ivanti

Endpoint Security

powered by HEAT Software

AntiVirus Best Practice Guide

Dec 2020

Contents

Introduction

The Ivanti Endpoint Security AntiVirus module provides protection against known malware using signature-based detection combined with behavioral analysis, including Sandbox technology to provide protection against unknown malware.

This document provides a best practice workflow to act as a guide for administrators when implementing AntiVirus.

Following the workflow outlined in this document should help to ensure a successful deployment and ongoing virus and malware protection.

What Does AntiVirus Do?

AntiVirus blocks known malware and provides protection against unknown malware without impacting productivity. AntiVirus examines executable files and employs the following capabilities to provide a multi-layered defense against existing and new malware:

- Full signature matching, also known as blacklisting, to recognize, block and remove known malware. Signature updates are made available twice daily to ensure that protection against the latest known malware is always available.
- DNA matching or partial signature matching to recognize, block and remove unknown malware and new variants of known malware based on inherited or re-used malware code fragments.
- Exploit detection to recognize, block and remove malware hidden or embedded in seemingly innocent files.
- Behavioral detection using SandBox technology which allows code to execute in an emulated environment and block and removes it if it exhibits malicious behavior.

Policies are defined on the Endpoint Security console to define the actions taken by the AntiVirus engine on the endpoint. The following policy types are available:

- Real-Time Monitoring: This policy defines the actions taken by the engine when files are opened, moved or copied.
- Recurring Scan: This policy defines the frequency at which full or partial disk scans are conducted to remove any dormant malware from the endpoints.
- Scan Now: This is a one-time scan which would typically be performed when AntiVirus is initially introduced, in the case of a suspected outbreak or prior to going into lock-down if deploying Ivanti Application Control.

If malware is detected on the endpoint, the AntiVirus engine will initially attempt to clean the malware and if it is unable to clean it, depending on the policy settings, it will either quarantine or delete the file. The endpoint will also send an alert to the server so that the administrator becomes aware of the incident and can take action, if necessary.

If the AntiVirus engine has been unable to clean the malware, the administrator can submit the file to Ivanti support for further analysis.

Overview

The recommended workflow can be summarized as follows:

1. "Phase 1: Prepare Your Infrastructure" on the next page

   Steps to be taken to prepare for the introduction of AntiVirus.

2. "Phase 2: Discover" on page 14

   Scan endpoints to identify if any known malware is present and clean, quarantine or delete the infected files as appropriate.

3. "Phase 3: Remediate" on page 18

   For files that have not been automatically cleaned, review alerts on the console to identify which endpoints need further action and what malware is present on those endpoints.

4. "Phase 4: Monitor" on page 20

   Create real-time and recurring scan policies to provide ongoing protection against known malware.

5. "Phase 5: Manage" on page 25

   Leverage reports, widgets, email notifications and other information provided by the Endpoint Security console to manage the AntiVirus module on an ongoing basis and understand if endpoints are getting infected or if a malware outbreak is occurring.

6. "Phase 6: Recover" on page 28

   In the event that an endpoint has experienced one or more false positives, take steps to restore clean files to their correct locations.

This workflow is discussed in greater detail in the remainder of this document. You should go through the entire workflow for a small number of endpoints / test group before rolling out to remaining endpoints.

In addition to following this workflow, you should also develop a recovery plan in the event that widespread infections occur. If it does not already exist you should also develop a support escalation plan so that users will be able to report if malware infections or false positives have occurred on their endpoints. Finally, you will also need to train your IT Help Desk team to deal with such escalations.

Phase 1: Prepare Your Infrastructure

Prior to introducing AntiVirus, you will need to take steps to ensure that the rollout is successful and that both the initial deployment and the ongoing definition and engine updates do not adversely impact on your overall network bandwidth and cause communication difficulties between office locations.

In this phase you will:

1. "Remove Existing/Previous AntiVirus Solution" below

   Ensure that any other vendor's AntiVirus solution is fully removed prior to installing AntiVirus.

2. "Deploy Caching Proxy Servers" on page 7

   Review your network topology to identify where caching proxy servers should be located to act as distribution points for AntiVirus definition and engine updates.

3. "Control AntiVirus Definition Distribution" on page 8

   Identify the strategy to be followed when rolling out new AntiVirus engine and definition updates to ensure that they get rolled out in a controlled manner and define the distribution groups to align with this strategy.

4. "Obtain AntiVirus Updates for Disconnected Endpoints" on page 9

   Set up a caching proxy server so that endpoints can still receive AntiVirus definition and engine updates when they are disconnected from the corporate network.

This phase is key to ensuring a successful and problem-free rollout of AntiVirus, so ensure that you take the time to lay the groundwork before proceeding to rollout on a large scale.

Remove Existing/Previous AntiVirus Solution

Having multiple antivirus products installed on the same endpoint is not a good practice and could cause issues such as:

- Endpoint becomes unstable or unusable.
- End users are disrupted and productivity decreases.

AntiVirus does not include inbuilt AntiVirus removal tools. However, customers can leverage the Endpoint Security capabilities to deploy an AntiVirus uninstall package to each endpoint to remove the old AntiVirus solution and clean up any residual files. It is important to minimize the protection gap – the gap that occurs between disabling or removing one AntiVirus solution and adding another. This section outlines the recommended steps to plan your migration strategy and minimize the risk of leaving an endpoint unprotected.

Before you begin removing AntiVirus:

1. Review the Previous AntiVirus Vendor's recommendations and best practices for uninstalling their security technologies.
2. Prior to planning your migration from the previous AntiVirus Vendor to Ivanti, make sure your Endpoint Security Server is licensed for the following products:
    - Patch and Remediation
    - AntiVirus
    - Content Wizard

AntiVirus Replacement Steps:

1. Create the <Previous AntiVirus vendor> Uninstall Package

    Use the Ivanti Content Wizard to create a package that detects and removes the previous AntiVirus vendor from your endpoints. When you create the package, make sure the content has the reboot flag to force a restart of the endpoint which should put the endpoint in a clean state.

    The properties of the package should contain the following attributes:

    - Applicable to only endpoints with <Previous AntiVirus Vendor> products installed.
    - Reboot Flag to restart the endpoint when <Previous AntiVirus Vendor> products have been uninstalled.

    Once the previous AntiVirus vendor uninstall package has been created, run the package in your lab to verify the correct uninstall behavior and expected outcome.
2. Add excludes to the <Previous AntiVirus vendor> AntiVirus policies for the Ivanti folders which will exist once AntiVirus is installed (C:\ProgramData\HEAT Software\ and C:\Program Files\HEAT Software\). This will help avoid potential conflicts while AntiVirus is being installed. Testing will need to be done to ensure there aren't any other features in <Previous AntiVirus vendor> which might otherwise block the install of AntiVirus.
3. Create groups to minimize the impact of rolling out AntiVirus. Assuming Ivanti Patch and Remediation is being used, you can leverage FastPath proxy servers at remote locations to seed the proxies with the install package. Using proxies and/or group-based rollout is necessary to avoid an AntiVirus storm on install when rolling out to large numbers of endpoints across the network. Do this out of hours where possible.
4. Install AntiVirus to groups in a controlled manner to minimize network bandwidth utilization issues. AntiVirus will be installed with no AntiVirus policies enabled. Work around any Windows Security Center notification issues.
5. Create AntiVirus real-time monitoring policy but do not assign it. Add recommended excludes as per Excluding files, folders and processes from AV scans knowledge article. Also, exclude <Previous AntiVirus vendor> directories if required.

