.

1. Select **Manage** > **Antivirus Policies**.

   Step Result: The ***Antivirus Policies*** page opens.

2. Select a policy to unassign.

Note: You can select more than one policy to unassign at a time.

Step Result: The **Unassign** button becomes available.

3. Click **Unassign**.

   Step Result: The ***Unassign Policy*** dialog opens, asking you to confirm the unassignment of the policy.

Figure 34: Confirm unassign Policy Dialog

> **Note:** If you have selected more than one policy, the dialog lists the policies and gives you the option of viewing them and removing them from the list.

4. Click **Yes**.

   Step Result: The selected policy is unassigned.

Deleting a Policy

Use the ***AntiVirus Policies*** page to delete unassigned policies.

1. Select **Manage** > **AntiVirus Policies**.

   Step Result: The ***AntiVirus Policies*** page opens.

2. Select a policy to delete.

> **Note:**
>
> - Only unassigned policies can be deleted.
> - You can only delete one policy at a time.

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

3. Click **Delete**.

   Step Result: The ***Delete Antivirus Policy*** dialog opens, asking you to confirm the deletion of the policy.

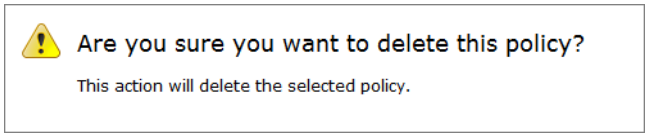


Figure 35: Delete Antivirus Policy Dialog

Note: If you have selected an assigned policy, the dialog lists the associations (endpoints or groups) that must be removed before the policy can be deleted.

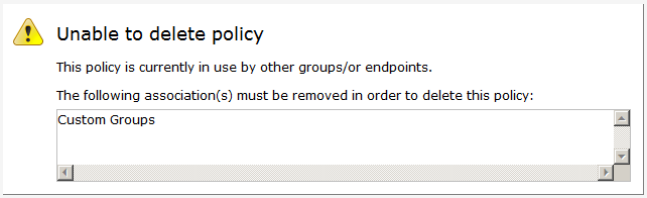


Figure 36: Unable to Delete Policy Dialog

4. Click **Yes**.

Result: The selected policy is deleted.

Editing a Policy

Use the ***AntiVirus Policies*** page to select a policy and edit it with the relevant wizard.

1. Select **Manage** > **AntiVirus Policies**.

   Step Result: The ***AntiVirus Policies*** page opens.

2. Select a policy to edit.

   Note: You can only edit one policy at a time.

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

3. Click **Edit**.

   Step Result: Depending on the type of policy selected, the relevant policy wizard opens.

4. Use the wizard to make the required changes to the policy. It provides the same functionality as when you are creating a policy. See Creating a Recurring Virus and Malware Scan Policy on page 120 or Creating a Real-time Monitoring Policy on page 129 for more information.
5. When you have made all required changes to the AntiVirus policy, click the wizard's **Finish** button.

Result: The AntiVirus policy has been edited.

Disabling a Policy

You can disable an AntiVirus policy, for troubleshooting purposes or when policy enforcement is temporarily not required, on the ***AntiVirus Policies*** page. By default, a policy is enabled upon creation.

Unlike deleting, by disabling a policy you retain the policy's details and can re-enable it later.

1. Select **Manage** > **Antivirus Policies**.

   Step Result: The ***Antivirus Policies*** page opens.

2. Select one or more policies to disable.

   Note: You can only disable a currently enabled policy, identified by the **Enabled** icon in the **Status** column.

   Step Result: The **Disable** button becomes available.

3. Click **Disable**.

   Step Result: The ***Confirm Disable Policy*** dialog opens, asking you to confirm the disabling of the policy.

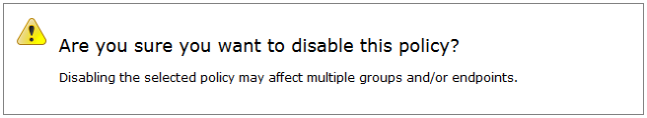


Figure 37: Confirm Disable Policy Dialog

.

4. Click **Yes**.

Result: The selected policy is disabled, and its **Status** icon changes to **Disabled**.

Enabling a Policy

Use the ***AntiVirus Policies*** page to select and enable antivirus policies.

1. Select **Manage** > **AntiVirus Policies**.

   Step Result: The ***AntiVirus Policies*** page opens.

2. Select one or more policies to enable.

   Note: You can only enable a currently disabled policy, identified by the **Disabled** icon in the **Status** column.

   Step Result: The **Enable** button becomes available.

3. Click **Enable**.

Result: The selected policy is enabled, and its **Status** icon changes to **Enabled**.

Managing Antivirus Policies on the Endpoint

You can manage antivirus policies on a selected endpoint.

An endpoint's ***Details*** page has an ***Antivirus Policies*** tab. From here you can assign and un-assign policies for the endpoint. You can also export details of the antivirus policies that apply to the endpoint.

Assigning an AntiVirus Policy on the Endpoint

You can assign one or more existing antivirus policies on an endpoint's ***Details*** page.

1. Select **Manage** > **Endpoints**.
2. Click the hyperlinked name of the desired endpoint.

   Step Result: The endpoint's ***Details*** page opens to the Information tab.
3. Click the ***AntiVirus Policies*** tab.

   Step Result: The ***AntiVirus Policies*** tab opens, displaying any policies that are already assigned to the endpoint.
4. Choose the type of policy to assign:

Option	Description
Recurring Virus and Malware Scan	Click **Assign** > **Recurring Virus and Malware Scan**.
Real-time Monitoring Policy	Click **Assign** > **Real-time Monitoring Policy**.

   Step Result: The ***Assign Policy*** dialog opens.
5. Select one or more policies to assign to the endpoint.
6. Click **OK**.

   Step Result: The dialog closes and the policy is added to the list on the ***AntiVirus Policies*** tab.

> **Note:** When a policy is assigned on an endpoint, it is no longer displayed in the ***Assign Policy*** dialog that opens for that endpoint. This is because a specific policy can be assigned only once to an endpoint.

Result: One or more AntiVirus policies have been assigned to the endpoint.

Unassigning an Antivirus Policy on the Endpoint

You can unassign antivirus policies from an endpoint on its ***Details*** page.

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

2. Click the hyperlinked name of the desired endpoint.

   Step Result: The endpoint's ***Details*** page opens.

3. Click the ***Antivirus Policies*** tab.

   Step Result: The ***Antivirus Policies*** tab opens, displaying any policies that are already assigned to the endpoint.

4. Select one or more policies to unassign from the endpoint.
5. Click **Unassign**.

   Step Result: The ***Unassign Policy*** dialog opens.

6. Click **Yes**.

   Step Result: The dialog closes and the policy is removed from the list on the ***Antivirus Policies*** tab.

Result: One or more antivirus policies are unassigned from the endpoint.

Managing Antivirus Policies on the Group

You can manage antivirus policies on a selected group.

A group's page has an **Antivirus Policies** view. From here you can assign and un-assign policies for the group. You can also export details of the antivirus policies that apply to the group.

Assigning an AntiVirus Policy on the Group

You can assign one or more existing AntiVirus policies on a group's page.

1. Select **Manage** > **Groups**.
2. Select a group fromthe **Browser**.
3. Select the ***AntiVirus Policies*** view.

   Step Result: The ***AntiVirus Policies*** view is displayed, showing any policies that are already assigned to the group.

4. Choose the type of policy to assign:

Option	Description
Recurring Virus and Malware Scan	Click **Assign** > **Recurring Virus and Malware Scan**.
Real-time Monitoring Policy	Click **Assign** > **Real-time Monitoring Policy**.

   Step Result: The ***Assign Policy*** dialog opens.

5. Select one or more policies to assign to the group.

6. Click **OK**.

   Step Result: The dialog closes and the policy is added to the list in the ***AntiVirus Policies*** view.

   Note: The policy is no longer displayed in the ***Assign Policy*** dialog that opens for that group. This is because a specific policy can be assigned only once to a group.

Result: One or more AntiVirus policies have been assigned to the group.

Unassigning an Antivirus Policy on the Group
You can unassign antivirus policies from a group on its group page.

1. Select **Manage** > **Groups**.
2. Select a group from the **Browser**.
3. Select the **Antivirus Policies** view.

   Step Result: The **Antivirus Policies** view is displayed, showing any policies that are already assigned to the group.

4. Select one or more policies to unassign from the endpoint.
5. Click **Unassign**.

   Step Result: The ***Unassign Policy*** dialog opens.

6. Click **Yes**.

   Step Result: The dialog closes and the policy is removed from the list of policies assigned to the group.

Result: One or more antivirus policies are unassigned from the group.

Chapter 7

Using Scan Now

In this chapter:

- About Scan Now
- The Virus and Malware Scan Wizard
- Running Scan Now on Selected Targets
- Scan Now Task Status
- Viewing the Last AntiVirus Scan Log on an Endpoint

To address potential threats, administrators occasionally need to run an immediate antivirus scan, rather than wait for a scan scheduled by policy. In Ivanti AntiVirus this type of scan is called *Scan Now*.

A Scan Now can be configured to run on selected endpoints and groups using the quick and convenient ***Virus and Malware Scan Wizard***. Scan results can then be viewed in a centralized location, and appropriate action can be taken to handle any detected viruses or malware.

About Scan Now

You can initiate an antivirus scan in matters of urgency using the Scan Now feature.

In Ivanti AntiVirus most virus scans are performed on a scheduled basis as a result of policy settings. But in some circumstances an administrator may wish to run an immediate scan to prevent possible problems.

