opentext™

ZENworks

Endpoint Security Antimalware Reference

Legal Notice

Contents

About This Guide

This *ZENworks Endpoint Security Antimalware Reference* provides information to help you configure, manage, and publish ZENworks Endpoint Security Antimalware policies.

Audience

This guide is written for the ZENworks Endpoint Security Management administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Endpoint Security Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks documentation website.

1 Concepts

ZENworks Endpoint Security Antimalware secures and protects Windows workstation and server devices against viruses, worms, Trojans, ransomware, zero-day exploits, rootkits, and spyware regardless of their location. This protection is configured through Antimalware policies and settings in ZENworks Control Center and enforced by the Antimalware Agent (scan engine) installed on the devices.

After deployment of the Antimalware Enforcement Policy, you can monitor the effectiveness of Antimalware protection via dashlets on the Security dashboard, as well as see specific malware threats and activity at the device and device folder level.

These sections provide an overview of Antimalware concepts that you need to understand to successfully protect your managed devices from malware threats.

About the Antimalware Agent

The Antimalware Agent is the scan engine that protects devices against malware threats. The agent uses a variety of technologies to detect malware, including:

- Malware signature files: The Antimalware Agent uses traditional signatures to quickly detect known malware threats. By default, the agent checks for signature updates every hour.
- Heuristic analysis: The Antimalware Agent uses complex heuristic algorithms and emulation to identify patterns and behaviors consistent with malicious files.

The agent provides real-time protection through on-access scans that occur whenever a file is opened, copied, moved, or executed. It can also perform on-demand scans (scheduled or user/administrator-initiated) of local, removable, and network drives, scan the device's boot sectors, memory, and registry, and can scan for keyloggers, rootkits, and Potentially Unwanted Applications (PUA).

You can control the level of interaction users have with the Antimalware Agent by completely hiding the agent or restricting the types of malware alerts that are displayed. For information about installation prerequisites and more details about the Antimalware Agent post installation, see Antimalware Agent Details.

About Antimalware Policies

ZENworks Endpoint Security Antimalware includes four policies: Antimalware Enforcement, Custom Scan, Network Scan, and Scan Exclusions. The Antimalware Enforcement Policy is the base policy required to install the Antimalware Agent and enforce settings configured for any of the four

policies. It provides comprehensive protection from malware threats with regularly scheduled scans. The Custom Scan and Network Scan policies provide targeted scans for specific threats. The Scan Exclusions policy enables you to exclude specific types of files from scheduled scans.

This guide helps you manage the Antimalware policies and applicable configurations required for malware signature updates and other content management related to employment of the Antimalware Agent.

For comprehensive information about deploying, managing, removing, and editing settings for Endpoint Security policies in general, to include Antimalware policies, see the *ZENworks Endpoint Security Policies Reference*

Descriptions of Antimalware Policies

You can use all or some of the Antimalware policies, depending on your organization's needs, but the Antimalware Enforcement Policy must be enforced on managed devices before you can use any of the features of the other three policies.

Policy	Purpose
Antimalware Enforcement	Installs the Antimalware Agent and configures the base on-access and on-demand scans that protect managed devices from malware threats. Because it is the base policy and installs the agent, it must be assigned to devices before any optional policies (Custom Scan Policy, Network Scan Policy, and Scan Exclusions Policy) can be assigned and enforced.
Custom Scan	Defines and schedules scans on local drives, in addition to the Full and Quick scans already defined in the Antimalware Enforcement Policy. Provides the capability to target specific threats that may not be covered in the regularly scheduled scans using the Antimalware Enforcement Policy.
Network Scan	Defines and schedules scans on files from network drives only. This policy gives you the capability to target a network drive from a specific device. For example, you could use this policy to scan a file storage disk in an array of disks. Network credentials must be configured in the policy to access network files.
Scan Exclusions	Customizes scan exclusions beyond those already configured in other Antimalware policies. Once this policy is created, you can add the Exclusions Policy option to the Custom Exclusions details of any of the three other Antimalware policies. The policy is then enforced based on having the same device assignment of the Exclusions Policy and the Antimalware policy that this option is configured in.

Antimalware Content Distribution Architecture

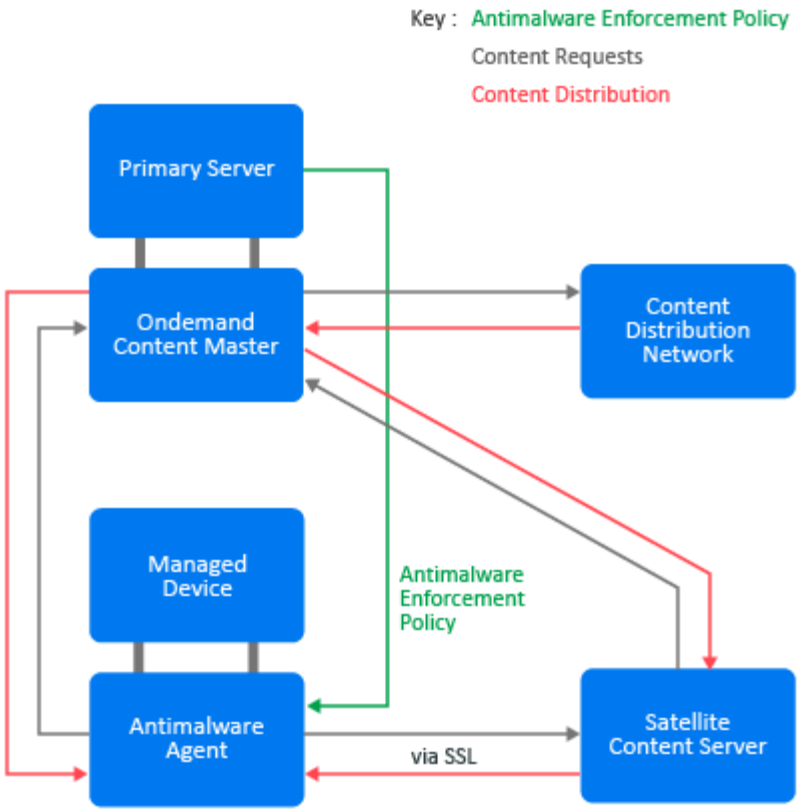
Ondemand content distributed to Antimalware agents in the content request process includes malware signature files to disinfect quarantined files and software updates to the Antimalware Agent.

The process for content requests originates with the Antimalware Agent on the workstation and each request moves upstream through content server channels until the request for content is fulfilled by a content server. The Antimalware Agent is a feature of ZENworks Endpoint Security. You install the agent on managed devices when you deploy the Antimalware Enforcement Policy.

All ZENworks Primary servers are content servers. Satellites that are assigned a Content Role also function as content servers. Satellites fulfilling this role need to be enabled for SSL for communication with the Antimalware Agent.

At least one Ondemand Content Master (OCM) is required to download content from the Content Distribution Network (CDN). Only Primary servers can function as OCMs. The Antimalware Server, when configured, defaults as an OCM. You can add additional OCMs via the Server Hierarchy configuration.

See the image below for a visual representation of the process described above. For more detailed information about ondemand content distribution, see the *ZENworks Ondemand Content Reference*.



Malware Threat - Antimalware Status Monitoring

Antimalware Dashlets

Antimalware Page

2 Antimalware Configuration

There are multiple settings that need to be configured to start protecting and monitoring managed devices from malware threats using ZENworks Endpoint Security Antimalware. There are also settings that are configured by default upon product activation, which you can modify as needed, but no initial configuration is required to begin using Antimalware. The rights to modify Antimalware settings is selected by default in the Zone Rights role for Administrator privileges. For more information about configuring Administrator rights, see the *ZENworks Administrator Accounts and Rights Reference*.