6. Disable <Previous AntiVirus vendor> AntiVirus on-access policy. Endpoints are now unprotected.
7. Assign AntiVirus real-time monitoring policy to groups that have <Previous AntiVirus vendor> on-access policy disabled. Endpoints are now protected.
8. Deploy your <Previous AntiVirus vendor> uninstall package including reboot to remove <Previous AntiVirus vendor> and clean up any residual files.

   Monitor the deployment to the group by leveraging the Manage > Deployment and Tasks page in the Endpoint Security Console to track status of the deployment.
9. Remove the <Previous AntiVirus vendor> excludes from the AntiVirus real-time monitoring policy as it is no longer required and is a potential security hole.

Deploy Caching Proxy Servers

AntiVirus definitions get distributed approximately twice per day and must be downloaded to each endpoint so that they remain updated and can detect the latest known malware. Unless planned for, these updates can place a significant load on the corporate network and could cause delays to occur on interoffice business communications.

The base definition file of AntiVirus definitions is approximately 400MB in size. This file is distributed on initial install and is also redistributed occasionally (e.g. when the AntiVirus engine is updated). In addition the twice daily incremental update file can range from ~1MB to ~15MB in size. The network infrastructure needs to be designed to cater for distribution of these files to all endpoints.

Where network infrastructure supports it, QoS settings can be used to deprioritize AntiVirus definition and engine updates vs other corporate critical communications. However, for a distributed enterprise environment, caching proxies such as the Ivanti Caching Proxy may be leveraged to assist in conserving WAN/LAN bandwidth during mass deployments through Endpoint Security.

A cache server is a dedicated network server or service acting as a server that saves Web pages or other Internet content locally. By placing previously requested information in temporary storage, or cache, a cache server both speeds up access to data and reduces demand on an enterprise's bandwidth. When an agent is configured to utilize a caching proxy, deployments sent to an agent will be cached by the caching proxy. This allows other agents to be given the cached payload from the caching proxy instead of the storage repository on the Endpoint Security Server, saving bandwidth between the caching proxy location and the Endpoint Security Server, while significantly increasing performance.

Ivanti Patch and Remediation includes FastPath which allows an administrator to assign caching proxies to specific groups of agents through a policy instead of assigning a proxy manually through the Agent Control Panel or during the installation of the agent. It is designed to provide backup caching proxies in case of a failure of the primary caching proxy.

For additional information, please consult the Ivanti Caching Proxy Setup Guide.

Control AntiVirus Definition Distribution

When new AntiVirus definitions or engine files become available, the Endpoint Security Server notifies all endpoints that updated files are available and, assuming they are online, endpoints will check-in and download the new files.

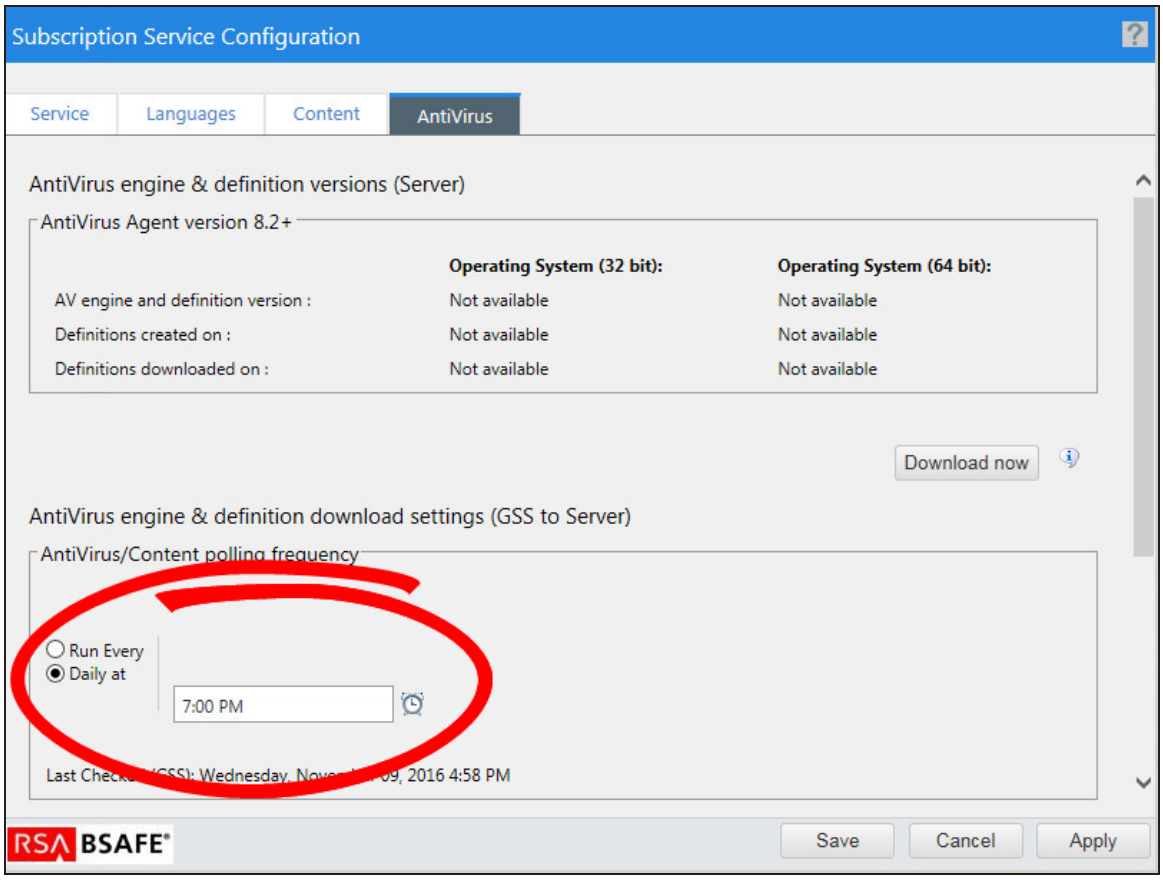
It is possible, however, to stagger definitions distribution so that all endpoints don't try to retrieve them simultaneously. There are a few reasons why you might want to do this:

- Provide an opportunity for caching proxies to get the new files first (seed the proxies) so that other endpoints at that location will obtain the files from there instead of pulling them across the network. To achieve this, create a group with a couple of endpoints (that are always online) from each location where a proxy has been added.
- If you want to test new definitions with a test group prior to rolling the definitions out to the general population. Create a group containing the test endpoints (which could also include the "caching proxy" endpoints above) which will receive the definitions immediately as soon as they are available on the server. Create another group for the general population to receive the definitions some time later. You could also create a third group for corporate critical servers which would receive the definitions after the general population.
- If you need to alleviate the impact on virtual infrastructures that are sensitive to increases in network latency during AntiVirus Definition distribution.