For example, when an administrator is notified of odd behavior among a group of endpoints, the suspect may be a recently announced virus variant (although no event alerts have so far been generated). Immediately running an antivirus scan on these endpoints will show whether they are infected. If it turns out that they are, the infected files can be cleaned or deleted. This kind of timely intervention can prevent malware spreading and damaging the network.

The *Scan Now* feature, (using the ***Virus and Malware Scan Wizard***) enables you to run an antivirus scan and set its options. The scan can be carried out immediately, or scheduled for a time that minimizes impact on network performance.

Note: There is a separate Scan Now feature that performs a Discover Applicable Updates (DAU) scan. This type of scan assists with the management and deployment of content items, and is not related to Ivanti AntiVirus.

The Virus and Malware Scan Wizard

A convenient wizard guides you through the process of configuring an antivirus scan.

You can access this wizard from the **Discover** menu or the ***Virus and Malware Event Alerts*** page. Using this wizard, you can:

- Schedule the scan
- Select the targets (endpoints or groups)
- Set the scan options
- Set exclusions from the scan

The request is then treated as an antivirus task. If the scan detects any malware, the results are displayed in the ***Virus and Malware Event Alerts*** page.

You can also access the ***Virus and Malware Scan Wizard*** after you have selected target endpoints or groups on the respective ***Endpoints*** or ***Groups*** pages. In this case, the wizard provides similar functionality except that it does not provide a ***Targets*** page because target selection has already been made.

Using the Virus and Malware Scan Wizard

When invoked from the **Discover** menu or the ***Virus and Malware Event Alerts*** page, the ***Virus and Malware Scan Wizard*** enables you to schedule an antivirus scan, build a list of targets, and set scan and exclusion options.

Prerequisites:

Ensure you have the latest version of the AntiVirus Engine and Definition file.

Use a Scan Now - Virus and Malware Scan in the following situations :

- Odd behaviour observed on endpoints.
- Virus outbreak in the network.
- Long duration between scheduled Virus and Malware scans.

1. Select **Discover** > **Scan Now – Virus and Malware Scan**. If you are on the ***Virus and Malware Event Alerts*** page, click **Scan Now**.

   Step Result: The ***Virus and Malware Scan Wizard*** opens to the ***Scan Name and Scheduling*** page.

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

   Note: By default, new virus scans are named `New Virus and Malware Scan`, followed by the server's date and time, which is formatted according to your browser's locale setting.

3. Schedule the scan using one of the following methods:

Method	Steps
To schedule an immediate scan:	Select the **Run scan immediately** option.
To schedule a later scan:	1. Select the **Run scan at** option. 2. Type the start date in the **Start date** field. You can also select the start date by clicking the **Calendar** icon. 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon. **Note:** The purpose of the deferred scan feature is to enable you to schedule the scan at a time that will not adversely affect network or endpoint performance.

4. Click **Next**.

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

5. Build a list of targets (endpoints) for the virus scan, using either or both of the following methods:

Method	Steps
To define targets using individual endpoints:	1. From the **Target type** list, select **Endpoints**. 2. In the search field, type an endpoint name in one of the following formats: *endpointname* or *domain\endpointname*. Alternatively, you can type an IP address. **Tip:** You can type a partial name or IP address to search for a range of endpoints. 3. Click the **Search** icon. One or more endpoints are displayed in the area under the search field. 4. Select the check box for the endpoint you want to scan. 5. Click **Add to Target List**.

Method	Steps
To define targets using endpoint groups:	1. From the **Target type** list, select **Endpoint Groups**. 2. In the tree control, select one or more endpoint groups. 3. Click **Add to Target List**. **Note:** You can exclude an endpoint or subgroup from a group that is to be scanned. Select the endpoint/subgroup in the tree control and click **Exclude from Target List**.

Note: You must add at least one endpoint or group for **Next** to become available. If you change your mind about anything you have added to the target list, you can remove it from the list by selecting its check box and clicking **Remove**.

Step Result: One or more endpoints are assigned to the scan.

6. Click **Next**.

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

7. Select the scan policy option:

Setting	Result
Use the endpoint's virus and malware scan policy	The scanning, performance, and logging options of the endpoint's policies will be used. You can click **Finish** to start the scan.
Override the endpoint virus and malware scan policy with the following:	Enables the **Scanning**, **CPU utilization %**, and **Logging level** controls. **Important:** Ensure you have a clear understanding of the scan options before overriding the default settings.

8. From the drop-down list, select the action that occurs when a virus is detected.

Setting	Result
Perform no action	Does nothing with the infected file, but sends an alert to the server.
Attempt to clean then quarantine	Attempts to clean the infected file. If this is not possible, the file is quarantined. An alert is sent to the server. **Note:** This option is the default selection.
Attempt to clean then delete	Attempts to clean the infected file. If this is not possible, the file is deleted. An alert is sent to the server.

Setting	Result
Attempt to clean then quarantine then delete	Attempts to clean the infected file. If this is not possible, the file is quarantined. If it is not possible to quarantine it, it is deleted. An alert is sent to the server.

Note:

- To *clean* an infected file means to completely remove the malicious code so that the file is safe to use. It is not always possible to remove the malicious code, however. When this happens, you can either delete the file or *quarantine* it. To quarantine means to move it to a safe place on the endpoint where it can be kept for further examination.

  In certain cases (such as when the malware is a Trojan) the entire file is malicious. Such a file cannot be cleaned, so the only options are to quarantine or delete it.
- Virus detection actions are not used for memory scans.

9. Set the **Scanning** options:

Setting	Result
Scan boot sectors	The virus scan will be more thorough if you scan boot sectors in addition to program and data files. **Note:** If malware is detected in a boot sector, the action taken depends on the virus detection option selected: • **Perform no action** - the boot sector is left as it is and an alert is sent to the ***Virus and Malware Event Alerts*** page. • **Clean/Delete/Quarantine** - the boot sector is automatically repaired.
Scan archives	The virus scan will be more thorough if you scan archive files such as `.zip` and `.cab` files. **Note:** Infected .rar files can be quarantined and deleted, but can't be cleaned. See Archive Types Supported for Scanning on page 114
Scan memory	The virus scan will be more thorough if you scan the memory in addition to the disk(s). **Note:** • If the scan detects a virus/malware in memory, it will report the event. It will not clean, delete, or quarantine the virus/malware. • Exclusions are not applied to memory scans.

Setting	Result
Rootkit detection	A rootkit, similar to a hack tool, enables attackers to gain administrator access to a system. They hide the attacker's presence and give them full control of a server or client endpoint without being noticed. **Note:** Rootkit detection is only supported on endpoints running Windows versions from Vista onwards.

10. Set the ***CPU utilization %*** threshold to control the level of impact the scan is to have on endpoint performance:

Setting	Result
High	Quicker scanning but may noticeably impact endpoint performance.
Medium	Balances scan speed with endpoint performance impact (default option).
Low	Slower scanning but has the lowest impact on endpoint performance.

11. Set the logging options:

Note: As logging information is kept on the endpoint, the option you choose will not affect the loggings sent to the server.

Setting	Result
Do not log scanning results	No scan log is generated.
Normal logging level (includes results summary)	A standard scan log is generated.
Detailed logging level (includes results summary, name, time and status for each scanned file)	A detailed scan log is generated. **Caution:** Logging detailed virus scan results typically generates large amounts of data, especially when recurring scans run frequently.

12. Click **Next** to exclude files and folders.

Step Result: The ***Exclude Files and Folders*** page opens.

This page enables you to exclude specified files and folders from the scan. You may want to do this because:

- You have some applications whose makers recommend be excluded from virus scans.
- You have folders containing large amounts of data that you consider relatively safe, such as graphics files. Excluding them from the scan saves time.
- You have files that cause known "false positives" during a scan.

Caution: Excluding files or paths from the scan always involves some degree of risk.

13. Exclude files and folders, using one of the following methods:

Tip: Masks and system variables can be used to exclude files and paths.

Method	Steps
Manually exclude specific files and folders from the scan.	1. Click **Add**. A blank entry is added to the exclusions list. 2. Select an exclusion type from the **Type** field. The types are File and Folder. 3. Enter the path to the item you want to exclude in the **Path** field. 4. Click  to add the exclusion to the list. Repeat this procedure for all files and folders you want to exclude from the scan. **Note:** Click **Remove** () to remove items from the exclusion list.
Import an XML file containing a formatted list of file and folder exclusions.	See Importing File, Folder and Process Exclusions on page 136.

14. Configure the **Optional drives** settings:

Setting	Result
Scan locally-attached media	All storage media (including external hard drives, USB devices, and DVD/CD media) are included in the scan.

15. Click **Finish**.

Step Result: The ***Virus and Malware Scan Wizard*** closes. The scan begins, either immediately or at the scheduled time. After the scan completes, the ***Virus and Malware Scan Results*** page displays details of any malware that has been detected.

After Completing This Task:
On completion of scanning, you can:

- View the Scan Now log file on endpoints in `<INSTALL_DIR>\LMAgent\logs\AV`.
- Manage detected threats in quarantine.
- Report threats as false positives to Ivanti.

Running Scan Now on Selected Targets

You can run a Scan Now from pages where you have selected target endpoints or groups.

Administrators will often use the ***Endpoints*** and ***Groups*** pages, as they provide useful information such as operating system details and agent information. If an administrator decides to run an antivirus scan on one or more groups or endpoints, the ***Virus and Malware Scan Wizard*** can be launched from these pages to run the scan.

Running Scan Now on an Endpoint

You can use the ***Virus and Malware Scan Wizard*** to run an antivirus scan on endpoints that are selected on the ***Endpoints*** page.