For Antimalware design best practices that you should consider before deploying Antimalware protection, see "Antimalware" in the *ZENworks Best Practices Guide*.

Refer to the items below for settings you need to configure when first deploying Antimalware protection, those that have default settings that you can customize as needed, and potential troubleshooting procedures:

Settings requiring initial configuration:

- Product Activation and Antimalware Entitlement
- Antimalware Server Settings
- Satellite Content Server Settings (including SSL)
- Deploying the Antimalware Enforcement Policy
- Configuring the Antimalware Database and Database Sync

Pre-configured settings (changes are optional):

- Antimalware Agent Schedules
- Antimalware Agent Notifications
- Application Only File Scans
- Security Dashboard Configuration

Troubleshooting Configuration Issues:

- Troubleshooting Antimalware Database Synchronization

Product Activation and Antimalware Entitlement

ZENworks Antimalware is a component of ZENworks Endpoint Security Management. You are required to activate Endpoint Security to employ Antimalware policies on client devices. Product activation requires a valid license key or the temporary evaluation license. The Antimalware Agent requires an entitlement key for activation and updates of the Antimalware Agent.

You can access Endpoint Security and Antimalware activation settings from the Getting Started page or the Configuration page in ZENworks Control Center:

- **Getting Started page:** Navigate to **Security** > **Getting Started** > **Protecting Against Malware**, and click the **Activate Product** link under Endpoint Security.
- **Configuration page:** Navigate to **Configuration** > **Licenses** panel > **Product Licensing**, and click the **ZENworks 2020 Endpoint Security Management** link.

Activate Endpoint Security

The Product Activation panel enables management of your product license:

- **Evaluate/Activate Product:** Either provide a valid product license key, or select **Use Evaluation** to use a temporary license for 60 days. If the evaluation period ends before you provide a valid license key, the locations in ZENworks Control Center related to the lapsed product are disabled (dimmed) until you provide a key.
- **Activate the product on all devices in the zone:** This option is displayed if the product is in Deactivated state and will be enabled if you select the Evaluate/Activate Product option.
  - If you select this option, the product is enabled on all the managed devices in the zone. You can disable the product or the ZENworks agent components at a later time, on selected managed devices at the device folder or the device level.
  - If you do not select this option, the product is not enabled across all the managed devices in the zone. You can enable the product or the ZENworks agent components on all devices or on specific devices at a later time, at the zone, device folder, or device level.

  To enable or disable the product at a later time on specific devices or device folders:
  - **At the device level:** Click the device link and navigate to **Settings** > **Device Management** > **ZENworks Agent** > **Endpoint Security Management**
  - **At the device folder level:** Click the device folder (Details) link and navigate to **Settings** > **Device Management** > **ZENworks Agent** > **Endpoint Security Management**
- **Deactivate Product:** Select this option to deactivate the product component. This causes all locations in ZENworks Control Center to no longer display anything related to the deactivated product.

Add an Antimalware Update Entitlement

The Activation - Antimalware Update Entitlement panel enables activation and updates management of the Antimalware Agent on devices that you assign the Antimalware Enforcement Policy. If you select the Use Evaluation mode for the Endpoint Security Management, the Antimalware Update Entitlement will automatically be added to the list and will be active for your evaluation period.

If you are providing a product license key, click **Add** in the Activation - Antimalware Update Entitlement panel and provide both a valid entitlement key and a valid email address to activate the Antimalware Agent. If you do not have an Antimalware Entitlement Key, contact your ZENworks Administrator or ZENworks Product Support to get one.

Antimalware Server Settings

The Antimalware Configuration settings define the server for malware cleanup and Antimalware Agent installation as well as the default server for an Ondemand Content Master. To access these settings, navigate to **Security** > **Getting Started** > **Protecting Against Malware**, and click the link under the Antimalware Server section. You can also access them under Security in the Management Zone Settings.

Antimalware Server

One Primary Server needs to be designated as the Antimalware Server to perform Antimalware-related maintenance tasks for your zone. This server also functions as an Ondemand Content Master (OCM) by default. If you designate one or more additional Primary servers as OCMs in the zone, the OCM designation can be removed from the server selected in this configuration as the Antimalware Server. You can make that change via the Server Hierarchy configuration.

Any Primary servers designated as OCMs need to meet the Ondemand Content Master requirements. For more information, see Ondemand Content Master - Requirements.

Maintenance Schedule

The Antimalware Server performs maintenance once a day, which can include cleaning up old malware events and rebuilding the bundle for the Antimalware Agent installation. You can define the time that the maintenance occurs and remove old malware events or rebuild an agent installation bundle manually.

When you configure the age limit for automatically removing old malware events according to the daily maintenance schedule, the configurable range is from 1-180 days.

Ondemand Content Master - Requirements

The Ondemand Content Master requires an Internet connection to communicate with and download content from the external Antimalware cloud service. This service is a Content Distribution Network (CDN) that manages all the malware signature files required to disinfect files on managed devices.

Configuring a proxy: If the OCM requires a proxy to access the service, the OCM server's Subscription proxy configuration file is used.

If you have configured your network to use a proxy server, you must configure the proxy server subscriptions.

1. On the Primary Server on which the Ondemant Content Master is configured to run, navigate to the `lpm-server.properties` file.
   - `/etc/opt/microfocus/zenworks/`

   An example of the content within the `lpm-server.properties` file is displayed below:

   ```
   Debug=false
   TTL=24
   subscription-proxyaddress=
   subscription-proxyport=
   subscription-proxyuser=
   subscription-proxypassword=
   subscription-useNTLM=false
   ```

2. Modify and save the file with the following subscription proxy details:
   - Set the value of `subscription-proxyaddress` to the IP address of the proxy server.
   - Set the value of `subscription-proxyport` to the port number of the proxy server.
   - (Conditional) If the proxy is authentication-based, set the value of `subscriptionproxyuser` to the name of the proxy user.
   - (Conditional) If the proxy is authentication-based, set the value of `subscriptionproxypassword` to the password associated with the proxy user name.
   - It is recommended to use the `zman srpp` command to specify an obfuscated password instead of specifying the raw password.
   - (Conditional) If the proxy server uses an NTLM realm, set the value of `subscriptionuseNTLM` to true. By default, the value is false.
3. Restart the ZENworks services.

Accessing the CDN: The following URL must be open to access the CDN: `https://microfocus-2dcb60a8-26c9-4560-9cc2-34a16ea5f6e6.2d7dd.cdn.bitdefender.net`

Proxy Server Settings: This setting is useful for restrictive environments where you do not want all of your production servers to have Internet access. For more information, see System Update Settings in the ZENworks System Updates Reference.

Information: while configuring, if the agent displays "You are at risk" alert message, then check the Troubleshooting section.

Satellite Content Server Settings

All Primary servers function as content servers. Satellites can function as content servers when you assign them a Content role via the Server Hierarchy configuration. You can assign this role when first configuring the managed device as a Satellite or at a later time. The Content role is one of five roles you can assign to a Satellite. Ondemand content for the Antimalware Agent is automatically included in content distribution for the Satellite when the Content role is assigned.

Satellites come into play for ondemand content requests and distribution when they are the closest content servers to managed devices that have the Antimalware Enforcement Policy assigned. To add a Satellite or to assign a Content role to an existing Satellite, navigate to the Server Hierarchy panel in the main Configuration page.

For detailed information about configuring Satellites and assigning a Content role in particular, see "Adding and Configuring Satellite Devices" in the *ZENworks Primary Server and Satellite Reference*.

IMPORTANT: SSL communication is required for ondemand content on a Satellite. When configuring Satellites with a Content role, ensure you select the **Use SSL to transport data securely** check box. If your zone is using an external Certificate Authority, make sure the Satellite has been configured with the appropriate external certificates. See "Adding and Configuring Satellite Devices" in the *ZENworks Primary Server and Satellite Reference* for details.