To apply different delays to these groups, use the "Delay AntiVirus definition distribution" setting in the Agent Policy sets. The default delay is 0. Change this value in the Global Agent Policy set to whatever delay you want to for the general population (e.g. 4 hours). Create a zero delay agent policy set (with the delay set to 0) and apply this policy set to the test group or cache proxy servers group. Create a critical server policy set (with the delay set to a figure greater than the general population (e.g. 8 hours). The maximum delay value that can be applied is 72 hours.

Remember that endpoints remain unprotected from new known malware until they receive the latest AntiVirus definitions so you should minimize any delay in getting definitions to the endpoints to ensure the best protection is available.

An additional option is available to achieve greater predictability for AntiVirus definition distribution and prevent definitions from being made available for distribution during business hours. On the Endpoint Security Server (see screen shot below), you can set the AntiVirus Subscription Service download time from GSS to Server. This allows the Administrator to control when AntiVirus definitions and engine are downloaded to the Endpoint Security Server which acts as the starting point for the subsequent delivery to endpoints.



Obtain AntiVirus Updates for Disconnected Endpoints

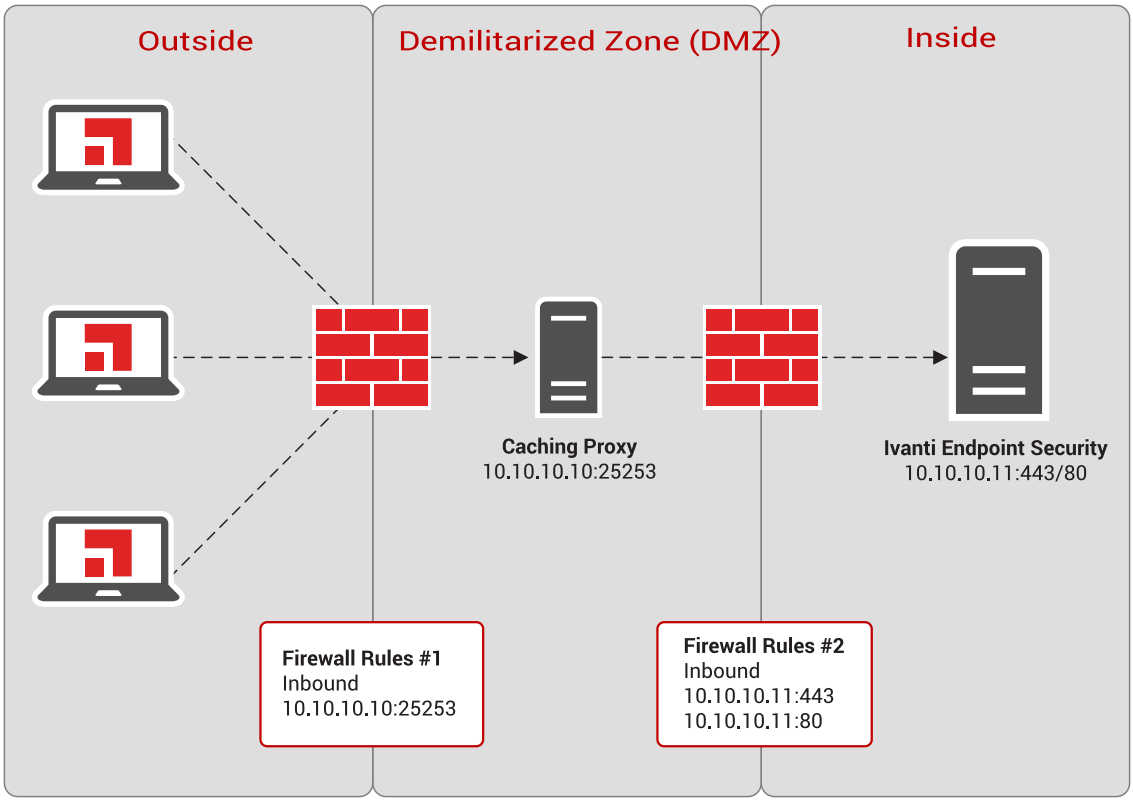
Endpoints obtain AntiVirus definition and engine updates from the Endpoint Security Server. As this server is not accessible outside of the corporate network, endpoints will generally only receive updates when they are connected to the network, either in a corporate office or connected via VPN.

However, it is possible to leverage HTTPS and HTTP protocols which allows IT Administrators to easily manage endpoints over the intranet and internet (no VPN tunnel required).

This section will guide IT Administrators on how to distribute AntiVirus Definitions to endpoints over the internet without publishing or exposing the Endpoint Security Server to the internet.

Network Diagram

The diagram below provides a high level overview on how the solution will work. In this example, there will be two static IP Addresses:



- 10.10.10.10 – IP Address for Ivanti Caching Proxy.
- 10.10.10.11 – IP Address for the Endpoint Security Server.

Steps

1. Install a Ivanti Caching Proxy inside your demilitarized zone (DMZ)

   The goal is to designate a caching server that will act as a "middle-man" between the Endpoint Security Server and managed endpoints. Ivanti recommends leveraging your existing caching solution that is internet facing or install the Ivanti Caching Proxy.

   Installing a caching proxy will also reduce the workload on the Endpoint Security Server during large deployments or security update rollouts.

2. Create Firewall Rule

   Create a firewall rule that allows the static IP Address for the Caching Proxy inbound access to the Endpoint Security Server. These rules are going to be explicit to allow TCP traffic from the Caching Proxy inside your DMZ to the Endpoint Security Server that is inside your enterprise network. See table below on recommended rules.

Direction	TCP Port Number	Description
Inbound	25253	This is the default port number for the Ivanti Caching Proxy.
Inbound	443	This is the default port number for the Endpoint Security Agent and is used for basic communication.
Inbound	80	This is the default port number for the Endpoint Security Agent and is used for http downloads.

   Test these firewall rules from outside the enterprise network to make sure proper connectivity is allowed to the Endpoint Security Server address.

3. Create Agent Policy for Mobile Computers

   In this task, we need to create a dedicated policy for your mobile computers so we can activate the FastPath Servers feature. This feature will configure the Agent to communicate to the Caching Proxy when the computer is not connected to the enterprise network.

   a. Log onto the Endpoint Security Console. Select Manage > Agent Policy Sets. Click the create button to create a new agent policy.

   b. Name the policy Mobile Computer Policy.

   c. Under FastPath Servers section, click the modify button to define the values.

   d. Add the following URLs to this page:

Address	Port	Description
http://10.10.10.10	25253	This setting will auto configure the Endpoint Security Agent to communicate with a Caching Server located inside the DMZ. Ivanti recommends using a DNS Record for 10.10.10.10 IP Address.
http://10.10.10.11	80	This setting will auto configure the Endpoint Security Agent to communicate to the Endpoint Security Server when the laptop is connected to the enterprise network.

   e. Configure the Interval to 60 minutes and click save.