This wizard is similar to the ***Virus and Malware Scan Wizard*** available on the **Discover** menu, except that it does not have a ***Targets*** page.

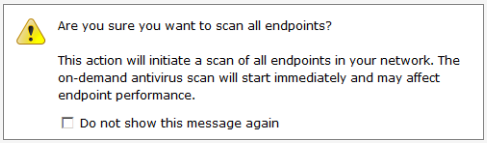
1. Select **Manage** > **Endpoints**.

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

2. Select the **Antivirus** tab.
3. Select one or more endpoints to be scanned.

4. Click **Scan Now**.

Note: If you do not select any endpoints before clicking **Scan Now** , *all* the endpoints are selected by default. You will then see the following dialog:



Click **Yes** to scan all endpoints, or click **No** to return to the list and select particular endpoints.

Step Result: The ***Scan Now - Virus and Malware Scan*** wizard opens to the ***Scan Name and Scheduling*** page.

5. [Optional] Type a new name in the **Scan Name** field.

Note: By default, new virus scans are named `New Virus and Malware Scan`, followed by the server's date and time, which is formatted according to your browser's locale setting.

6. Schedule the scan using one of the following methods:

Method	Steps
To schedule an immediate scan:	Select the **Run scan immediately** option.
To schedule a later scan:	1. Select the **Run scan at** option. 2. Type the start date in the **Start date** field. You can also select the start date by clicking the **Calendar** icon. 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon. **Note:** The purpose of the deferred scan feature is to enable you to schedule the scan at a time that will not adversely affect network or endpoint performance.

7. Click **Next**.

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

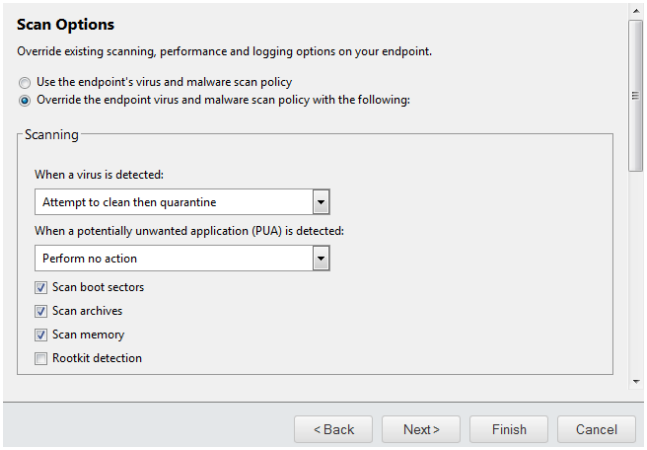


Figure 38: Scan Options

8. From the drop-down list, select the action that occurs when a virus is detected.

Setting	Result
Perform no action	Does nothing with the infected file, but sends an alert to the server.
Attempt to clean then quarantine	Attempts to clean the infected file. If this is not possible, the file is quarantined. An alert is sent to the server. **Note:** This option is the default selection.
Attempt to clean then delete	Attempts to clean the infected file. If this is not possible, the file is deleted. An alert is sent to the server.

Setting	Result
Attempt to clean then quarantine then delete	Attempts to clean the infected file. If this is not possible, the file is quarantined. If it is not possible to quarantine it, it is deleted. An alert is sent to the server.

Note:

- To *clean* an infected file means to completely remove the malicious code so that the file is safe to use. It is not always possible to remove the malicious code, however. When this happens, you can either delete the file or *quarantine* it. To quarantine means to move it to a safe place on the endpoint where it can be kept for further examination.

  In certain cases (such as when the malware is a Trojan) the entire file is malicious. Such a file cannot be cleaned, so the only options are to quarantine or delete it.
- Virus detection actions are not used for memory scans.

9. From the drop-down list, select the action to be taken when a potentially unwanted application (PUA) is detected:

Setting	Result
Perform no action	The system ignores the potentially unwanted application. **Note:** This option is the default selection.
Send alert only	An alert is sent to the server only.
Alert and action (treat as malware)	An alert is sent to the server and the file is cleaned, quarantined, or deleted, according to the action you selected in the **When a virus is detected** drop down.

10. Set the **Scanning** options:

Setting	Result
Scan boot sectors	The virus scan will be more thorough if you scan boot sectors in addition to program and data files. **Note:** If malware is detected in a boot sector, the action taken depends on the virus detection option selected: • **Perform no action** - the boot sector is left as it is and an alert is sent to the ***Virus and Malware Event Alerts*** page. • **Clean/Delete/Quarantine** - the boot sector is automatically repaired.

Setting	Result
Scan archives	The virus scan will be more thorough if you scan archive files such as `.zip` and `.cab` files. **Note:** Infected .rar files can be quarantined and deleted, but can't be cleaned. See Archive Types Supported for Scanning on page 114
Scan memory	The virus scan will be more thorough if you scan the memory in addition to the disk(s). **Note:** • If the scan detects a virus/malware in memory, it will report the event. It will not clean, delete, or quarantine the virus/malware. • Exclusions are not applied to memory scans.
Rootkit detection	A rootkit, similar to a hack tool, enables attackers to gain administrator access to a system. They hide the attacker's presence and give them full control of a server or client endpoint without being noticed. **Note:** Rootkit detection is only supported on endpoints running Windows versions from Vista onwards.

11. Set the ***CPU utilization %*** threshold to control the level of impact the scan is to have on endpoint performance:

Setting	Result
High	Quicker scanning but may noticeably impact endpoint performance.
Medium	Balances scan speed with endpoint performance impact (default option).
Low	Slower scanning but has the lowest impact on endpoint performance.

12. Set the logging options:

Note: As logging information is kept on the endpoint, the option you choose will not affect the loggings sent to the server.

Setting	Result
Do not log scanning results	No scan log is generated.
Normal logging level (includes results summary)	A standard scan log is generated.
Detailed logging level (includes results summary, name, time and status for each scanned file)	A detailed scan log is generated. **Caution:** Logging detailed virus scan results typically generates large amounts of data, especially when recurring scans run frequently.

13. Exclude files or paths, using one of the following methods:

Tip: Masks and system variables can be used to exclude files and paths.

Method	Steps
Manually exclude specific files and folders from the scan.	1. Click **Add**. A blank entry is added to the exclusions list. 2. Select an exclusion type from the **Type** field. The types are File and Folder. 3. Enter the path to the item you want to exclude in the **Path** field. 4. Click  to add the exclusion to the list. Repeat this procedure for all files, folders and processes you want to exclude from the scan. **Note:** Click **Remove** () to remove items from the exclusion list.
Import an XML file containing a formatted list of file and folder exclusions.	See Importing File, Folder and Process Exclusions on page 136.

14. When you are satisfied with all settings made on the ***Virus and Malware Scan Wizard***, click **Finish**.

Step Result: The ***Virus and Malware Scan Wizard*** closes. After the scan job completes, you can see the results on the ***Virus and Malware Scan Results*** page.

Running a Custom Scan Now on an Endpoint Using the Agent Control Panel

An endpoint user can manually initiate an on-demand virus and malware scan that targets specific drives, folders, and files.

Prerequisites:

- You must be on an endpoint hosting a Ivanti Endpoint Security Agent.
- No Scan Now or Recurring Virus and Malware Scan in progress.
- Ensure the endpoint has the latest version of the AntiVirus Engine and Definition file.
- Connect any removable media you want to scan to the endpoint (for example, a USB drive).

The ability to narrow scan scope enables you to use a custom Scan Now to:

- Target suspicious sections of media (for example, folders where content is frequently modified and accessed).
- Discover infected files before you use them.
- Scan only specific removable media (for example, a USB drive or DVD).
- Immediately scan files downloaded from the Internet or received by e-mail.

The scan settings used for a custom Scan Now to control performance and manage detected viruses are:

- **Scan boot sectors**: Off
- **Scan archives**: On
- **Scan memory**: Off
- **Rootkit detection**: On (supported on endpoints running Windows versions from Vista onwards)
- **CPU utilization %**: Resolved by the endpoint's resultant policy (default of "Medium" where no Recurring Virus and Malware Scan Policy is assigned).
- **Virus detection actions**: Resolved by the endpoint's resultant policy. Default of “Attempt to clean then quarantine then delete” where no Real-time Monitoring Policy is assigned.
- **Potentially Unwanted Application (PUA) detection action**: Resolved by the endpoint's resultant policy. Default of "Alert and action (treat as malware)" where no Real-time Monitoring Policy is assigned.
- **File and Path Exclusions**: Off

When you target a drive or folder, all files and folders it contains (including hidden) are scanned and permissions overruled.

Tip: You can view the resultant policy assigned to an endpoint on the Endpoints details page.

1. On the endpoint, select **Start** > **Control Panel**
2. Double-click **Agent Control Panel**.

   Step Result: The ***Agent Control Panel***.

3. From the main menu, click **AntiVirus** > **Scan Now & Events**.

   Step Result: The ***Scan Now & Events*** panel displays.

4. Click **Custom Scan**.

   Note: The **Custom Scan** button is disabled when a Scan Now or Recurring Virus and Malware Scan is in progress on the endpoint.

   Step Result: A dialog box that enables you to select files and folders displays.

5. Select the drives, folders, and files you want to scan, and then click **OK**.

Result: A custom Scan Now commences on the endpoint and "Scan In Progress" displays at the top of the panel. Viruses and malware detected during the scan appear on the ***Virus and Malware Event Alerts*** page in the Ivanti Endpoint Security Management Console.

After Completing This Task:
On completion of scanning, you can:

- View the Scan Now log file on the endpoint in `<INSTALL_DIR>\LMAgent\logs\AV`.
- Manage detected threats in quarantine.
- Report threats as false positives to Ivanti.