For information about configuring the ondemand content schedule and content cache settings, see "Ondemand Content Configuration" in the *ZENworks Ondemand Content Reference*.

Deploying the Antimalware Enforcement Policy

The Antimalware Enforcement Policy enables you to configure and deploy the Antimalware Agent to Windows managed devices (servers and clients) to protect against malware threats in your zone. This policy is the primary enforcer of the ZENworks Endpoint Security Antimalware capability, which protects managed devices from malware threats by performing on-access and on-demand scans on those devices. This policy is required to use an Antimalware Scan Exclusions, Custom Scan, or Network Scan policy. Policy defaults are automatically set in the policy during policy creation.

You can initiate creation and deployment of the Antimalware Enforcement Policy from the Policies page or from the Protecting Against Malware page in Security > Getting Started. Only one Antimalware Enforcement policy is enforced on a device. If multiple policies are assigned, the standard policy resolution methods are used to determine which policy is "closest" to the device and is therefore applied. Several of the more granular settings when creating a new policy are preset based on the higher-level settings you choose in the Policy wizard. To see or customize the granular settings, open the policy from the Policies page after policy creation and click the **Details** tab.

NOTE: Before you assign and publish the Antimalware Enforcement Policy to devices, ensure that all pre-existing antimalware or antivirus software is removed from those devices. This includes completing any required reboots from software removal. For more information about prerequisites to installing the Antimalware Agent, see Agent Installation Requirements.

For information about modifying or customizing the policy after policy creation, see Antimalware Enforcement Policy.

The following instructions assume that you are on the **Configure On-Access Scanning** page in the Create New Antimalware Enforcement Policy wizard. For information about creating policies in general or the common steps in policy creation, see "Creating Security Policies" in the *ZENworks Endpoint Security Policies Reference*.

Configure On-Access Scanning

You can retain the most balanced approach between security and system performance by retaining the default setting of **Normal** or configure on-access scans with greater security or with greater performance by choosing **Aggressive** or **Permissive**, respectively. Once the policy is created, you will have the option to make more specific configuration changes through the Details tab on the selected policy. Although not recommended, you can also disable on-accessing scanning altogether.

The descriptions below are the same shown for each scan level when selected in the page. They are also provided here in aggregate for comparison.

- **Aggressive:** Provides advanced security with moderate use of resources. Scans all files accessed from local and network drives including archived and lower risk files.
- **Normal:** Provides best balance between security and performance. Scans all files accessed from local drives and application files accessed from network drives. Does not scan archived and lower risk files.
- **Permissive:** Provides basic security with reduced use of resources. Scans application files accessed from local drives and incoming emails. Does not scan lower risk files, spyware, and less dangerous types of malware. This option is recommended only for use on devices with resource limitations.

Configure Ondemand Scanning

All on-demand scanning options are enabled by default. Familiarize yourself with the descriptions for the different options in the policy wizard page to make informed decisions on how to tailor on-demand scans to your enterprise needs. After the policy is created, you can customize the settings for these scans as needed, including disabling or enabling the different scan options provided in the page.

To configure how often Full and Quick scans run, navigate to **Configuration** > **Security** > **Antimalware Agent Schedules**. The default options are as follows:

- Full Scan: New installation set to run a full scan once weekly.
- Quick Scan: New installation set to run a quick daily scan, 6 out of 7 days of the week.

For information about configuring the schedules, see Antimalware Agent Schedules.

Configure Quarantine Behavior

Each device has a local quarantine. The quarantine is an encrypted folder that contains malware-infected or malware-suspected files that have been detected by a scan. Quarantined files cannot do any harm because they cannot be executed or read.

Files are moved to quarantine based upon the scan remediation actions defined in the policies assigned to a device.

Quarantined files are sent to the Malware Research Lab on a regular basis to analyze and create routines for disinfection. If new signatures are created that can disinfect these types of files, those signatures will be included in the malware signature update, whereupon, the quarantined file will get disinfected and removed from quarantine.

All configurable options are enabled by default. For information about each option, see below:

- **Delete quarantined files older than (days):** This setting is provided to delete files that stay in quarantine for an extended period of time because the malware signatures updates have not provided a routine to disinfect the quarantined files. It cannot be disabled. The default setting to delete files is 30 days. The range for configuration is in increments from 1 to 180 days.
- **Submit quarantined files and critical threat data to Malware Research Lab every (hours):** You may want to configure this setting based on the amount of activity you get for quarantined files, while also considering conserving resources. Disabling this setting is not recommended. The default setting is every hour. The range for configuration is incremental from 1 to every 24 hours.
- **Rescan quarantine after malware signature updates:** This option is provided to disinfect quarantined files that could not be disinfected previously after a fix is included in a content update. Disabling this setting is not recommended. However, if your dashboard consistently shows low volume of quarantined files or the quarantined files are not essential to your daily operations, the flexibility is provided to disable the feature.
- **Copy files to quarantine before applying the disinfect action:** This option is provided to prevent data loss in case of false positives. You can restore legitimate files from quarantine from the Antimalware page on a selected device.
- **Allow users to take action on local quarantine:** Enables endpoint users to restore or delete files quarantined on their devices via Endpoint Security Agent Actions in the ZENworks Agent.

Configure Scan Exclusions

Scan exclusions can include both built-in file exclusions and custom exclusions. Built-in exclusions include Windows directories recommended for exclusion by Microsoft and some ZENworks directories. However, ZENworks built-in exclusions are not controlled by this setting. These built-in items will not be scanned for the scan types you configure in the policy. Scan types include, On-Access, Full, Quick, and Contextual scans.

For information about Microsoft recommended exclusions for Windows, see Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows.

Custom exclusions can include file exclusions added directly in the Custom Exclusions panel, exclusions implemented by assigned Antimalware Exclusion policies, or a combination of both. Scan types include, On-Access, Full, Quick, External Device, and Contextual scans. Scan Exclusion types are designated as File, Folder, Extension, or Process.

For more detailed information about configuring exclusions in this policy after you create the policy, see *Exclusions*.

Assign and Publish the Policy

You can only assign Antimalware policies to devices. They cannot be assigned to users. For information about assigning and publishing Endpoint Security policies, see the topics below in the *ZENworks Endpoint Security Policies Reference*:

- "Assigning Security Policies"
- "Publishing Policies"

Configuring the Antimalware Database and Database Sync

When you first deploy the Antimalware Agent, it is enabled on devices but no malware activity is rolled up for viewing in the ZENworks Control Center. To enable monitoring of malware activity, you must configure the Antimalware Database required to store the rolled-up malware data. In addition, if your zone does not already have a Linux Primary Server, you must first add one in order for data to be synced between the main ZENworks database and the Antimalware database. After you enable Kafka and configure the Antimalware Database, you need to populate the Antimalware Database with the required data from the ZENworks Database (database sync).

To enable Kafka, configure the Antimalware Database, and then populate the database, navigate to **Security** > **Getting Started** > **Protecting Against Malware** in the ZENworks Control Center, and use the links under Linux Primary Server and Antimalware Database. You have to configure the Linux Primary Server before you can configure the Antimalware database.

NOTE: To perform configuration tasks, ensure that you have Super Administrator rights.

- "Linux Primary Server" on page 20
- "Antimalware Database" on page 21

Linux Primary Server

A Linux primary server is required for the Kafka platform to sync the Antimalware database with the ZENworks database to monitor Antimalware implementation and status. If possible, the Kafka synchronization should be the primary function of this Linux server. You can also use the ZENworks Virtual Appliance for this server.