4. Create a new Custom Group for Mobile Computers.

   We need to create a new group for your Mobile Computers so we can assign the Mobile Computer Policy with the FastPath Server settings.

   a. Select Manage > Groups. Right-click Custom Group and select create group.

   b. For the Group Name, type Mobile Computers Group and click save.

   c. Change the view settings to Endpoint Membership and add at least a single endpoint to the group so we can test the settings.

   d. Change the view setting to Agent Policy Sets and assign the Mobile Computer Policy to the Mobile Computer Group. This will assign the FastPath settings to all members of the Mobile Computer Group.

5. Test the settings

   If possible, if you have a Guest Wi-Fi Router that does not have access to the enterprise network, configure the computer to connect to the Guest Wi-Fi. Make sure this computer is the same computer is that a member of the Mobile Computers Group.

   If you leverage Squid Proxy Server or our Ivanti Caching Proxy as your caching appliance you can monitor the traffic by review the access.log located in <installpath>\ CachingProxy\var\logs.

6. Add all mobile computers to the Mobile Computers Group

   Once you are satisfied with the testing results, now you can add all of your mobile computers being managed by the Endpoint Security Server to the Mobile Computers Group. This will activate the FastPath Settings and now you can manage endpoints over the Internet with the Endpoint Security Server being inside enterprise network.

Phase 1: Recap

This phase is used to prepare the environment for the introduction of AntiVirus and to ensure that the AntiVirus rollout is successful. Distribution of the initial AntiVirus module along with on-going AntiVirus definition and engine updates consume network bandwidth and it is important to ensure that the network has been designed to handle this traffic / traffic pattern as otherwise it could impact business productivity. Implementations differ from one vendor to another so you should not simply assume that because you already had an AntiVirus solution in place already that this preparation phase is not required.

If replacing an existing AntiVirus solution, you also need to ensure that the existing solution gets removed prior to enabling AntiVirus while ensuring that you minimize the protection gap when neither AntiVirus solution is enabled.

You can configure your AntiVirus definition distribution so that it minimizes any impacts to the network and end-users, and provides a test window if required.

You can also configure your network so that endpoints continue to receive AntiVirus definitions when endpoints are disconnected from the corporate network.

At the end of this phase the AntiVirus module should be installed on some or all endpoints and you can now proceed to the next phase.

Phase 2: Discover

In the discovery phase, endpoints are scanned to identify any dormant, known malware and remove it from the endpoints.

1. "Schedule Scan" below

   Conduct a thorough AntiVirus scan to remove any dormant malware on your endpoints.
2. Schedule the scan to execute out of hours, where possible, to minimize any productivity impact.
3. Communicate with your users so they understand why this scan is being performed.
4. "Review Scan Progress" on the next page

   Use the Deployments & Tasks page to understand when the Scan Task has completed.
5. Use Custom Scan to assess external drives.

In this section we describe how you would scan your endpoints using AntiVirus. As this is the very first time these endpoints are being scanned with AntiVirus, the recommendation is to perform a thorough scan to ensure that any dormant malware (e.g., malware buried within archives) is identified and removed.

A thorough AntiVirus scan could take an extensive amount of time to complete so you should schedule the scan to execute out of hours, if possible, to minimize any user disruption. If the scan is executed during working hours, ensure that you communicate with the affected users so that they are aware of what is happening.

Schedule Scan

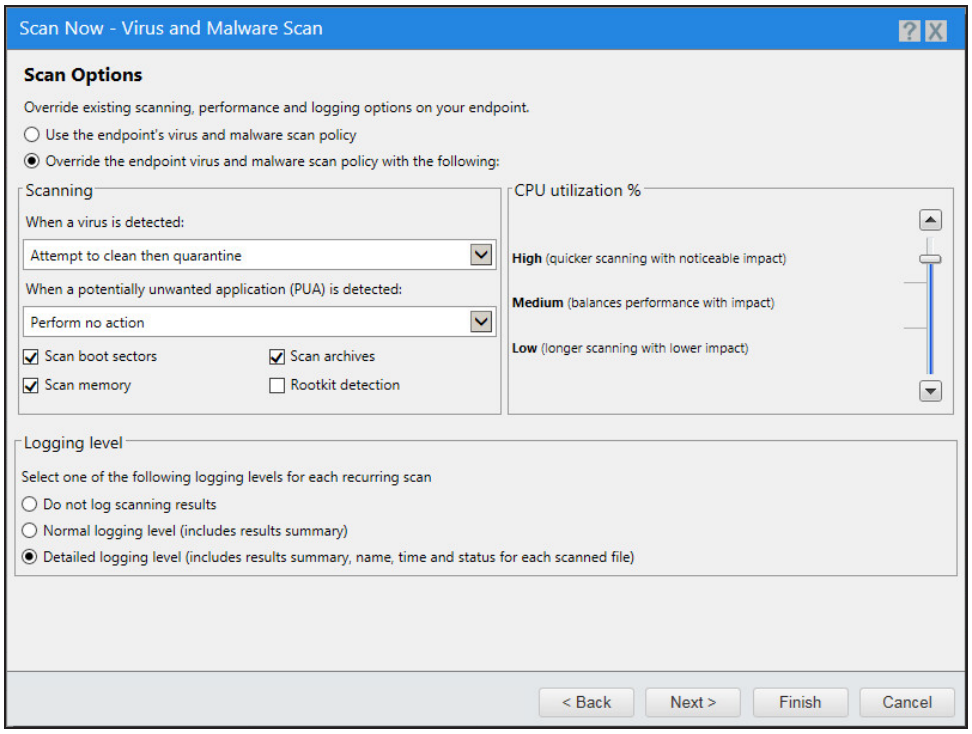
In addition to being able to run the scan immediately, it is also possible to schedule the scan to run at a later date & time. Note, however, that the scan will always be scheduled in server time. If there are endpoints in different time zones and you want the scan to occur at a specific time in that time zone, you will need to create a specific Scan Now task for the group of endpoints at that location and schedule it based on the appropriate offset from server time.

Scanning Offline Endpoints

The recurring AntiVirus scan schedule is controlled by an endpoint scheduler. So long as the recurring scan policy has been delivered to the endpoint, the scan will execute at the appointed time so long as the endpoint is powered up at that time. The endpoint does not need to be online at the time the scan is due to execute.

Scan Options

To implement a thorough AntiVirus scan using AntiVirus, conduct a “Scan Now – Virus and Malware Scan” and select all the scanning options including Archive scan as shown below.