Running a Full Scan Now on an Endpoint Using The Agent Control Panel

An endpoint user can quickly initiate a thorough local on-demand virus and malware scan that targets all drives, folders, and files without the need to manually configure scan settings.

Prerequisites:

- You must be on an endpoint hosting a Ivanti Endpoint Security Agent.
- No Scan Now or Recurring Virus and Malware Scan in progress.
- Ensure you have the latest version of the AntiVirus Engine and Definition file.
- Connect any removable media you want to scan to the endpoint (for example, a USB drive).

Use a full Scan Now in the following situations :

- Odd behaviour observed on the endpoint.
- Virus outbreak in the network.
- After considerable Internet use and downloading activity.
- Long duration between scheduled Virus and Malware scans.

Scan settings configure automatically based on the endpoint's resultant policy. The default settings when no Recurring Virus and Malware Scan Policy is assigned are:

- **Scan boot sectors**: On
- **Scan archives**: On
- **Scan memory**: On
- **Rootkit detection**: On (supported on endpoints running Windows versions from Vista onwards)
- **CPU utilization %**: Medium
- **Virus detection actions**: Attempt to clean then quarantine then delete
- **Potentially Unwanted Application (PUA) detection action**: Alert and action (treat as malware)
- **File and Path Exclusions**: None

All files and folders (including hidden) are scanned and permissions overruled.

Tip: You can view the resultant policy assigned to an endpoint on the Endpoints details page.

1. On the endpoint, select **Start** > **Control Panel**
2. Double-click **Agent Control Panel**.

   Step Result: The ***Agent Control Panel*** opens.
3. From the main menu, click **AntiVirus** > **Scan Now & Events**.

   Step Result: The ***Scan Now & Events*** panel displays.
4. Click **Full Scan**.

   Note: The **Full Scan** button is disabled when a Scan Now or Recurring Virus and Malware Scan is in progress on the endpoint.

Result: A full Scan Now commences on the endpoint and "Scan In Progress" displays at the top of the panel. Viruses and malware detected during the scan appear on the ***Virus and Malware Event Alerts*** page in the Ivanti Endpoint Security Management Console.

After Completing This Task:
On completion of scanning, you can:

- View the Scan Now log file on the endpoint in `<INSTALL_DIR>\LMAgent\logs\AV`.
- Manage detected threats in quarantine.
- Report threats as false positives to Ivanti.

Running Scan Now on a Group

You can use the ***Virus and Malware Scan Wizard*** to run a virus scan on groups that have been selected on the ***Groups*** page.

This wizard is similar to the ***Virus and Malware Scan Wizard*** available on the **Discover** menu, except that it does not have a ***Targets*** page.

1. Select **Manage** > **Groups**.

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

2. Use the **Group Browser** to select one or more groups to be scanned.
3. Select **Virus and Malware Event Alerts** from the **View** list.
4. Click **Scan Now**.

   Step Result: The ***Virus and Malware Scan Wizard*** opens to the ***Scan Name and Scheduling*** page.

5. [Optional] Type a new name in the **Scan Name** field.

   Note: By default, new virus scans are named `New virus and malware scan`, followed by the server's date and time, which is formatted according to your browser's locale setting.

6. Schedule the scan using one of the following methods:

Method	Steps
To schedule an immediate scan:	Select the **Run scan immediately** option.
To schedule a later scan:	1. Select the **Run scan at** option. 2. Type the start date in the **Start date** field using a *mm/dd/yyyy* format. You can also select the start date by clicking the **Calender** icon . 3. Type the start time in the **Start time** field using a *hh:mm* format followed by AM or PM. This field supports both 12- and 24-hour time. Alternatively, you can select the start time by clicking the **Clock** icon . **Note:** The purpose of the deferred scan feature is to enable you to schedule the scan at a time that will not adversely affect network or endpoint performance.

7. Click **Next**.

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

8. Select the scan policy option:

Setting	Result
Use the endpoint's virus and malware scan policy	The scanning, performance, and logging options of the endpoint's policies will be used. You can click **Finish** to start the scan.

Setting	Result
Override the endpoint virus and malware scan policy with the following:	Enables the **Scanning**, **CPU utilization %**, and **Logging level** controls. **Important:** Ensure you have a clear understanding of the scan options before overriding the default settings.

9. From the drop-down list, select the action that occurs when a virus is detected.

Setting	Result
Perform no action	Does nothing with the infected file, but sends an alert to the server.
Attempt to clean then quarantine	Attempts to clean the infected file. If this is not possible, the file is quarantined. An alert is sent to the server. **Note:** This option is the default selection.
Attempt to clean then delete	Attempts to clean the infected file. If this is not possible, the file is deleted. An alert is sent to the server.
Attempt to clean then quarantine then delete	Attempts to clean the infected file. If this is not possible, the file is quarantined. If it is not possible to quarantine it, it is deleted. An alert is sent to the server.

Note:

- To *clean* an infected file means to completely remove the malicious code so that the file is safe to use. It is not always possible to remove the malicious code, however. When this happens, you can either delete the file or *quarantine* it. To quarantine means to move it to a safe place on the endpoint where it can be kept for further examination.

  In certain cases (such as when the malware is a Trojan) the entire file is malicious. Such a file cannot be cleaned, so the only options are to quarantine or delete it.
- Virus detection actions are not used for memory scans.

10. Set the **Scanning** options:

Setting	Result
Scan boot sectors	The virus scan will be more thorough if you scan boot sectors in addition to program and data files. **Note:** If malware is detected in a boot sector, the action taken depends on the virus detection option selected: • **Perform no action** - the boot sector is left as it is and an alert is sent to the ***Virus and Malware Event Alerts*** page. • **Clean/Delete/Quarantine** - the boot sector is automatically repaired.
Scan archives	The virus scan will be more thorough if you scan archive files such as `.zip` and `.cab` files. **Note:** Infected .rar files can be quarantined and deleted, but can't be cleaned. See Archive Types Supported for Scanning on page 114
Scan memory	The virus scan will be more thorough if you scan the memory in addition to the disk(s). **Note:** • If the scan detects a virus/malware in memory, it will report the event. It will not clean, delete, or quarantine the virus/malware. • Exclusions are not applied to memory scans.
Rootkit detection	A rootkit, similar to a hack tool, enables attackers to gain administrator access to a system. They hide the attacker's presence and give them full control of a server or client endpoint without being noticed. **Note:** Rootkit detection is only supported on endpoints running Windows versions from Vista onwards.

11. From the drop-down list, select the action to be taken when a potentially unwanted application (PUA) is detected:

Setting	Result
Perform no action	The system ignores the potentially unwanted application. **Note:** This option is the default selection.
Send alert only	An alert is sent to the server only.
Alert and action (treat as malware)	An alert is sent to the server and the file is cleaned, quarantined, or deleted, according to the action you selected in the **When a virus is detected** drop down.

12. Set the ***CPU utilization %*** threshold to control the level of impact the scan is to have on endpoint performance:

Setting	Result
High	Quicker scanning but may noticeably impact endpoint performance.
Medium	Balances scan speed with endpoint performance impact (default option).
Low	Slower scanning but has the lowest impact on endpoint performance.

13. Set the logging options:

Note: As logging information is kept on the endpoint, the option you choose will not affect the loggings sent to the server.

Setting	Result
Do not log scanning results	No scan log is generated.
Normal logging level (includes results summary)	A standard scan log is generated.
Detailed logging level (includes results summary, name, time and status for each scanned file)	A detailed scan log is generated. **Caution:** Logging detailed virus scan results typically generates large amounts of data, especially when recurring scans run frequently.

14. Exclude files or paths, using one of the following methods:

Tip: Masks and system variables can be used to exclude files and paths.

Method	Steps
Manually exclude specific files and folders from the scan.	1. Click **Add**. A blank entry is added to the exclusions list. 2. Select an exclusion type from the **Type** field. The types are File and Folder. 3. Enter the path to the item you want to exclude in the **Path** field. 4. Click  to add the exclusion to the list. Repeat this procedure for all files and folders you want to exclude from the scan. **Note:** Click **Remove** () to remove items from the exclusion list.
Import an XML file containing a formatted list of file and folder exclusions.	See Importing File, Folder and Process Exclusions on page 136.

15. When you are satisfied with all settings made on the ***Virus and Malware Scan Wizard***, click **Finish**.

Step Result: The ***Virus and Malware Scan Wizard*** closes. After the scan job completes, you can see the results on the ***Virus and Malware Scan Results*** page.

Scan Now Task Status

Scheduled, *In Progress* and *Completed* are the three statuses of Scan Now tasks.

A *Scan Now* task is a one-off antivirus scan run immediately or scheduled for another time. Available statuses are:

- **Scheduled**: The scan has not run as the start date and time are yet to occur. You can modify, reschedule or cancel the scan.
- **In Progress**: Target groups and endpoints are being scanned for viruses and malware. You cannot modify, reschedule or cancel the scan.
- **Completed**: The scan has run successfully and detailed results are available for viewing.

Viewing Scan Now Tasks

You can view Scan Now tasks that have been run or are scheduled on the ***Deployments and Tasks*** page.

Select **Manage** > **Deployment and Tasks**.

Step Result: The ***Deployments and Tasks*** page opens.

Result: Now you can view all Scan Now tasks, identified by the Type "Virus and Malware Scan". If required, filter the view to only include Scan Now tasks by selecting **Virus and Malware Scan** from the **Type** filter and clicking **Update View**. Expand the rows to show task details.