Click **Enable Kafka** to select the Linux server that you will use for Antimalware and ZENworks database synchronization. You must already have a Linux server set up as a ZENworks primary server in the Server Hierarchy to enable this feature.

If you have multiple Linux primary servers, we recommend that you select one that is not already tasked with other functions such as the Patch Subscription Service.

See the following to understand the process of enabling Kafka and any follow-on actions you might need to take based on the Status indicator:

1. **Completed:** Kafka enablement is completed. Because delays can occur as the service is connecting, you should check the status of the Kafka service before starting to configure the Antimalware database. Click **Check Status of Services** under Antimalware Database to navigate to the Diagnostics page.

   In the Kafka Cluster panel, make sure that the service is running on the Linux Primary Server you selected. If it is not yet running, wait a while for it to start. If it does not start after a while, manually start Kafka on the server. For information about manually starting Kafka on the server, see "Enabling Kafka on a Single Server" in the *Kafka Reference Guide*.

2. **In Progress:** Kafka is currently being enabled on the selected Linux Primary Server. If the task remains in progress for an extended period of time (more than 20 minutes), it may be that the Kafka service has actually been enabled and the completed message was not returned for some reason. Click **Check Status of Services** under Antimalware Database to navigate to the Diagnostics page.

   In the Kafka Cluster panel, see if the service is running on the Linux Primary Server you selected. If it is not running, manually start Kafka on the server. For information about manually starting Kafka on the server, see "Enabling Kafka on a Single Server" in the *Kafka Reference Guide*.

3. **Failed:** Enabling Kafka on the selected Linux Primary Server failed. Make sure the server is running and then use the **Enable Kafka** link to retry enabling the service.

   To troubleshoot Kafka connections, see Troubleshooting Antimalware Database Synchronization.

If you need information to install a ZENworks primary server on Linux or would like to install the ZENworks Virtual Appliance, see the following references:

- "Linux Installation Workflow" in *ZENworks Server Installation*
- *ZENworks Appliance Deployment and Administration Reference*

Antimalware Database

The Antimalware database is separate from the ZENworks database, but must be of the same type for synchronization between the two databases. For example, PostgreSQL, Oracle, or Microsoft SQL. When configuring the Antimalware Database, ZENworks determines which type of ZENworks database your zone has and provides the Antimalware configuration for that database type. The only exception to this is PostgreSQL, which can be embedded or remote. If you are presented the **Antimalware database type** drop-down option, you must choose the PostgreSQL type that you want.

The process for configuration and database sync includes first configuring the Antimalware Database, and then populating the Antimalware Database with ZENworks data. If you will be using Embedded PostgreSQL, this is a one-step process for configuring the Antimalware Database. When you select this option, click **Next** and then **Finish** to create the database.

For information about configuring another type of database, populating the database after completing the configuration, or troubleshooting synchronization post configuration, reference the sections below:

- Database Configuration Prerequisites
- Configure Remote PostgreSQL Server

- Configure Microsoft SQL Server
- Configure Oracle Database
- Populate the Antimalware Database

Database Configuration Prerequisites

In the Antimalware database configuration sequence, ZENworks can create a new database or configure an existing database. Or in the case of using Oracle, create a new user schema or use an existing user schema.

NOTE: An “existing database” implies an Antimalware database configured for the specific purpose of running the Antimalware Database Configuration tool launched from Security > Getting Started > Protecting Against Malware page in ZENworks Control Center, as opposed to configuring a new database using the same tool.

Depending on the database type and whether it’s a new or existing database determines which credentials you require: Database Administrator (DBAdmin), Database Access, or both, as shown below:

Database Type	New Database	Existing Database
Remote PostgreSQL	• Database Administrator credentials • Database Access credentials	• Database Administrator credentials • Database Access credentials
Microsoft SQL Server	• Database Administrator credentials • Database Access credentials	• Database Access credentials
Oracle	• Database Administrator credentials • Database Access credentials	• Database Access credentials

---

NOTE:

- The Database Administrator should not provide the following database user names when the chosen option is **configure an existing database**:
  - Remote PostgreSQL: *postgres* or *zenpostgres*
  - Microsoft SQL Server: *sa* or *Administrator*
  - Oracle: *System* or *Sys*
- When configuring the Antimalware database if the database type is Microsoft SQL, we recommend using the same database authentication scheme as configured for ZENworks database.

If you need your database administrator to configure a new external Antimalware database or Oracle user schema, this is executed using command line to run the ZENworks `setup.exe` file. When presented with a database selection option in this process, the administrator needs to choose **Antimalware Database**, not ZENworks Database or Audit Database. The commands used to run `setup.exe` for database configuration are below:

- **Windows server:** `DVD_drive:\setup.exe -c`
- **Linux server:** `sh /media/cdrom/setup.sh -c`

NOTE: ZENworks no longer supports Windows Server as a Primary Server from version 24.2 onwards. For more information, see End of Windows Primary Server Support.

NOTE: Only GUI installation is available for configuring a database instance with Linux.

After choosing Antimalware Database in this process, the database administrator should follow database configuration instructions in the *ZENworks Server Installation* reference, post selecting the database type. This reference also includes information about administrator rights and prerequisites.

Configure Remote PostgreSQL Server

If you are referencing this section, you should have PostgreSQL as your ZENworks database and selected **Remote PostgreSQL** as your database type in the Antimalware database configuration options.

To configure remote PostgreSQL Server:

1. Click **Next** after selecting Remote PostgreSQL as the database type.
2. Click **Next** in the Database Administrator Rights dialog box.

   If you need more information about database rights to create a new database, see Database Configuration Prerequisites.
3. Choose to **create a new database** or **configure an existing database**, and click **Next**.
4. Enter the server address and connection port for the existing database or where the new database will be installed, and click **Next**. For example:
   - Server address: `serverName.company.domainName.com`
   - Port: 54327
5. Proceed according to your configuration.
   - **Configure New Antimalware Database**:
     1. Specify the name for the new Antimalware database.
     2. Specify the database administrator credentials required to create the new database.
     3. Specify the database access credentials that will be used for ongoing access to the Antimalware database.
     4. Click **Next** and **Finish**.
   - **Configure Existing Antimalware Database**:
     1. Specify the name of the existing Antimalware database.
     2. Specify the database administrator credentials.

3. Specify the access credentials provided by your database administrator. These will be used for ongoing access to the Antimalware database.
4. Click **Next** and **Finish**.

Configure Microsoft SQL Server

If you are referencing this section, you should have Microsoft SQL Server pre-configured as your database type in the Select Antimalware Database Type dialog box.

To configure Microsoft SQL Server:

1. Click **Next** in the Select Antimalware Database Type dialog box.
2. Click **Next** in the Database Administrator Rights dialog box.

   If you need more information about database rights to create a new database, see Database Configuration Prerequisites.
3. Choose to **create a new database** or **configure an existing database**, and click **Next**.
4. Enter the server address, connection port, and named instance for the existing database or for the new database that will be installed, and click **Next**. For example:
   - Server address: `serverName.company.domainName.com`
   - Port: 1433
   - Named instance: `AD LDS Instance-Antimalware Database`
5. Proceed according to your configuration.
   - **Configure New Antimalware Database**:
     1. Specify the name for the new Antimalware database.
     2. Provide the server location where the database will be installed.

        For example: `c:\database`
     3. Select the authentication method for the database administrator: **Windows Authentication** or **SQL Server Authentication**.
     4. Specify the database administrator credentials who has permission to create a database, based on the type of authentication selected.
     5. If using Windows Authentication, enter the domain name. For example: `domainName`

        The domain name is available in the zdm.xml or dmaccounts.properties file.
     6. Select the authentication method for the database access credentials.
     7. Specify the access credentials for the type of authentication selected. These credentials will be used for ongoing access to the Antimalware database.
     8. If using Windows Authentication, enter the domain name. For example: `domainName`

        The domain name is available in the zdm.xml or dmaccounts.properties file.
     9. Click **Next** and **Finish**.
   - **Configure Existing Antimalware Database**:
     1. Specify the name of the existing Antimalware database.
     2. Select the authentication method: **Windows Authentication** or **SQL Server Authentication**.