CPU Utilization

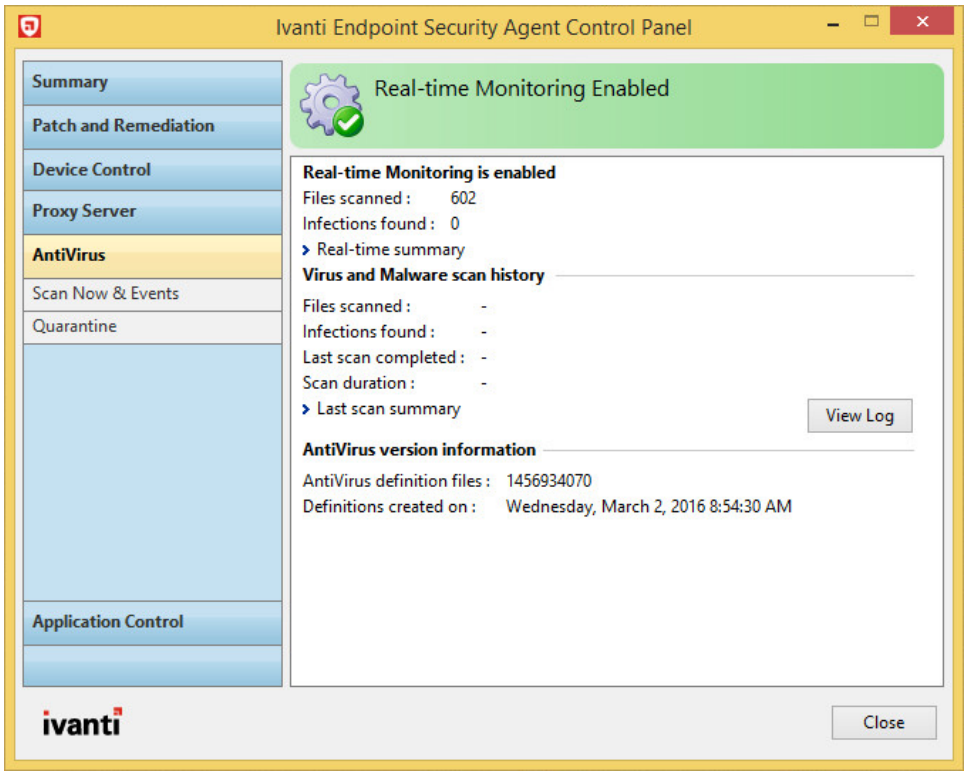
The Scan Wizard contains a CPU utilization control which can be used to determine how much CPU gets consumed when the scan is being performed. If the scan is being performed out of hours, select the high CPU utilization setting which will cause the scan to use as much CPU as possible so that the scan completes more quickly. However, if the scan is being performed during business hours, you should select a medium or low CPU utilization level. This will cause the scan to take longer but the scan will have less of an impact on the user.

Review Scan Progress

Once a Scan Now has been initiated, you can observe the scan progress on the Deployments & Tasks page. This will help you to understand when the scans have been completed across all of the endpoints.

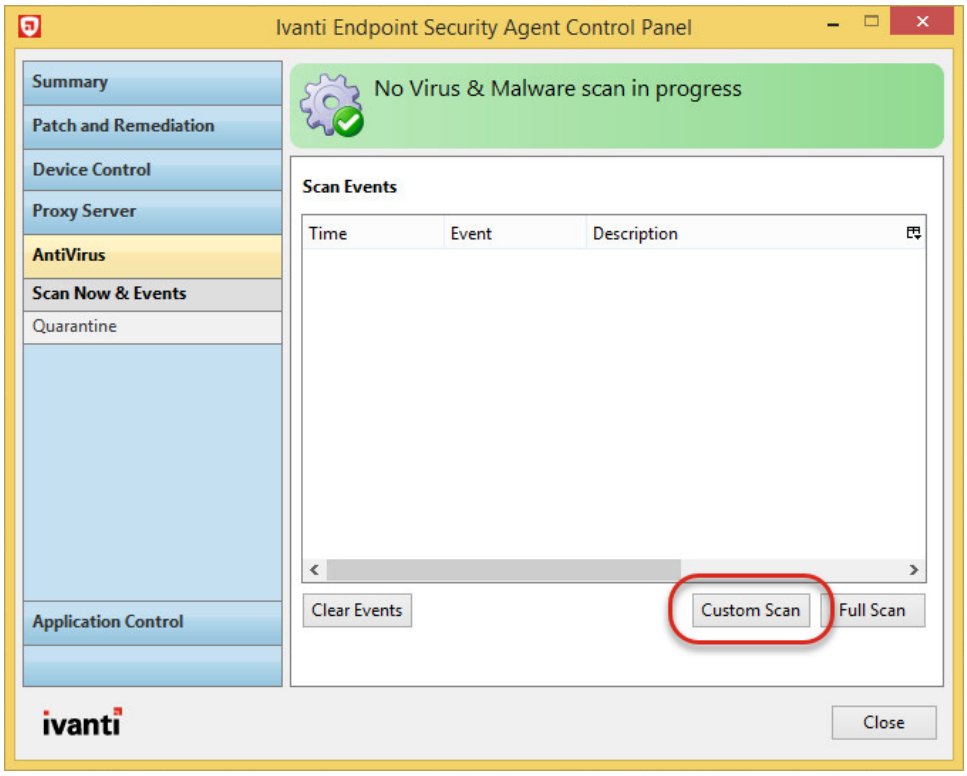
View Scan progress on the Endpoint

When an AntiVirus scan is running, you can view the progress of the scan via the AntiVirus tab on the Agent Control Panel. If a scan has been conducted previously, this tab will show the number of files scanned and the scan duration. If this is a recurring scan and there hasn't been much change on the endpoint, the number of files and duration should be similar to previous scans. You can monitor the progress as the number of files scanned will increment as the scan progresses.



Custom Scan

There may be a certain directory, external drive or individual file on an endpoint that you'd like to scan without having to do a full system scan to save time. The Custom Scan on the endpoint can be used to scan a USB drive before opening any files on the external media.



Clicking on "Custom Scan" will present the user with a list of all available drives which can then be used to navigate and drill down to the individual file(s) and/or folder(s) you intend to scan (both internal or external drives, but not network drives)

Phase 2: Recap

Conduct a thorough scan of your endpoints to identify and remove any dormant malware prior to creating AntiVirus policies for on-going management.

Schedule the scan to run out of hours where possible. If this is not possible, select a lower CPU utilization setting to minimize the impact on end users and communicate with your end users so they understand why these scans are being performed.

View scan progress on the server via the Deployments & Tasks page or via the Agent Control Panel on the endpoint.

Use Custom Scan on the endpoint to perform targeted scans for files, directories or external drives.

At the end of this phase, all endpoints will have been scanned using the AntiVirus scan engine and all known malware will have been identified and removed, where possible. If further remediation is required, this will be tackled in the next phase.