Viewing the Last AntiVirus Scan Log on an Endpoint

You can view a summary of the security threats detected and actions taken by the AntiVirus scan engine on an endpoint during its last completed on-demand scan directly from the Ivanti Endpoint Security Agent Control Panel.

Prerequisites:

- You must be on an endpoint hosting a Ivanti Endpoint Security Agent.
- A Scan Now or Recurring Virus and Malware Scan must have completed.

1. On the endpoint, select **Start** > **Control Panel**
2. Double-click **Agent Control Panel**.

   Step Result: The ***Agent Control Panel*** opens.
3. Select **AntiVirus** from the main menu.
4. In the ***Virus and Malware scan history*** section, click **View Log**.

   Step Result: The ***AntiVirus Scan Log*** report opens.

Result: Displayed is a report that details the actions performed on each individual infected file, as well as scan start and end times, scanned file statistics, and infection names.

A more detailed last scan log for use by Ivanti Technical Support is located in: `<INSTALL_DIR>\LMAgent\logs\AV`

Tip: In the Ivanti Endpoint Security Web console, use the ***Virus and Malware*** tab on an endpoint's ***Endpoint Details*** page (**Manage** > **Endpoints**) to view all alerts generated by virus and malware scans performed by Ivanti AntiVirus on a selected endpoint.

After Completing This Task:
You can review the last scan log and take appropriate action:

- If there are uncleaned and quarantined files, send the detailed last scan log located in `<INSTALL_DIR>\LMAgent\logs\AV` to Ivanti Technical Support.
- Verify that the latest AntiVirus Definitions file is loaded on the endpoint. For more information, see Checking the version of the AntiVirus Engine and Definition on page 107.
- Examine what AntiVirus policies are assigned to the endpoint. For more information, see Viewing Endpoint Antivirus Policies on page 119

Chapter 8

Viewing Virus Scan Results

In this chapter:

- About Virus Scan Results
- The Virus and Malware Event Alerts Page
- The Virus/Malware Details Page
- Endpoint Malware Details
- Group Malware Details
- Checking Virus Scan Status

When virus scanning activities detect malware, the results are displayed in the ***Virus and Malware Event Alerts*** page.

This page provides access to additional information on any malware detected during the scan, and the endpoint on which it was found. You can then (if necessary) take further action to remove any remaining malware threat to the network.

You can also view the status of Scan Now and recurring scans on individual endpoints even if they have not detected any malware.

About Virus Scan Results

When a virus scan detects a virus or malware an *event alert* is generated and displayed in the ***Virus and Malware Event Alerts*** page.

The centralized view of all generated alert messages offered by the ***Virus and Malware Event Alerts*** page, which includes the malware detected and endpoints affected, is a good starting point for assessing the overall impact on the network.

To access more detailed information, each alert message provides two links:

- The **Virus/Malware Name** link provides details on the detected malware.
- The **Endpoint Name** link provides details on the affected endpoint.

When a scan runs and does *not* detect any malware, no event alerts are generated and nothing changes on the ***Virus and Malware Event Alerts*** page. However, an endpoint's ***Details*** page displays details of the last scan carried out on that endpoint.

Viewing Virus and Malware Event Alerts

To view event alerts generated by virus and malware scans, navigate to the ***Virus and Malware Event Alerts*** page.

1. Select **Review** > **Virus and Malware Event Alerts**.

   Step Result: The ***Virus and Malware Event Alerts*** page opens.

2. View the results and, if necessary, modify their display by
   a) Selecting filter options.
   b) Using the **Group By** row.

The Virus and Malware Event Alerts Page

The ***Virus and Malware Event Alerts*** page provides a centralized view of all alerts generated by virus and malware scans performed by Ivanti AntiVirus.

Table 51: Virus and Malware Event Alerts Features

Feature	Function
Filters	Filters list of event alerts.
Toolbar	Manages event alerts and launches ***Virus and Malware Scan Wizard***.
Group By row	Groups the list of event alerts.
Event Alerts list	Lists event alerts generated by virus scans.

The information and features enable you to:

Review current status	You can see the types of malware that have been detected and the endpoints that have been infected. This information will help you to determine how the infection originated and the best way to handle it.
Take remedial action	You can use Scan Now to launch the ***Virus and Malware Scan Wizard***, configuring it to perform specific actions that will reduce the threat to the network. See Using the Virus and Malware Scan Wizard on page 150 for more information.

The Virus and Malware Event Alerts Page Toolbar

The ***Virus and Malware Event Alerts*** page toolbar enables you to perform functions on the listed event alerts, and to run an on-demand scan.

Table 52: Virus and Malware Event Alerts Toolbar

Button	Function
Scan Now	Opens the ***Virus and Malware Scan Wizard***. This enables an administrator to react to incoming alerts with an immediate scan. When configured appropriately, this scan can eliminate the problem by cleaning or deleting the infected files. For more information on running these scans, see Using the Virus and Malware Scan Wizard on page 150.

Button	Function
Remove	Removes the selected event alert(s) from the list.
Export	Exports the event alerts list to a comma separated value (`.csv`) file.

Note: Only event alerts from the previous 90 days are displayed. If there are a large number of event alerts and you no longer need to view all of them, you can use the **Remove** button to remove unwanted alerts from the list. This does not delete them from the database, however, so you can always view these removed alerts by generating an appropriate report.

The Virus and Malware Event Alerts Page List

The ***Virus and Malware Event Alerts*** page provides a comprehensive and constantly updated list of all event alerts generated by the virus and malware scanning.

Table 53: Virus and Malware Event Alerts List

Column	Description
Virus/Malware Name	The name of the virus or malware detected. Each example links to the relevant entry in the ***Virus/Malware Details*** page.
Endpoint Name	The name of the endpoint where the virus or malware was detected. **Note:** Each example links to the relevant entry in the endpoint's ***Details*** page.
IP Address	The IP address of the endpoint where the virus or malware was detected.
Alert Source	The type of scan that generated the alert: • Real-time Monitoring Policy • Recurring Virus and Malware Scan • Scan Now
Status	The alert status: •  (Cleaned) •  (Deleted) •  (Not Cleaned) •  (Quarantined) **Note:** Both the *Cleaned* status and *Deleted* status use the same icon because in both cases the malicious code has been removed and no longer presents a danger.

Column	Description
Alert Message	The message related to the alert status: • Cleaned • Deleted • Not Cleaned • Quarantined
File Name	The name of the file in which the malware was detected.
File Path	The file path of the file in which the malware was detected.
Last Detected Date (Server)	The date and time the alert was generated (server time).

Tip: You can use the **Group By** row, available above the list, to sort list items into groups based on column headers. This feature (along with the filters above the toolbar) is useful when you need to examine a large number of event alerts.

The Virus/Malware Details Page

The ***Virus/Malware Details*** page provides information on the specific type of malware detected and lists the endpoints affected by that malware.

Viewing the Virus/Malware Details Page

To view detailed information on a detected virus or malware, navigate to the ***Virus/Malware Details*** page.

1. Select **Review** > **Virus and Malware Event Alerts**.

   Step Result: The ***Virus and Malware Event Alerts*** page opens. If a virus scan has detected viruses or malware, they will be displayed in the **Virus/Malware** column.

2. Click the hyperlink for the virus or malware you want to investigate.

   Step Result: The ***Virus/Malware Details*** page opens.

The Virus/Malware Details Page List

The ***Virus/Malware Details*** page gives detailed information on all the endpoints affected by a specific virus or malware.

The following table describes the information found in the list of affected endpoints. Each endpoint can be listed multiple times, depending on how many examples of the malware are infecting it.

Table 54: Affected Endpoints List

Column	Description
Endpoint Name	The name of the endpoint where the virus or malware was detected.
IP Address	The IP address of the endpoint where the virus or malware was detected.
Alert Source	The type of scan that generated the alert: • Recurring Virus and Malware Scan • Real-time Monitoring Policy • Scan Now
Status	The alert status: •  (Cleaned) •  (Deleted) •  (Not Cleaned) •  (Quarantined) **Note:** Both *Cleaned* status and *Deleted* status use the same icon because in both cases the malicious code has been removed and no longer presents a danger.
Alert Message	The message related to the alert status: • Cleaned • Deleted • Not Cleaned • Quarantined
File Name	The name of the file in which the virus or malware was detected.
File Path	The file path of the file in which the virus or malware was detected.

Column	Description
Last Detected Date (Server)	The date and time the alert was generated (saved as server time).

Tip: You can collapse the display of any endpoint's details by clicking the arrow beside it. This is useful when an endpoint has many files infected with the same malware.

Endpoint Malware Details

You can see all the malware event alerts for a specific endpoint on the ***Virus and Malware*** tab of that endpoint's ***Details*** page.

Viewing Endpoint Malware Details

You can see all the malware alerts for a specific endpoint on the ***Virus and Malware*** tab of its ***Details*** page.

1. Select **Review** > **Virus and Malware Event Alerts**.

   Step Result: The ***Virus and Malware Event Alerts*** page opens. If a virus scan has detected viruses or malware, the affected endpoints are displayed in the **Endpoints** column.

2. Click the hyperlink for the endpoint you want to investigate.

   Step Result: The endpoint's ***Details*** page opens on the ***Virus and Malware*** tab.

Endpoint Details Virus and Malware Tab

The ***Virus and Malware*** tab of an endpoint's ***Details*** page summarizes recent scan activity and provides a list of the alert messages associated with the endpoint.

The **Virus and malware scan summary** provides information on the last ScanNow or recurring scan that was carried out on the endpoint.