For Windows Authentication, the specified user must already exist in the Active Directory domain.

3. Specify the access credentials for the type of authentication selected. These credentials will be used for ongoing access to the Antimalware database.
4. If using Windows Authentication, enter the domain name. For example: `domainName`

   The domain name is available in the zdm.xml or dmaccounts.properties file.
5. Click **Next** and **Finish**.

Configure Oracle Database

If you are referencing this section, you should have Oracle pre-configured as your database type in the Select Antimalware Database Type dialog box.

To configure the Oracle database:

1. Oracle partitioning with ZENworks is enabled by default in the Select Antimalware Database Type dialog box. If you want to disable this feature, select **No** in the partitioning option.

   Otherwise, leave **Yes** selected, and click **Next**.
2. Click **Next** in the Database Administrator Rights dialog box.

   If you need more information about database rights to create a new user schema, see Database Configuration Prerequisites.
3. Choose to **create a new user schema** or **configure an existing user schema**, and click **Next**.
4. Enter the server address, connection port, and service name for the existing database or for the new database that will be installed, and click **Next**. For example:
   - Server address: `serverName.company.domainName.com`
   - Port: `1521`
   - Service name: `zenworks.provo.novell.com`
5. Proceed according to your configuration.
   - **Configure New User Schema**:
     1. Specify the database administrator credentials who has permission to create a new user schema.
     2. Define new user credentials to be created. These credentials will be used for ongoing access to the Antimalware database. This also enables ZENworks to create tables, procedures, triggers, and sequences in the database.
     3. Select whether to let ZENworks create tablespaces for the new user defined above or to have the database administrator create the tablespaces.
     4. If you chose the option to have ZENworks create the tablespaces, define the tablespace names for tables and for indexes, and the DBF file locations for those tables and indexes.

        If you chose **Let DBA create the tablespace**, skip to the next step.
     5. Click **Next** and **Finish**.
   - **Configure Existing User Schema**:
     1. Specify the database access credentials that enable ZENworks to access the user schema and to create tables, procedures, triggers, and sequences in the database.

2. Define the tablespace names for tables and for indexes.
3. Click **Next** and **Finish**.

Populate the Antimalware Database

After you complete the Antimalware Database configuration for your zone, you should see a status link next to “Configure Database” in the Antimalware Database section of the Getting Started page. For example, Configure Database (Status:Completed). If there are any issues, the hyper-linked text would read differently, such as “Completed with Issues”. Click the link next to **Status:** to open the Database Configuration Status to see the status of two tasks: Database Configuration and Configuration Replication.

If there are no issues and the Antimalware Database is configured, the **Populate Database** link should be enabled. Click the link to populate the newly configured Antimalware Database with ZENworks data. If the zone runs on a single server using a Linux operating system, all ZENworks services will temporarily stop while the data is synchronized between the two databases, ZENworks and Antimalware, and then be restarted.

If you have multiple primary servers in your zone, open a command prompt or terminal as a Super Administrator on one of the primary servers and enter the command as shown below to execute the Populate Database action:

```
microfocus-zenworks-configure -c PopulateAMDatabaseConfigureAction
```

After running the command, you can specify the parameters as prompted.

```
-DsuperAdminUsername=%superadmin%
-DsuperAdminPassword=%superadminpass%
-DproceedMigrationOnServiceFailure=Y or N
```

Example:

```
-DsuperAdminUsername=Administrator
-DsuperAdminPassword=novell
-DproceedMigrationOnServiceFailure=Y or N
```

In this example, ‘Administrator’ is %superadmin% and ‘novell’ is %superadminpass%

- Windows: Run the command from the command prompt of a ZENworks Primary Server, and follow the prompts to perform and monitor the migration.
- Linux: Run the command from the terminal of a ZENworks Primary Server, and follow the prompts to perform and monitor the migration.

After giving time for the process to complete, the Configure Database status will update.

After running the configure action on any one Primary server in the zone, services will be stopped automatically on all Primary Servers. Post-migrating data, services will be started automatically.

If the status displays an output other than “Completed”, you can reference Troubleshooting Antimalware Database Synchronization to resolve potential issues.

Troubleshooting Antimalware Database Synchronization

Data synchronization between the ZENworks Database and the Antimalware Database is managed by the Kafka service, and can be optimized by tuning Kafka settings and database connections. If you are seeing potential issues with data synchronization post database configuration, information for tuning database synchronization in the *ZENworks Best Practices Guide* is a good place to get a health check of these settings in your zone. For more information, see "Tuning Antimalware Database Synchronization" in the *ZENworks Best Practices Guide*.

If Antimalware Database tuning appears to be in order, reference the following sections for potential troubleshooting scenarios with the Antimalware Database:

- "Kafka Connector Troubleshooting" on page 27
- "Server Replication Troubleshooting" on page 27
- "Vertica Integration Troubleshooting" on page 28

Kafka Connector Troubleshooting

When enabling Kafka for Antimalware, you should get a green status for all the components in the Kafka Cluster panel on the Diagnostics page. If subsequently the Populate Database action fails when configuring the Antimalware Database, check the `microfocus-zenworks-configure-service.log`. If the log states "Successfully started the loader service on that server (<server name>)", then check the loader message of the server. If the zookeeper timeout exception (shown below) is logged, then the issue might be because of the zookeeper exception.

```
ZookeeperClientException: Timed out waiting to connect to ZooKeeper!
```

To try fixing this issue, do one of the following:

- Single Primary Server zone: Click the **Status** link for Configure Database, and rerun the **Populate Database** action.
- Multi-Primary Server zone: Run the `PopulateAMDatabaseConfigureAction` command again on one of the primary servers. For more information, see Populate the Antimalware Database.

If the issue persists, please contact Global Technical Support.

Server Replication Troubleshooting

Configuration replication across all primary servers in the zone is a key task that ZENworks runs when configuring the Antimalware Database. If the configuration replication task fails on any of these servers, the Configure Database (Status:) might read "Completed with Issues", and the **Populate Database** option will not be enabled.

Servers that failed to replicate should be listed in the Database Configuration Status dialog box when opened. If you have one or more servers listed here that can be ignored for Antimalware configuration replication, you can still run the `PopulateAMDatabaseConfigureAction` command on the primary server where configuration replication is successfully completed. For information on running the command, see Populate the Antimalware Database.

To fix the configuration replication issue on these servers, copy the `amedatasource.properties` file from a primary server without issues on to the servers with issues, in the following directory:

- Linux: `/etc/opt/microfocus/zenworks/antimalware`
- Windows: `C:\Program Files (x86)\Micro Focus\ZENworks\services\antimalware\conf`

Vertica Integration Troubleshooting

If your zone is integrated with Vertica for ZENworks dashboard enhancements prior to upgrading to ZENworks 2020 Update 2, you could potentially experience loss of Antimalware Enforcement Policy synchronization with the ZENworks Database. If you see this issue in your Antimalware environment, execute the zman command below on the ZENworks Primary Server to fix it:

```
zman server-role-kafka-reconfigure-connectors
```

-or-

```
zman srkccn
```

Antimalware Agent Schedules

The Antimalware Agent Schedules enable you to schedule when a device's Antimalware Agent performs scans and updates. You can also determine when the Antimalware Agent is installed on the device after the Antimalware Enforcement Policy is assigned to it.

The schedules apply to all devices in the zone. Overrides to these schedules can be implemented at the device folder and device levels.