Phase 3: Remediate

In the remediate phase, alerts from the endpoints are reviewed to identify any endpoints that need to be remediated.

In this phase you will:

1. "Review Alerts" below

   Review alerts on the Centralized Alerts page.

2. "Identify Alerts" below

   Identify alerts and the associated endpoints that need further action.

3. "Malware Cleaner" on the next page

   Obtain tool to remediate 'not cleaned' detections.

4. "Submit Files for Analysis" on the next page

   Submit files to Ivanti Support for further analysis.

Review Alerts

When endpoints identify malware, they create alerts which are sent back to the Endpoint Security Server. If the AntiVirus engine has identified malware on the endpoints and has been unable to clean it, alerts are sent up the server immediately as prompt action may be required. However, if the engine has already cleaned and/or has quarantined the file or deleted the file, the AntiVirus module waits until the scan has been completed before sending up the alerts. This is done to minimize the number of messages being sent for unimportant events.

When the alerts are returned to the server, they can be viewed on the Centralized Alerts page. On this page, the endpoints are grouped into categories of:

- Not Cleaned
- Quarantined
- Cleaned
- Deleted

Identify Alerts

Files which are Not Cleaned are still active on the endpoints and additional remediation is required to remove this malware and stop it from being spread throughout your environment.

Files which are quarantined may also require additional attention. Once a file has been quarantined it will no longer be allowed to execute or, if this file is part of an application, that application may be blocked from executing or may execute with errors. The file has been quarantined because the engine was unable to clean it directly so additional steps may be required to clean the file so that it can be restored. The file can be submitted to Ivanti Support for further analysis.

Malware Cleaner

While Ivanti does not provide standalone Malware Cleaners, these tools can be obtained from other vendors such as MalwareBytes. In the event that AntiVirus has identified malware but is unable to remediate it directly, a first step is to use these tools to try and clean any infected endpoints.

Submit Files for Analysis

It is recommended that you submit suspect files via Ivanti Support so that progress on the analysis can be tracked and, in the event that it is a false positive rather than a malicious file, the false positive can be addressed with the next set of AntiVirus definitions and the file gets automatically restored.

Phase 3: Recap

When the AntiVirusscans have completed, you can identify which endpoints require additional remediation using the Centralized Alerts page. You can also submit suspect files for additional analysis.

Once this phase is completed, all endpoints should now be in a “known good” state in that they are free of known malware.

Phase 4: Monitor

In the monitor phase, real-time and recurring scan policies are created to provide ongoing malware protection.

In this phase you will:

1. "Create Real-Time Monitoring Policy" below

   Create real-time monitoring policies to provide protection every time files are opened or executed.

2. "Add/Import Exclusions" on page 22

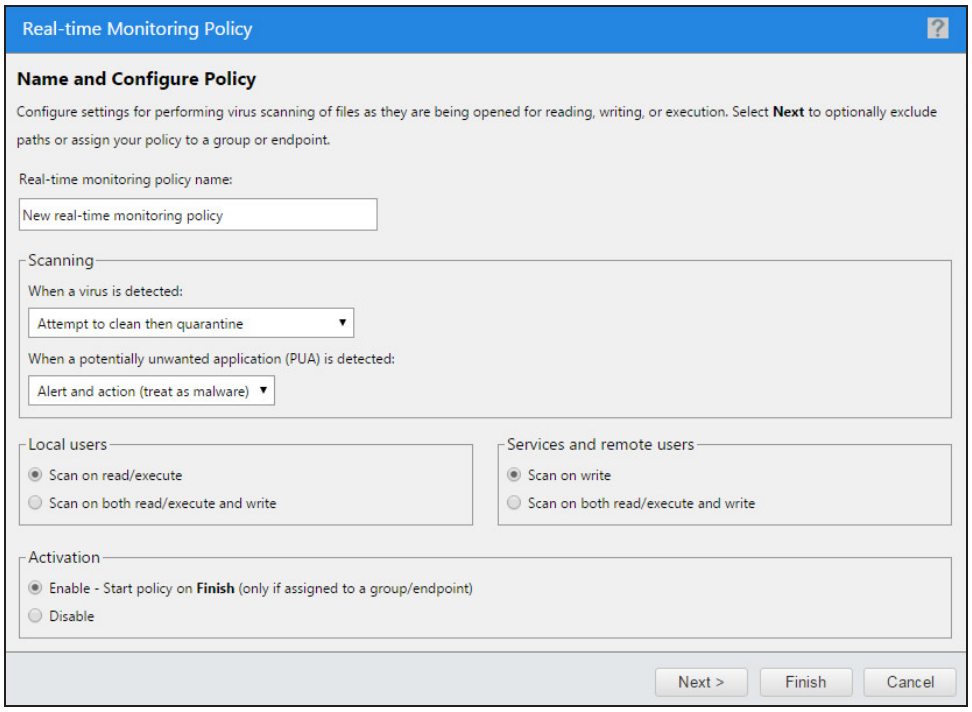
   Add or import files or file paths to be excluded from the AntiVirus scan to reduce the performance impact associated with scanning for malware.

3. "Create a Recurring Virus and Malware Scan Policy" on page 22

   Create recurring scan policies to scan for malware on a scheduled basis.

Create Real-Time Monitoring Policy

Real-time monitoring policies can be assigned to endpoints or groups and provide protection every time a file is opened or executed. There are a number of default policy settings as shown below and these should be left unchanged unless there is a specific reason to select alternative settings.



Scanning Options

When a virus is detected, the default behavior is to attempt to clean the file but, if the AntiVirus engine is unable to clean it, to move it into quarantine for further action. Other actions can be selected including:

- Perform no action
- Attempt to clean then delete
- Attempt to clean then quarantine then delete

The option to perform no action might be selected to prevent critical files from being moved to quarantine which might render the system unusable. In such cases, an alert would be sent up to the server. This option should only be selected if there are processes in place to deal with alerts immediately when they are created as otherwise the malware will be allowed to operate unhindered and spread to other endpoints in your network.

The default option of "Clean then Quarantine" is designed to prevent the file from executing if it cannot be cleaned by placing it in a protected quarantine folder. This is also useful in terms of locating a sample of the file for further analysis, for example, in the case that it is a suspected false positive. In the event that such analysis is not required, it is possible to select either of the "Delete" options which will cause the file to be deleted if the AntiVirus engine is unable to clean it or quarantine it. However, note that, in the event that the file is incorrectly identified as malware (i.e. a false positive) and the file has been deleted, it can no longer be restored.

Local Users/Services and Remote Users

Files are treated differently for scanning purposes depending on whether the file action was initiated by a local or remote user. A local user is any file interaction that happens on the local machine in the local user context. A service running on the local machine is considered to be a local user. Remote user is anything which is initiated externally. Connections via RDP, Citrix, Terminal services are considered to be remote users.

In the case of local users, the default behaviour is to scan files when they are read or executed. For remote users, the default behaviour is to scan when the remote user or service is writing to the file to ensure that they are not adding malware to the system.