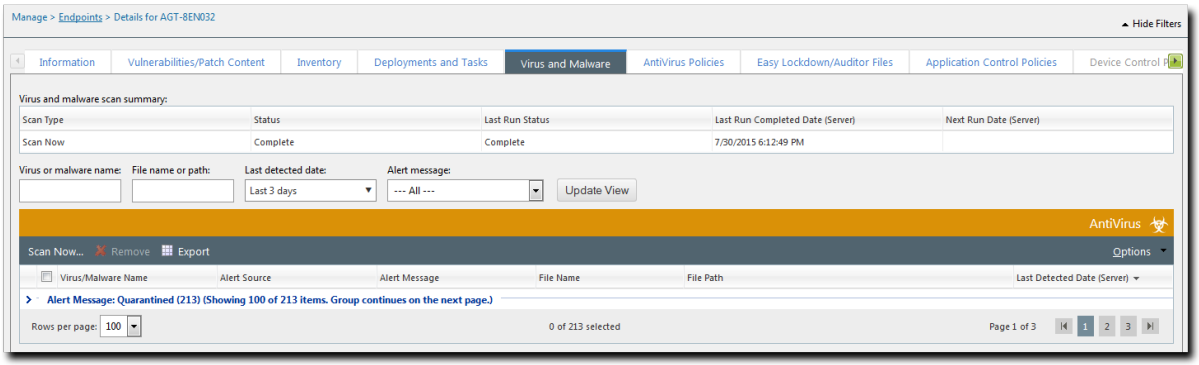


Figure 39: Virus and Malware Scan Summary

Table 55: Virus and malware scan summary

Column	Description
Scan Type	• Real-time Monitoring Policy • Recurring Virus and Malware Scan • Scan Now - Virus and Malware Scan
Status	Completed
Last Run Status	• Complete • Failure
Last Run Completed Date	The time and date that the scan last completed
Next Run Date	In the case of a recurring scan, the time and date it is due to run again.

The **Found virus and malware** list provides detailed information on the status of the malware detected:

Table 56: Found virus and malware list

Column	Description
Virus/Malware Name	The name of the virus or malware detected on the endpoint. This can be listed multiple times, depending on how many examples of it have been detected in different files and folders on the endpoint.

Column	Description
Alert Source	The type of scan which generated the alert: • Recurring Virus and Malware Scan • Real-time Monitoring Policy • Scan Now
Status	The alert status: • (Cleaned) • (Deleted) • (Not Cleaned) • (Quarantined) **Note:** Both *Cleaned* status and *Deleted* status use the same icon because in both cases the malicious code has been removed and no longer presents a danger.
Alert Message	The message related to the alert status: • Cleaned • Deleted • Not Cleaned • Quarantined
File Name	The name of the file in which the virus or malware was detected.
File Path	The file path of the file in which the malware was detected.
Detected Date	The date and time the alert was generated.

Group Malware Details

You can see all the malware event alerts for a group on the ***Virus and Malware Event Alerts*** view of that group's page.

Viewing Group Malware Details

You can see all the malware alerts for the endpoints in a selected group on that group's **Virus and Malware Event Alerts** view.

1. Select **Manage** > **Groups**.
2. Select the required group from the ***Browser***.

3. Select the **Virus and Malware Event Alerts** view.

   Step Result: The virus and malware event alerts for all endpoints in the selected group are displayed.

   Tip: The event alerts are normally sorted by the column header(s) in the **Group By** row. You can change the column header(s) if required.

Group Virus and Malware Event Alerts View

The ***Virus and Malware Event Alerts*** view of a Groups page provides a list of the alert messages for all endpoints in the group.

A group is a collection of endpoints, so the results on this page are simply a list of the event alerts for all endpoints in the selected group.

Table 57: Found virus and malware list

Column	Description
Virus/Malware Name	The name of the virus or malware detected on the endpoint. This can be listed multiple times for the same endpoint, depending on how many examples of it have been detected in different files and folders.
Endpoint Name	The name of the endpoint where the malware was detected.
IP Address	The IP address of the endpoint where the malware was detected.
Alert Source	The type of scan which generated the alert: • Recurring Virus and Malware Scan • Real-time Monitoring Policy • Scan Now
Alert Message	The message related to the alert status: • Cleaned • Deleted • Not Cleaned • Quarantined
File Name	The name of the file in which the virus or malware was detected.
File Path	The file path of the file in which the malware was detected.
Last Detected Date (Server)	The date and time the alert was generated (server time).

Checking Virus Scan Status

Even if a virus scan has not generated an alert, you can check its status if it is a Scan Now or recurring scan.

When a virus scan detects a virus or other malware, it generates an event alert which is displayed on the ***Virus and Malware Event Alerts*** page. But sometimes it is useful to check the status of a scan, even if it has not generated any alerts. You can do this on the following pages:

Deployments and Tasks page	Displays the status of Scan Now tasks that have executed already or are scheduled to execute.
Endpoint Details page	The **Virus and Malware** tab displays the status of the last Scan Now or recurring scan that was run on a specific endpoint.

Viewing the Virus/Malware Details Page

To view detailed information on a detected virus or malware, navigate to the ***Virus/Malware Details*** page.

1. Select **Review** > **Virus and Malware Event Alerts**.

   Step Result: The ***Virus and Malware Event Alerts*** page opens. If a virus scan has detected viruses or malware, they will be displayed in the **Virus/Malware** column.

2. Click the hyperlink for the virus or malware you want to investigate.

   Step Result: The ***Virus/Malware Details*** page opens.

The Virus/Malware Details Page List

The ***Virus/Malware Details*** page gives detailed information on all the endpoints affected by a specific virus or malware.

The following table describes the information found in the list of affected endpoints. Each endpoint can be listed multiple times, depending on how many examples of the malware are infecting it.

Table 58: Affected Endpoints List

Column	Description
Endpoint Name	The name of the endpoint where the virus or malware was detected.
IP Address	The IP address of the endpoint where the virus or malware was detected.
Alert Source	The type of scan that generated the alert: • Recurring Virus and Malware Scan • Real-time Monitoring Policy • Scan Now

Column	Description
Status	The alert status: •  (Cleaned) •  (Deleted) •  (Not Cleaned) •  (Quarantined) **Note:** Both *Cleaned* status and *Deleted* status use the same icon because in both cases the malicious code has been removed and no longer presents a danger.
Alert Message	The message related to the alert status: • Cleaned • Deleted • Not Cleaned • Quarantined
File Name	The name of the file in which the virus or malware was detected.
File Path	The file path of the file in which the virus or malware was detected.
Last Detected Date (Server)	The date and time the alert was generated (saved as server time).

Tip: You can collapse the display of any endpoint's details by clicking the arrow beside it. This is useful when an endpoint has many files infected with the same malware.

Chapter 9

Managing Quarantined Files

In this chapter:

- Understanding Quarantine
- Viewing Files in Quarantine
- Restoring a File from Quarantine
- Deleting a File from Quarantine
- Deleting Files from Quarantine Automatically
- Centralized Quarantine

Quarantine enables you to manage files containing threats detected by both On-Demand and On-Access scans that were not automatically eliminated during scanning.

Understanding Quarantine

Quarantine is a storage area on endpoints that isolates infected and suspicious files that cannot be cleaned or deleted at time of detection. Files are prevented from running through encryption, which counters any threats posed by viruses and malware.

The types of files sent to quarantine, when `Attempt to clean then quarantine` (default) or `Attempt to clean then quarantine then delete` are set during scan configuration, are:

- Files AntiVirus was unable to disinfect.
- *False positive* detections in the rare cases when AntiVirus mistakes legitimate files for viruses because they contain viral code patterns.

When a file that needs to be isolated is detected, it is moved to the endpoint's `\LMAgent\Data\persist\AV\quarantine` folder and a Virus and Malware Event Alert of "Quarantined" is generated. Quarantined files can be viewed and managed in two ways:

<table>
<tr>
<td>On the Endpoint</td>
<td>Quarantine pane of the Agent Control Panel. Actions that can be performed are :
<table>
<tr><td>Delete</td><td>Removes the infected file permanently from the endpoint.</td></tr>
<tr><td>Save As</td><td>Enables you to move a file back to its original location or another location (for example, for submitting to Ivanti for analysis). Choose this action for a file you believe was incorrectly detected as infected.</td></tr>
</table>
</td>
</tr>
<tr>
<td>On the Ivanti Endpoint Security Management Console</td>
<td>Centralized Quarantine page provides a network-wide view of all files quarantined on endpoints. Actions that can be performed are:
<table>
<tr><td>Scan now</td><td>Runs an immediate AntiVirus scan on the endpoints you select.</td></tr>
<tr><td>Delete</td><td>Removes the infected file permanently from the endpoints you select.</td></tr>
</table>
</td>
</tr>
</table>

	Restore	Move a file back to its original location on the endpoints that you select.

AntiVirus scans quarantined files after each virus definition update. Cleaned files are automatically moved back to their original location, if no file with the same name is already present.

Quarantine related activity can be viewed on the ***Endpoints with Unresolved AV Alerts*** dashboard widget, which displays the number of endpoints with unresolved AntiVirus event alerts. There are two types of unresolved antivirus event alerts: not cleaned and quarantined.

Viewing Files in Quarantine

You can view the files in an endpoint's quarantine folder using the ***Centralized Quarantine*** page or the ***Agent Control Panel*** on endpoints..

Prerequisites:

- An AntiVirus scan must have completed, with the "Attempt to clean then quarantine" or "Attempt to clean then quarantine then delete" setting configured, where a threat that could not be cleaned was detected.

Viewing Quarantined Files Using Centralized Quarantined

You can view quarantined files from the Ivanti Endpoint Security Management Console, particularily if the same file has been quarantined on several endpoints.

Click **Manage** > **Centralized Quarantine**.