NOTE: When you modify the Antimalware Agent Schedules, there is a 2 hour delay for the built-in server refresh and an additional few minutes for the ZENworks Database and the Antimalware Database to sync. This needs to be taken into consideration when viewing the Next Scan status and Next Scheduled Scan status in the Antimalware page and Device Malware Status dashlet, respectively.

To access the schedules in the ZENworks Control Center, navigate to **Configuration** > **Security** > **Antimalware Agent Schedules**. For information about configurable options for each schedule, click the applicable option link in the table below:

Schedule Type	Description	Configurable Options
Full Scan	Protects scan targets by checking for all types of malware threatening their security.	◆ Days of the Week ◆ Monthly ◆ Fixed Interval ◆ Wake-on-LAN

Schedule Type	Description	Configurable Options
Quick Scan	A reduced-scope on-demand scan that typically runs in less than a minute and uses a fraction of the resources needed to run a full scan.	◆ Days of the Week ◆ Monthly ◆ Fixed Interval ◆ Wake-on-LAN
Malware Signature Update	Checks for and downloads the newest malware signature files which may be used to disinfect infected files.	◆ Days of the Week ◆ Fixed Interval ◆ Wake-on-LAN
Antimalware Agent Update	Checks for and installs updates to the Antimalware Agent.	◆ Days of the Week ◆ Fixed Interval ◆ Postpone reboot ◆ Force reboot after update... ◆ Wake-on-LAN
Antimalware Agent Installation Schedule	Defines when managed devices install the Antimalware Agent.	◆ At policy enforcement ◆ Days of the Week ◆ Monthly ◆ Wake-on-LAN

Configurable Options in Agent Schedules

Reference the sections below for information about the configurable options available in the Antimalware Agent Schedules.

Days of the Week

This schedule lets you specify the days during the week that you want the scan to run or to install updates. The action is run on these same days each week.

Select **Days of the Week**, then fill in the following fields:

- **Sun ... Sat:** Specifies the days of the week you want to execute the action.
- **Start Time:** Specifies the time you want to run the scan.
- **Process immediately if device unable to execute on schedule:** The action is considered past due if it is not executed on the configured schedule for some reason.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don’t select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Start at a Random Time between Start Time and End Time:** Starts the action at a randomly selected time between the time you specify in the **Start Time** and **End Time** fields. You can use this option to avoid possible network overload from concurrently scheduled scans or updates.

- **Restrict Schedule Execution to the Following Date Range:** Limits executing the action to the time period specified by the starting and ending dates.

Monthly

This schedule lets you specify one or more days during the month to run the scan or install updates.

Select **Monthly**, then fill in the following fields:

- **Day of the Month:** Specifies the day of the month to execute the action. Valid entries are 1 through 31. If you specify 29, 30, or 31 and a month does not have those days, the action is not executed that month.
- **Last Day of the Month:** Executes the action on the last day of the month, regardless of its date (28, 30, or 31).
- ***First Sunday*:** Specifies a specific day of a week. For example, the first Monday or the third Tuesday. Click  to add multiple days.
- **Start Time:** Specifies the time you want to execute the action.
- **Process Immediately if Device Unable to Execute on Schedule:** Any action is considered past due if it is not executed on the configured schedule for some reason.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Start at a Random Time between Start Time and End Time:** Executes the action at a randomly selected time between the time you specify in the Start Time and End Time boxes. You can use this option to avoid possible network overload from concurrently scheduled events.
- **Restrict Schedule Execution to the Following Date Range:** Limits executing the action to the time period specified by the starting and ending dates.

Fixed Interval

This schedule lets you specify an interval between days to run the scan or install updates. For example, you can execute the action every 14 days.

Select **Fixed Interval**, then fill in the following fields:

- **Months, Weeks, Days, Hours, Minutes:** Specifies the interval between times when the action is executed. You can use any combination of months, weeks, days, hours, and minutes. For example, both *7 days, 8 hours* and *1 week, 8 hours* provide the same schedule.
- **Start Date:** Specifies the initial start date for the interval.
- **Start Time:** Specifies the initial start time for the interval.
- **Process Immediately if Device Unable to Execute on Schedule:** A action is considered past due if it is not executed on the configured schedule for some reason. If you select this option:
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time

zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

- **Restrict Schedule Execution to the Following Date Range:** Limits executing the action to the time period specified by the start date, end date, and end time.

Wake-on-LAN

If the device is not on at the scheduled time, this option attempts to use Wake-on-LAN technology to power on the device. The device must support Wake-on-LAN.

For information about Wake-on-LAN options or how it works, see "Wake-on-LAN in ZENworks Control Center" in the *ZENworks Using Wake-on-LAN* reference.

Reboot Options for Antimalware Agent Updates

The two configurable options for scheduling device reboots after an Antimalware Agent update runs, are defined below:

- **Postpone reboot:** If the device requires a reboot after an Antimalware Agent update runs, this option will postpone the reboot from occurring automatically. Use the **Force reboot...** option in conjunction with this setting to schedule when the postponement expires.
- **Force reboot (if needed) after update every:** Use this option in conjunction with the **Postpone reboot** setting to schedule when the postponement expires. You can set a daily time or a specific day of the week.

At Policy Enforcement

The **At policy enforcement** option is the default setting for installation of the Antimalware Agent on managed devices when the Antimalware Enforcement Policy is assigned to those devices. You can change this setting to run at a specific day and time of the week in the Antimalware Agent Installation Window schedule.

Antimalware Agent Notifications

Antimalware Agent Notifications controls the settings for Antimalware generated notifications on managed devices in the management zone. Some notifications inform the end user of security events and the actions taken by the Antimalware Agent and others inform the user of security and status alerts that may require user action or inform of a pending or required system restart. A full description for each notification setting is provided in the Antimalware Agent Notifications page.

When enabling the different **Agent Status Alert** options, you can choose how each notification gets displayed:

- Show as Warning
- Do not show
- Show as Critical

To access the Antimalware Agent Notifications page in the ZENworks Control Center, navigate to **Configuration** > **Security** > **Antimalware Agent Notifications**.

IMPORTANT: If this feature is disabled, users on these managed devices will not have access to the Antimalware Agent or receive any notifications of agent actions. For more information, see Antimalware Agent Details.

Application Only File Scans

When you configure scans in one of the Antimalware policies, you can select an option to scan **Applications only**. This option includes a default list of file types that will be scanned when applicable to the policy-assigned device. You can add additional file types to this list by modifying a configuration file and distributing it to managed devices where the policy is deployed.

How to Customize the Scan List

To add file extensions not included in the Default Scan List:

1. Create a text file, "`ZenworksAntimalwareApplicationExtensionDefintions.txt`".
2. Add the required file extension types to the new file. The format is **one application extension** per line. For example:

   ```
   bat
   com
   msg
   ```

3. Copy the new file into the 32-bit and 64-bit folders of the `%ZENWORKS_HOME%\zav` directory on the Primary Server that is set as the Antimalware Server. For example:
   - `C:\Program Files (x86)\Micro Focus\ZENworks\zav\zenAVAgent-32`
   - `C:\Program Files (x86)\Micro Focus\ZENworks\zav\zenAVAgent-64`
4. Navigate to **Configuration** > **Security** > **Antimalware Configuration** in the ZENworks Control Center, and click **Rebuild Now** in the Maintenance Schedule panel.

   Step 4 is not required if you can wait the for the rebuild to run as configured in the Maintenance Schedule.
5. After the rebuild runs, a refresh is required on the devices that have the Antimalware Agent installed. You can run a quick task to refresh selected devices in aggregate. For more information, see "Using Quick Tasks" in the *ZENworks Control Center Reference*.