In the case of a malware outbreak, changing the settings to "scan on both read/execute and write" will provide a greater level of protection. However, note that it also increases the performance impact associated with AntiVirus scans.

Add/ImportExclusions

Specific files, file types or file paths can be excluded from AntiVirus scans. This can be done, for example, where scanning these entities provides no benefit because they are safe but scanning them causes a noticeable performance impact on the endpoint. Exclusions might also be used temporarily in the event of a false positive whereby a clean file gets quarantined incorrectly. Adding an exclusion for this file enables the file to be restored immediately instead of waiting for an updated set of AntiVirus definitions whereby the file will be restored automatically if the false positive has been addressed with that new set of definitions.

You can view a set of recommended exclusions based on application vendor recommendations on Excluding files, folders and processes from AV scans community article. The article includes XML files containing these excludes which can be imported directly into the policy. There is one XML file for core system excludes which should be applied to all endpoints in your environment (subject to your review and acceptance). In addition, there is a Common Application Exclusions XML file which should be edited and applied selectively for any endpoints containing those applications.

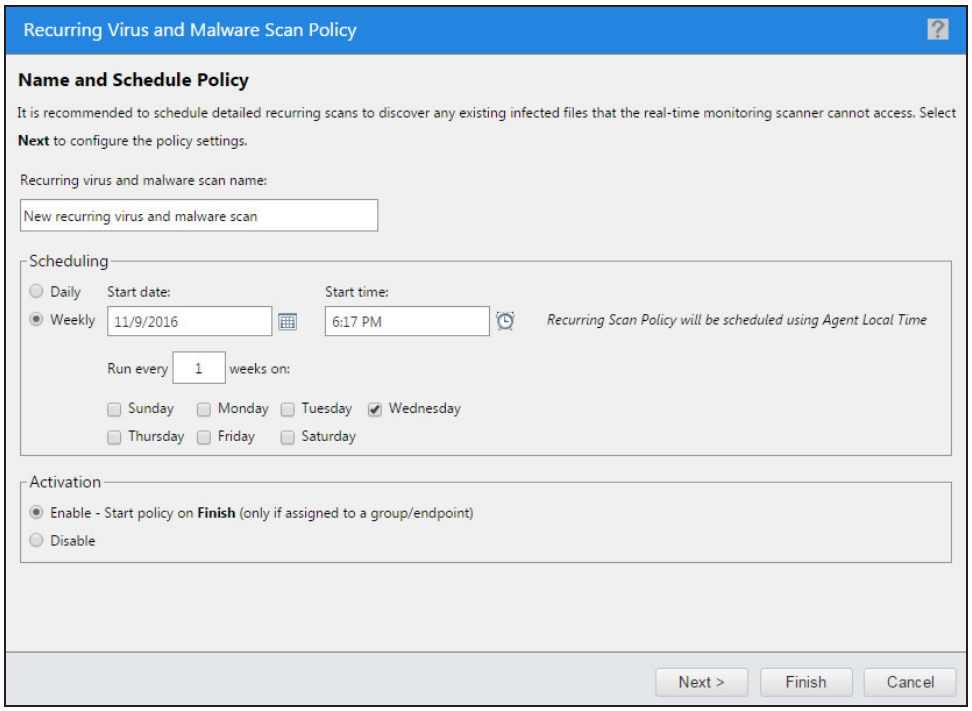
Excluding file paths adds risk in that malware can execute from these locations without being scanned. You should minimize the use of file path exclusions to minimize the associated risk.

Create a Recurring Virus and Malware Scan Policy

While the real time monitoring policy is used to protect users from malware whenever they open or execute files, you should also create a recurring virus and malware scan policy and this policy is used to scan for malware on a scheduled basis to remove any dormant malware from the endpoint.

Scan Frequency

The recurring scan can be executed daily or weekly as shown below. In general, customers will opt to conduct weekly or fortnightly recurring scans. As real-time monitoring provides immediate protection when files are accessed, there may be limited benefit from conducting more frequent recurring scans to remove dormant malware.



Scan Options

The scan options available are very similar to the "Scan Now – Virus and Malware Scan" (see Discover section). Particular attention should be paid to the CPU utilization setting and archive scan settings.

CPU Utilization

The CPU utilization setting can be adjusted to determine how much CPU gets consumed when the scan is being performed. If the scan is being performed out of hours, select the high CPU utilization setting which will cause the scan to use as much CPU as possible so that the scan completes more quickly. However, if the scan is being performed during business hours, you should select a medium or low CPU utilization level. This will cause the scan to take longer but the scan will have less of an impact on the user.

Scan Archives

While it makes sense to scan archives on a one-time scan using the Scan Now – Virus and Malware scan option, it may not be necessary to scan archives during a recurring scan as any malware lying dormant in these files will get detected by the real-time monitoring policy if the associated file is extracted from the archive. Scanning archives could result in the scan taking a lot longer so the default setting is to not scan archives. It is possible to set up an infrequent recurring scan (e.g. weekly scan which runs every 8 weeks scheduled to run at the weekend) which includes an archive scanning option.

Logging

The log level for real-time monitoring is set to "Normal" which means that log events are created in the event that malware is detected. It is possible to change this level to "Detailed" whereby a log entry is created for every file that is scanned. This logging level would only be used for diagnostic purposes (e.g. to analyse an application conflict or performance issue) so is not available as a policy option because it would create large log files and could cause performance issues. However, if you need to do some troubleshooting and require a detailed logging level, please contact Ivanti Support to get this enabled temporarily.

Phase 4: Recap

In this phase, real-time and recurring scan policies are created to provide ongoing protection against malware. These policies can be tuned to balance performance and productivity using exclusions and policy settings including CPU utilization and archive scanning. Recurring scans can be scheduled to execute out of hours to minimize end-user impact.

Phase 5: Manage

Now that the policies have been established, on-going AntiVirus management is achieved through the use of AntiVirus reports, dashboard widgets and email notifications.

In this phase you will:

- "Email Notifications" below

  Create email notifications to alert the administrator of unusual malware activity that requires attention

- "AntiVirus Dashboard Widgets" on the next page

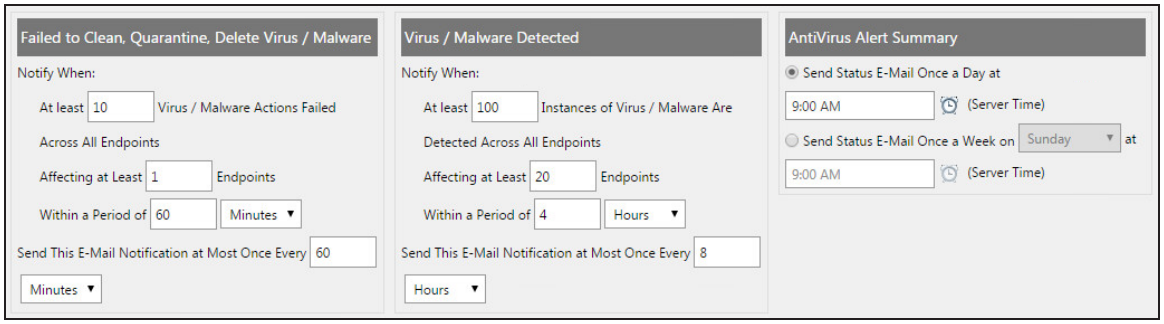
  Enable AntiVirus dashboard widgets to provide an at-a-glance indication of the overall system status from a malware perspective.