Result: The ***Centralized Quarantine*** page is displayed and files with threats that could not be cleaned during an AntiVirus scan are listed. The information provided for each file is:

- **File Name**
- **Virus/Malware Name** - Name of the Virus or Malware detected in the file.
- **Last Detection Date (server)** - Point in time when the latest file of this type was detected in your environment.
- **Endpoints Affected** - Number of endpoints with the same file in quarantine.
- **Endpoint** - Name of the endpoint with the quarantined file. Click the hyperlink for more details.
- **IP Address** - IP address of the endpoint with the quarantined file.
- **AV Definition Detected** - Version number of the AV definition file installed on the endpoint.
- **Status** - The current status of the quarantined file. The status will be pending when you the system is in the process of deleting or restoring the file from endpoints.
- **File Path** - Path of the location on the endpoint where the file was originally before it was moved to quarantine.
- **Detection Date** - Point in time when the file was scanned using the latest AntiVirus definition file.
- **SHA-256 Hash** - The unique hash assigned to the file.

Viewing Quarantined Files Using the Agent Console

You can view quarantined files directly from the endpoint.

1. On the endpoint, select **Start** > **Control Panel**.
2. Double-click **Agent Control Panel**.

   Step Result: The ***Agent Control Panel***.

3. Select**AntiVirus** > **Quarantine** from the main menu.

Result: The ***Quarantine*** pane is displayed and files with threats that could not be cleaned during an AntiVirus scan are listed. The information provided for each file is:

- **File Name**
- **Status** - The available statuses are Not Cleaned and Cleaned.
- **Last Update Date** - Date and time when the file was scanned using the latest AntiVirus definition file.
- **Original Location** - Path of the location where the file was originally before it was moved to quarantine.
- **Quarantined Date** - Date and time when the file was moved to quarantine.
- **Details** - Additonal information about the quarantined file, for example the type of infection.

After Completing This Task:
Now you can:

- Wait for the next AntiVirus definition file update to see if it will clean and restore a file.
- Restore a file from quarantine. For more information, see Restoring a File from Quarantine on page 189.
- Delete a file from quarantine. For more information, see Deleting a File from Quarantine on page 191.

Restoring a File from Quarantine

A file quarantined by AntiVirus that you know to be safe (false positive) can be manually restored to its source folder or an alternate protected location using the ***Centralized Quarantine*** page or the ***Agent Control Panel*** on endpoints.

Prerequisites:

- Ensure the latest version of the AntiVirus definition file is installed on endpoints, as it may contain the definition required to clean the threat detected.
- Consider submitting the quarantined file you want to restore to Ivanti for further analysis. It may be a new virus or a variant of an existing one.
- Ensure the file has been in quarantine for at least two AntiVirus definition file updates. Updates occur a minimum of once a day. Files in quarantine are automatically scanned upon update and if cleaned are moved back to their original location.
- Use the ***Centralized Quarantine*** page in the Ivanti Endpoint Security Management Console to check if the same files was quarantined on other endpoints.
- Consider isolating the endpoints to which the file is to be restored and moving important files to a backup location.

The only quarantined files you should restore are those for which no back-up exists or no copy can be obtained from a trustworthy source, like a vendor. It can be a file that contains important information

(for example, a document) or is required to regain the functionality of a program that needs the file to run. The agent places the files in an endpoint's local quarantine, therefore the procedure must be performed through the Agent Control Panel.

Restoring a Quarantined File Using Centralized Quarantine

You can restore a quarantined file from the Ivanti Endpoint Security Management Console, particularly if the same file has been quarantined on several endpoints.

1. Click **Manage** > **Centralized Quarantine**.
2. Find the file you want to restore.
   Use the filters to search for specific items.
3. Expand its section to reveal the endpoints the file is quarantined on and additional information.

   Note: Use the **AV Definition Detected** column to ensure the latest version of the AntiVirus definition file is installed on endpoints, as it may contain the definition required to clean the threat detected.

4. Select the endpoints you want to restore the file to and click **Restore**.

Restoring a Quarantined File Using the Agent Console

You can restore a quarantined file directly from the endpoint.

1. Log on to the endpoint and select **Start** > **Control Panel**.
2. Double-click **Agent Control Panel**.

   Step Result: The ***Agent Control Panel*** opens.

3. Select**AntiVirus** > **Quarantine**from the main menu.

   Step Result: The ***Quarantine*** pane is displayed.

4. Select a file from the list and then click **Save As**.

   Step Result: The ***Save As*** dialog opens to the directory where the file originated from.

5. Navigate to the directory in which you would like to save the file, then click **Save**.
   You can not overwrite a file with the same name in the selected location.

Result: The file is removed from quarantined and returned to the location you specified. A `Restored` alert message will be generated and can be viewed in **Review** > **Virus and Malware Event Alerts**.

After Completing This Task:

- Monitor the endpoints to which the file was restored for suspicious behavior.
- Exclude the file from scans if it was an authentic false positive. For more information, see Ivanti Community Article 58945.

Deleting a File from Quarantine

You can manually delete a file quarantined by AntiVirus, along with all associated registry keys, using the ***Centralized Quarantine*** page or the ***Agent Control Panel*** on endpoints.

Prerequisites:

- Ensure the latest version of the AntiVirus definition file is installed on the endpoint, as it may contain the definition required to clean the threat detected.
- Monitor the endpoint for behavior that indicates the quarantined file is required by a program to function, requiring that a replacement file be obtained.
- Consider submitting the quarantined file you want to delete to Ivanti for further analysis. It may be a new virus or a variant of an existing one.
- Ensure the file has been in quarantine for at least two AntiVirus definition file updates. Updates occur a minimum of once a day. Files in quarantine are automatically scanned upon update and if cleaned are moved back to their original location.

Occasionally the damage caused by a virus renders a file unable to be cleaned and must be deleted. If the file is required to regain the functionality of a program, recover it from a back-up or obtain a copy from a trustworthy source, like the vendor.

Tip: You can configure AntiVirus scans to automatically delete infected files by using the "Attempt to clean then delete" or "Attempt to clean then quarantine then delete" settings during their creation.

You can also set the option **Enable the automatic deletion of files from Quarantine** on **Tools** > **Options** > **AntiVirus tab**.

Deleting a Quarantined File Using Centralized Quarantine

You can delete a file from the Ivanti Endpoint Security Management Console, particularily if the same file has been quarantined on several endpoints.

1. Click **Manage** > **Centralized Quarantine**.
2. Find the file you want to delete.

   Use the filters to search for specific items.
3. Expand its section to reveal the endpoints the file is quarantined on and additional information.

   Note: Use the **AV Definition Detected** column to ensure the latest version of the AntiVirus definition file is installed on endpoints, as it may contain the definition required to clean the threat detected.
4. Select the endpoints you want to restore the file to and click **Delete**.

Deleting a Quarantined File Using the Agent Console

You can delete a quarantined file directly from the endpoint.

1. Log on to the endpoint and select **Start** > **Control Panel**.
2. Double-click **Agent Control Panel**.

   Step Result: The ***Agent Control Panel***.
3. Select**AntiVirus** > **Quarantine**from the main menu.

   Step Result: The ***Quarantine*** pane is displayed.
4. Select a file from the list and then click **Delete**.

   You can select multiple files by holding `CTRL`.

   Step Result: The dialog opens prompting you to confirm the deletion.
5. Click **Yes**.

Result: The file is removed from quarantined and deleted from the endpoint. A `Deleted` alert message will be generated and can be viewed in **Review** > **Virus and Malware Event Alerts**.

Deleting Files from Quarantine Automatically

You can configure a global setting that will delete quarantined files on endpoints after a specified number of days.

Prerequisites:

- Ensure the latest version of the AntiVirus definition file is installed on endpoints, as it may contain the definition required to clean the threat detected.
- Monitor endpoints for behavior that indicates a quarantined file is needed by a program to function, requiring that a replacement file be obtained.
- Consider submitting quarantined files to Ivanti for further analysis. It may be a new virus or a variant of an existing one.
- Ensure files have been in quarantine for at least 30 AntiVirus days. Updates occur several times daily. Files in quarantine are automatically scanned upon update and if cleaned are moved back to their original location.

1. Select **Tools** > **Options**.
2. Click the AntiVirus tab.
3. Select **Enable the automatic deletion of files from Quarantine**.
4. In the **Delete from quarantine after** field, enter the quarantine age of files to be automatically deleted in days.

   1 to 60 days from the date a file was quarantined can be entered. Default: 30 days.

5. Click **Save**.

Result: Quarantined files will now be deleted from endpoints when their age surpasses the number of days you entered.

Centralized Quarantine

Use this page to centrally view and manage all infected and suspicious files quarantined on endpoints in your environment that cannot be cleaned or deleted at time of detection

Scan Now	Launches the ***Scan Now -Virus and Malware Scan*** wizard. Ensure the latest version of the definition file is installed on the endpoint, as it may contain the definition required to clean the threat detected. Expand the section to view the ***AV Definition Detected*** column.
Delete	Deletes selected files from the quarantine on the endpoints. Occasionally the damage caused by a virus renders a file unable to be cleaned and must be deleted. If the file is required to regain the functionality of a program, recover it from a back-up or obtain a copy from a trustworthy source, like the vendor.
Restore	Restores selected files and click to . The only files you should restore are those for which no back-up exists or no copy can be obtained from a trustworthy source, like a vendor. It can be a file that contains important information (for example, a document) or is required to regain the functionality of a program that needs the file to run.