NOTE: If needed, you can copy the customization file directly into the `zav` folder (`%ZENWORKS_HOME%\zav`) on any device that has the Antimalware Agent installed.

Default Scan List

Reference the list of file extensions shown below to see which file types are included by default in Antimalware scans when the **Application only** setting is selected in an Antimalware policy.

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl;
acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi;
chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc;
docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp;
gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu;
jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda;
mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu;
oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd;
php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm;
pptx; prc; prf; prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx;
rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp;
spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd;
wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll;
xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

Security Dashboard Configuration

When viewing the Device Malware Status dashlet, status categories include Resolved, Unresolved, No Threats, and Unknown.

The **Unknown** status is determined by the setting configured here. Unknown is defined as devices that have not contacted the server for x number of days. The default setting is 3 days, but you can modify the value based on your requirements. This setting is defined as the “Unknown Threshold”.

The recommended value is in the range of 3-7 days. If you set the value too low, the frequency of the Unknown status in the security dashlets may get cumbersome. If you set the value too high, you may make a false assessment of device protection based on the status in the dashlets.

To change the threshold value, navigate to **Configuration** > **Management Zone Settings** > **Security** > **Security Dashboard**, and modify the value in the **Device Malware Status Unknown Threshold** section.

Email Notification

Email Notification page provides you the option to define the users who receive the notifications whenever new threats are detected by the Antimalware Server. You can use the Antimalware Email Notification option to configure the e-mail notifications whenever new threats are detected. You can decide which e-mail address is used to send notifications and you can also specify the recipients. The email notification is generated by the Antimalware Server during its scheduled maintenance period.

To configure the Email Notification, you need to:

- Configure an SMTP Server
- Configure the Primary Server that will connect to the SMTP Server

To configure the Primary Server:

1. Go to **Configuration** > **Event and Messaging** > **Notification Servers**
2. Click the **Primary Server** browse icon and then select a Primary Server that sends patch management and antimalware related E-mail notifications. This is an optional field.

   If you do not configure a Primary Server, then by default the notifications will be sent from the server on which patch or antimalware server is running.

To configure Antimalware Notification:

1. Select **Configuration** in the ZENworks navigation menu and go to **Configuration** > **Security** > **Email Notification** > **Antimalware Email Notification.**
2. Type the desired email addresses in the **From**, **To**, and **CC** fields.
3. Click **Apply** to save changes.
4. Click the **Notification Servers** link in the Email Notification panel to go to that configuration and configure the SMTP Server and the Primary Server connection to it.

For more information about the Notification Servers configuration, see the **Notification Servers** Help page in the ZENworks application.

NOTE: ◆By default, the schedule to retrieve any newly detected malware and send email is 10 minutes and runs only on the Antimalware Server. To change the default value, update the `am.db.poll.batch.job.schedule` property in the `application.properties` file on the Antimalware Server.

For example, to change the default schedule setting from 10 minutes to 30 minutes, modify the property as: `am.db.poll.batch.job.schedule=0 */30 * ? * *`

Location of the application.properties file on the Linux server is: `/etc/opt/microfocus/zenworks/antimalware/application.properties`.

ZENworks no longer supports Windows Server as a Primary Server from version 24.2 onwards. For more information, see End of Windows Primary Server Support.

- The default email size is 25 MB. To change the default email size, update the `am.email.size property` in the `application.properties` file on the Antimalware Server.

  For example, to change the default email size from 25 MB to 50 MB, modify the property as: `am.email.size=50`

---

3 Policy Management

After configuring the required Antimalware settings and creating an Antimalware Enforcement Policy, you can view the policy settings with more granularity in the Details page of the policy. At that point, you can either make modifications to the settings or deploy the policy with base-level settings that you configured upon policy creation. Once the policy is enforced, you can also deploy custom Antimalware policies to exclude certain files from malware scans or to target specific threats or content.

The following sections, first provide information about creating custom policies (Custom Scan, Network Scan, and Scan Exclusions), and then provide information for modifying the more granular policy settings in the Details page of all four Antimalware policies:

Creating a Custom Scan Policy

The Custom Scan Policy is an optional policy that lets you supplement the scans provided by the base Antimalware Enforcement policy. Examples of this are targeting emerging threats that may not be covered by the regularly scheduled scans, or an every other month scan of all archive files on a device. This policy enables you to define and schedule scans on local and removable drives, in addition to the Full and Quick scans already defined in the Antimalware Enforcement Policy.

The policy wizard configures base-level and default settings for the policy. You can see and configure more details after policy creation. For information about modifying or customizing policy details after policy creation, see Custom Scan Policy.

The following instructions assume that you are on the **Select the Scan Level** page in the policy wizard for the Create New Antimalware Custom Scan Policy.

For information about creating policies in general, see "Creating Security Policies" in the *ZENworks Endpoint Security Policies Reference*.

- “Configure Scan Exclusions” on page 37
- “Assign and Publish the Policy” on page 37

Select the Scan Level

You can retain the most balanced approach between security and system performance by retaining the default setting of **Normal** or configure scans with greater security or with greater performance by choosing **Aggressive** or **Permissive**, respectively. Once the policy is created, you will have the option to make more specific configuration changes through the Details tab on the selected policy.

The descriptions below are the same shown for each scan level when selected in the page. They are also provided here in aggregate for comparison.

- **Aggressive:** Provides advanced security with moderate use of resources. Scans all files accessed from local drives including archived and lower risk files.
- **Normal:** Provides best balance between security and performance. Scans all files accessed from local drives. Does not scan archived and lower risk files.
- **Permissive:** Provides basic security with reduced use of resources. Scans application files accessed from local drives and incoming emails. Does not scan lower risk files, spyware, and less dangerous types of malware. This option is recommended only for use on devices with resource limitations.

Add the Scan Targets

Click **New** to add a scan target. Built-in options include **All Local Drives** or **All Removable Drives**, or you can adding a specific target and enter either a drive path or an environment variable, for example:

- `C:\Windows`
- `%WINDIR%\system32`

Once you add to or update the Scan Targets list, whichever items you have listed in the configuration are the targets that will be scanned.

NOTE: Ensure the paths or variables that you enter for scan targets are valid on the devices you assign the policy to. The policy does not validate these paths. In like manner, when the scan is run on devices, the Antimalware Agent runs the scan irrespective of a valid path. Invalid targets are simply logged as no malware detected.

Set the Scan Schedule

Choose one of the three options for the scan schedule and select **Wake-on-LAN** if you need that requirement for your scan. Information about each setting is provided below:

- **No Schedule:** Select this scheduling option if you do not want the scan to run automatically. This option has no preset to kickoff a scan. It is designed to allow the flexibility for running scans via the **Initiate Malware Scan** quick task, which you can initiate on a selected device when you

select the option in the quick task list or by entering a **zac command** in the Windows Command Prompt on the agent device. For more information about these options, see the following references:

- Antimalware Quick Tasks
- "Antimalware Commands" in the *ZENworks Command Line Utilities Reference*

- **Date Specific:** This schedule is designed to run a scan one or more times on the specified date(s) and time. For information about configuring this schedule, see Configure a Date Specific Schedule.
- **Recurring:** This schedule enables you to configure scans to run at a specified interval. For information about configuring this schedule, see Configure a Recurring Schedule.
- **Wake-on-LAN:** If the device is not on at the scheduled time, this option attempts to use Wake on LAN (WoL) technology to power on the device. The device must support Wake on LAN.

  For information about Wake-on-LAN options or how it works, see "Wake-on-LAN in ZENworks Control Center" in the *ZENworks Using Wake-on-LAN* reference.

Configure Scan Exclusions

Scan exclusions can include both built-in file exclusions and folders, files, and applications you designate for exclusion (custom). Built-in exclusions include Windows directories recommended for exclusion by Microsoft and some ZENworks directories, which can vary for Windows directories depending on the operating system. However, ZENworks built-in exclusions are not controlled by this setting. These items will not be scanned for the scan types you configure after the policy is created.