- "AntiVirus Reports" on the next page

  Create reports to perform more detailed analysis

Email Notifications

Email notifications can be established to alert the administrator of unusual malware activity. There are three different situations which can cause an email notification to be sent. See screenshot below.



Failed to Clean, Quarantine, Delete Virus Malware

This notification is used to indicate that malware has been detected which the AntiVirus module has been unable to remediate. While this malware has been prevented from executing, it is still present on the endpoint and needs to be removed or remediated. Thresholds can be defined to determine when email notifications should be sent. Because this notification represents malware which needs a prompt response, the threshold levels should be set very low so that an email is sent whenever this activity is detected. If the administrator receives emails too frequently, the threshold settings can be adjusted to reduce the frequency.

AntiVirus Alert Summary

It is also possible to get a daily or weekly email summary of the overall AntiVirusmodule status which can be used as a daily or weekly reminder of the AntiVirus remediation tasks which need to be performed. Depending on your preferences and security posture, this could be used as an alternative to either of the other email notifications.

AntiVirus Dashboard Widgets

There are three dashboard widgets which can be enabled to provide an at-a-glance indication of the overall status of the AntiVirus module. Each of these widgets is actionable, in that the administrator can click on the widget to drill down to obtain the associated detailed information from which the widget is derived:

Endpoints with Unresolved AntiVirus Alerts

This widget identifies the number of endpoints which have malware which the AntiVirus engine has quarantined or has been unable to clean. These represent malware which requires prompt action and is useful in terms of prioritising malware response.

Top 10 Infected Endpoints

This widget identifies which endpoints have got the greatest number of malware infections and is useful in prioritizing endpoints requiring remediation or follow-up security training.

Top 10 Virus/malware Threats

This widget identifies the most prevalent malware that has been detected in your environment and is useful in terms of understanding how malware is getting into your environment enabling you to take steps to reduce the associated attack vectors.

AntiVirus Reports

There are 2 standard reports which can be created for more detailed analysis:

AntiVirus Definition Version Status

This report can be used to determine which endpoints are most out-of-date with respect to AntiVirus definitions and to take remedial action to bring them up to date.

Endpoints/Groups with infections by date

This report enables you to perform analysis to determine how malware is entering your environment by identifying which endpoints get infected most frequently or were first to report on specific types of malware. This information can then be used to determine how to prevent future occurrences and provide end-user security training as appropriate.

Phase 5: Recap

In this phase, email notifications and dashboard widgets are used to act as a reminder and to help you prioritize the AntiVirus remediation activities that are required. In addition, AntiVirus reports can be used for more detailed analysis to help you manage your environment and take action to reduce the incidence of malware in the future.

Phase 6: Recover

At this point you have completed all of the steps needed to be in control of your environment from an AntiVirus perspective. However, you will occasionally encounter incidents that require further investigation.

In this phase you will:

- "Submit Suspect Files for Analysis" below

  Submit suspect files for analysis or for validation and removal as false positives.

- "Create Temporary Exclusions for False Positives" on the next page
- "Manually Restore or Delete Files From Quarantine" on page 30

  Manually restore or delete files from quarantine that have not been automatically restored.

Submit Suspect Files for Analysis

Submit suspect files for analysis If a file has been quarantined, you can submit this for further analysis to obtain remediation information (in the event that it is confirmed to be malware) or to get the AntiVirus signatures updated to remove/modify this signature (in the event that this is a false positive). There are a couple of different methods that can be used to submit files for analysis.

Submit file to Ivanti Support

This is the best mechanism to submit files for analysis. It ensures that the submission is tracked and prioritized. As the file has been detected as malware, the file needs to be protected prior to submission as otherwise it could get blocked during transmission. Quarantined files are stored in a hardened location in the endpoint's \Ivanti\LMAgent\Data\persist\AntiVirus\quarantine folder. If this folder is not accessible then contact Ivanti Support for details on how to retrieve the file.

To prepare a file for submission, the file should be added to a password protected archive file with password = Infected. Once this has been done the file can then be safely emailed to Ivanti Support, added to a case in the Ivanti Self-Service Portal , or uploaded to an FTP location for download (if too large for email).

Ivanti Support will then have the file analyzed and report back on the results whether the file contained malware or was a false positive.

Submit file for analysis directly

In order to get an initial assessment on a quarantined file, you can submit it directly via Virus Total.

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, Trojans, and all kinds of malware. This website can be used to upload a virus file where it will hash the file and compare it against a number of AntiVirus vendors.

Create Temporary Exclusions for False Positives

In the event that a file which has been quarantined is a false positive rather than malware, it is safe to restore this file. However, because the current set of AntiVirus definitions consider this file to be malware, it will be immediately returned to quarantine once it is restored. Once the AntiVirus definitions have been updated to address the false positive, the quarantined file will be automatically restored. This correction will generally take place on the next set of AntiVirus definitions which are released (i.e. within about 12 hours).

However, if it is necessary to restore the quarantine file prior to the new set of definitions being made available, this can be achieved by adding an exclude for this file to the AntiVirus scan policies. The file can then be restored successfully. Once the definitions have been updated to address this false positive, the exclude should then be removed.

Manually Restore or Delete Files From Quarantine

Quarantined files will automatically be restored from quarantine if they can be successfully cleaned or are considered clean (i.e. false positive) with a new set of AntiVirus definitions. In some circumstances, it may not be possible to automatically restore a cleaned file from quarantine.

This includes:

- If the filename already exists in the restored location (i.e. the file has already been replaced).
- If the file was quarantined from removable media (e.g. USB stick), the file will not be automatically restored for security reasons.

In these situations, the quarantined file can be manually restored from the quarantine or deleted as appropriate.

Phase 6: Recap

In this phase, you will submit files for further analysis to confirm whether they are malware or to determine whether they have been quarantined in error (i.e. false positive). Submitting the files will enable you to obtain remediation steps in the case of malware or get an updated set of definitions with a signature correction in the case of a false positive. While false positives will be automatically restored with the updated set of definitions you can exclude these files so that they can be restored in advance of the new definitions being available. You can also manually restore files which are not automatically restored from quarantine which can occur in certain situations.

Document Summary

This document has been written to provide a best practice process for administrators when implementing AntiVirus in their environments. Hopefully you find this to be useful as you roll the product out in your environment.

If you identify any issues in this document or any best practices you think should be added, please send an email to Ivanti Support with the details.