Important: Before you Delete or Restore a file:

- Monitor the endpoint for behavior that indicates the quarantined file is needed by a program to function, requiring that a replacement file be obtained.
- Ensure the latest version of the definition file is installed on the endpoint, as it may contain the definition required to clean the threat detected. Expand the section to view the ***AV Definition Detected*** column.
- Consider submitting the quarantined file you want to restore for further analysis. It may be a new virus or a variant of an existing one.

Table 59: Main Table Columns

Column	Description
File Name	Name of the file AntiVirus has quarantined
Virus/Malware Name	Name of the Virus or Malware detected in the file.

Column	Description
Last Detection date (server)	Point in time when the latest file of this type was detected in your environment.
Endpoints Affected	Number of endpoints in your environment where this file is infected.

Table 60: File Details Columns

Column	Description
Endpoints	Name of the endpoint with the quarantined file. Click the hyperlink for more details.
IP Address	IP address of the endpoint with the quarantined file.
AV Definition Detected	Version number of the AV definition file installed on the endpoint.
Status	The current status of the quarantined file. The status will be pending when you the system is in the process of deleting or restoring the file from endpoints.
File Path	Path of the location on the endpoint where the file was originally before it was moved to quarantine.
Detection Date	Point in time when the file was scanned using the latest AntiVirus definition file.
SHA-256 Hash	Unique hash assigned to quarantined infected file. SHA-256 is a cryptographic hash function with a 256-bit hash value, typically expressed as a 64 digit hexadecimal number.

Chapter 10

Reporting

In this chapter:

- About Antivirus Reports
- The Antivirus Reports Page
- Generating an AntiVirus Definition Version Status Report
- Generating an Endpoint/Groups with Infections by Date Report

Ivanti AntiVirus can generate reports summarizing the status of antivirus activity.

Two report types are available. One details the versions of the antivirus definition files that are in use, while the other lists the endpoints infected with viruses or malware over a specified time period.

When generating a report you can specify parameters and options to target specific endpoints and groups, if required.

About Antivirus Reports

Ivanti AntiVirus provided two types of antivirus report: *AntiVirus Definition Version Status* and *Endpoint/Groups with Infections by Date*.

AntiVirus Definition Version Status	Returns a detailed list of current antivirus definition versions for specified devices and groups. This helps you determine if the antivirus definitions are up-to-date.
Endpoint/Groups with Infections by Date	Returns a list of endpoints and/or groups infected with viruses and other malware over a custom date selection. This gives a historic overview of virus/malware activity in the network.

The Antivirus Reports Page

All available reports are generated from the ***All Reports*** page. From this page, you select an antivirus report type and define the report parameters and options.

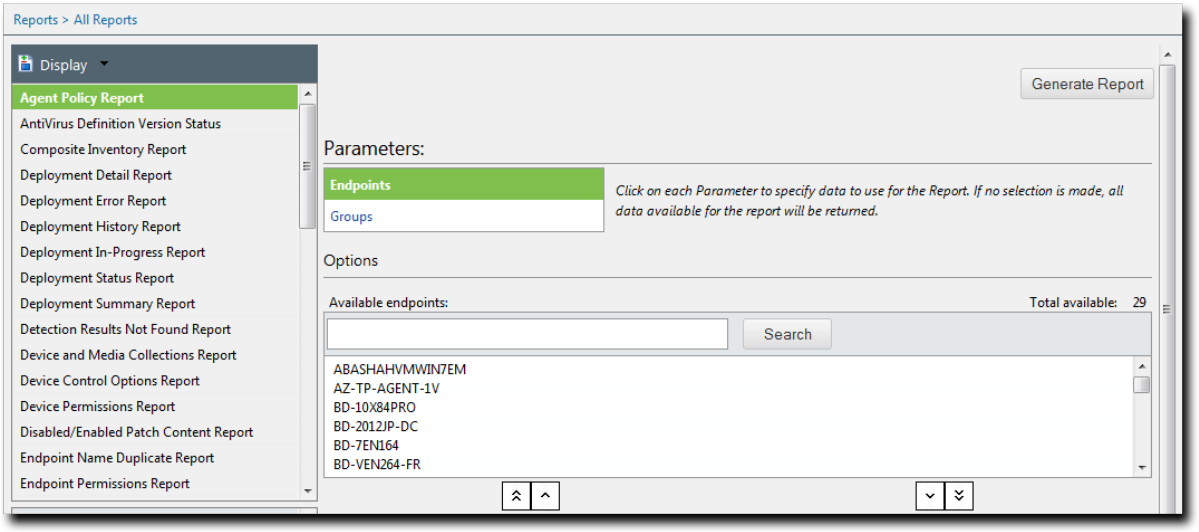


Figure 40: AntiVirus Reports Page

The **Display** list shows all the reports that can be generated. Expanding the **AntiVirus** heading displays the reports associated with antivirus activities:

- AntiVirus Definition Version Status
- Endpoint/Groups with Infections by Date

The report description provides a brief overview of the report type that is selected, along with its type, category, and format.

The **Parameters** list specifies the data to use for the report. Both antivirus reports have **Endpoints** and **Groups** parameters. In addition, the *Endpoint/Groups with Infections by Date* report has a **Date Range** parameter.

There are two **Generate Report** buttons. They both produce the same output.

The **Options** section enables you to refine the Endpoints and Groups parameter selection. It contains the following:

Search field and button

Available list

Selected list

Buttons to move entries between the Available and Selected lists.

- The double up-arrow button moves all entries in the Selected list up to the Available list.
- The single up-arrow button moves highlighted entries in the Selected list up to the Available list.
- The single down-arrow button moves highlighted entries in the Available list down to the Selected list.
- The double down-arrow button moves all entries in the Available list down to the Available list.

Setting Parameters and Options

In AntiVirus, you can set Endpoint and Group parameters to specify the data used in reports.

Because many networks contain large numbers of endpoints, you may want to limit the scope of a report to specific endpoints and/or groups. You can do this by setting the Endpoints and Groups parameters and their respective options.

Note: The Endpoint/Groups with Infections by Date report has a third parameter called *Date Range*. For information on using this parameter, see Generating an Endpoint/Groups with Infections by Date Report on page 198.

1. If you want to limit the report to certain endpoints, select the **Endpoints** parameter.

   Step Result: The **Available endpoints** list is populated with all available endpoints.

2. If necessary, find the required endpoint(s) by entering a full or partial endpoint name in the Search field and clicking the **Search** button.
3. Select the required endpoint(s) and click the single down-arrow button (⌄).

   Tip: You can move all the endpoints in the **Available endpoints** list by clicking the double down-arrow button (⌄⌄).

   Step Result: The selected endpoints are moved to the **Selected endpoints** list.

4. If you want to limit the report to certain groups, select the **Groups** parameter.

   Step Result: The **Available groups** list is populated with all available groups.

5. If necessary, find the required group(s) by entering a full or partial group name in the Search field and clicking the **Search** button.
6. Select the required group(s) and click the single down-arrow button (⌄).

   Tip: You can move all the groups in the **Available groups** list by clicking the double down-arrow button (⌄⌄).

   Step Result: The selected groups are moved to the **Selected groups** list.

7. When all the required endpoints and/or groups have been selected, click **Generate Report**.

Note: Your browser may block the pop-up window containing the generated report from displaying. Consult your browser's help to temporarily allow the pop-up, permanently allow the Ivanti Endpoint Security URL, or disable the pop-up blocker.

Generating an AntiVirus Definition Version Status Report

The AntiVirus Definition Version Status report allows you to review the current antivirus definition versions for an entire network or specific endpoints and groups.

It is important that you maintain up-to-date virus definitions for all the endpoints on the network.

1. Select **Reports** > **AntiVirus**.

   Step Result: The ***All Reports*** page opens with the **AntiVirus** section expanded.

2. Select **AntiVirus Definition Version Status**.
3. (Optional) Set parameters to narrow the report's scope:
   a) In the **Parameters** section, choose **Endpoints** or **Groups**.

      Step Result: Available options for the selected parameter are displayed in the **Options** section.

   b) Specify options you want to include in your report.

      Tip: Press `Ctrl` to select multiple options in the list.

   c) Click the single down-arrow.

      Step Result: The options you specified move to the **Selected** pane.

4. Click **Generate Report**.

Result: You have generated an AntiVirus Definition Version Status report in HTML format.

After Completing This Task:
You can now:

- Export the report to CVS, XLS, or XML format.
- Print the report by selecting **Printer-friendly Version** and using your Web browser's print functionality.

Generating an Endpoint/Groups with Infections by Date Report

The Endpoint/Groups with Infections by Date report allows you to analyze endpoints and groups infected with malware over a custom date range.

Use this report to determine where a malware infection started and how it spread through the network.

1. Select **Reports** > **AntiVirus**.

   Step Result: The ***All Reports*** page opens with the **AntiVirus** section expanded.

2. Select **Endpoint/Groups with Infections by Date**.
3. (Optional) Set parameters to narrow the report's scope:

Parameter	Steps
`Endpoints` **or** `Groups`	1. In the **Parameters** section, choose **Endpoints** or **Groups**. Available options for the selected parameter are displayed in the **Options** section. 2. Specify options you want to include in your report. **Tip:** Press `Ctrl` to select multiple options in the list. 3. Click the single down-arrow. The options you specified move to the **Selected** pane.
`Date Range`	1. In the **Parameters** section, choose **Date Range**. Calendar and Time controls are displayed. 2. Specify the start and end dates and times of the report period. **Remember:** You can create reports only for the past.

4. Click **Generate Report**.

Result: You have generated an Endpoint/Groups with Infections by Date report in HTML format.

After Completing This Task:
You can now:

- Export the report to CVS, XLS, or XML format.
- Print the report by selecting **Printer-friendly Version** and using your Web browser's print functionality.