Custom exclusions can include exclusions added directly in the Exclusions tab of policy Details, exclusions implemented by selected Antimalware Scan Exclusion policies, or a combination of both. Exclusion types are designated as File, Folder, or Extension.

For information about configuring exclusions in the Custom Scan or Network Scan policies after policy creation, see Exclusions.

Assign and Publish the Policy

You can only assign Antimalware policies to devices. They cannot be assigned to users. For information about assigning and publishing Endpoint Security policies, see the topics below in the *ZENworks Endpoint Security Policies Reference*:

- "Assigning Security Policies"
- "Publishing Policies"

Creating a Network Scan Policy

The Network Scan Policy is optional, but it gives you the capability to scan network drives, which you cannot do with the Enforcement or Custom Scan policies. This policy gives you the capability to target a network drive from a specific device. For example, you could use this policy to scan a file storage disk in an array of disks.

Network Credentials

Network credentials must be configured in the policy to access network files. In order to configure this setting, you must already have credentials specified for the applicable network in the Credential Vault before you create this policy.

For information about adding credentials in the Credential Vault, see "Using the Credential Vault" in the *ZENworks Control Center Reference*.

The policy wizard configures base-level and default settings for the policy. You can see and configure more details after policy creation. For information about modifying or customizing policy details after policy creation, see Network Scan Policy. The following instructions assume that you are on the **Select the Scan Level** page in the policy wizard for the Create New Antimalware Network Scan Policy.

For information about creating policies in general, see "Creating Security Policies" in the *ZENworks Endpoint Security Policies Reference*.

- "Select the Scan Level" on page 38
- "Add the Scan Targets" on page 39
- "Set the Scan Schedule" on page 39
- "Configure Scan Exclusions" on page 39
- "Assign and Publish the Policy" on page 40

Select the Scan Level

You can retain the most balanced approach between security and system performance by retaining the default setting of **Normal** or configure scans with greater security or with greater performance by choosing **Aggressive** or **Permissive**, respectively. Once the policy is created, you will have the option to make more specific configuration changes through the Details tab on the selected policy.

The descriptions below are the same shown for each scan level when selected in the page. They are also provided here in aggregate for comparison.

- **Aggressive:** Provides advanced security with moderate use of resources. Scans all files accessed from local and network drives including archived and lower risk files.
- **Normal:** Provides best balance between security and performance. Scans all files accessed from local drives and application files accessed from network drives. Does not scan archived and lower risk files.
- **Permissive:** Provides basic security with reduced use of resources. Scans application files accessed from local and network drives and incoming emails. Does not scan lower risk files, spyware, and less dangerous types of malware. This option is recommended only for use on devices with resource limitations.

Add the Scan Targets

Click **New** to add a scan target. The target path must use IP address or FQDN format. As a best practice for a single network directory and file you should enter both the IP and FQDN paths. For example:

- `\\hostName\shareName\filePaths`
- `\\IPaddress\shareName\filePath`

Once you add to or update the Scan Targets list, whichever items you have listed in the configuration are the targets that will be scanned.

Network Scan File Credentials: To enable scans on network files, click  to browse and locate the applicable credential from the Credential Vault, and add the credentials in the `domain\user format`. For more information, see Network Credentials.

Set the Scan Schedule

Choose one of the three options for the scan schedule and select **Wake-on-LAN** if you need that requirement for your scan. Information about each setting is provided below:

- **No Schedule:** Select this scheduling option if you do not want the scan to run automatically. This option has no preset to kickoff a scan. It is designed to allow the flexibility for running scans via the **Initiate Malware Scan** quick task, which you can initiate on the policy when you select it in the quick task Policies list or by entering a **zac command** in the Windows Command Prompt on the agent device. For more information about these options, see the following references:
  - Antimalware Quick Tasks
  - "Antimalware Commands" in the *ZENworks Command Line Utilities Reference*
- **Date Specific:** This schedule is designed to run a scan one or more times on the specified date(s) and time. For information about configuring this schedule, see Configure a Date Specific Schedule.
- **Recurring:** This schedule enables you to configure scans to run at a specified interval. For information about configuring this schedule, see Configure a Recurring Schedule.
- **Wake-on-LAN:** If the device is not on at the scheduled time, this option attempts to use Wake on LAN (WoL) technology to power on the device. The device must support Wake on LAN.

  For information about Wake-on-LAN options or how it works, see "Wake-on-LAN in ZENworks Control Center" in the *ZENworks Using Wake-on-LAN* reference.

Configure Scan Exclusions

Scan exclusions can include both built-in file exclusions and folders, files, and applications you designate for exclusion (custom). Built-in exclusions include Windows directories recommended for exclusion by Microsoft and some ZENworks directories, which can vary for Windows directories depending on the operating system. However, ZENworks built-in exclusions are not controlled by this setting. These items will not be scanned for the scan types you configure after the policy is created.

Custom exclusions can include exclusions added directly in the Exclusions tab of policy Details, exclusions implemented by selected Antimalware Scan Exclusion policies, or a combination of both. Exclusion types are designated as File, Folder, or Extension.

For information about configuring exclusions in the Custom Scan or Network Scan policies after policy creation, see Exclusions.

Assign and Publish the Policy

You can only assign Antimalware policies to devices. They cannot be assigned to users. For information about assigning and publishing Endpoint Security policies, see the topics below in the *ZENworks Endpoint Security Policies Reference*:

- "Assigning Security Policies"
- "Publishing Policies"

Configuring a Custom or Network Policy Schedule

Reference the topics in this section for specific information on how to configure a Date Specific or Recurring schedule when creating an Antimalware Custom Scan or Antimalware Network Scan policy.

- "Configure a Date Specific Schedule" on page 40
- "Configure a Recurring Schedule" on page 41

Configure a Date Specific Schedule

The Date Specific scheduling option lets you specify one or more dates on which to run the scan.

NOTE: The following sections describe all of the Date Specific schedule options. Depending on the scan you are scheduling, some options might not be available.

- "Start Dates" on page 40
- "Run Event Every Year" on page 40
- "Process Immediately if Device Unable to Execute on Schedule" on page 41
- "Select When Schedule Execution Should Start" on page 41
- "Use Coordinated Universal Time (UTC)" on page 41

Start Dates

Click  to display a calendar you can use to select a date for the scan. You can add multiple dates one at a time.

Run Event Every Year

Select this option to run the scan every year on the dates shown in the **Start Date(s)** list.

Process Immediately if Device Unable to Execute on Schedule

A scan is considered past due if it is not executed on the configured schedule for some reason. If you select this option the past due scan is executed during the immediate device refresh.

NOTE: The scan is executed immediately after device refresh because the configured schedule which is passed does not recur.

Select When Schedule Execution Should Start

Select one of the following options:

- **Start Immediately at Start Time:** Starts the scan at the time you specify in the **Start Time** field.
- **Start at a Random Time between Start Time and End Time:** Starts the scan at a randomly selected time between the time you specify in the **Start Time** and **End Time** fields. You can use this option to avoid possible network overload from concurrently scheduled events.

Use Coordinated Universal Time (UTC)

The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

Configure a Recurring Schedule

The Recurring scheduling option lets you repeat the scan at a specified interval.

NOTE: The following sections describe all of the Recurring schedule options. Depending on the scan you are scheduling, some options might not be available.

- "When a Device Is Refreshed" on page 41
- "Days of the Week" on page 42
- "Monthly" on page 42
- "Fixed Interval" on page 43
- "Wake-on-LAN" on page 43

When a Device Is Refreshed

This schedule causes the scan to occur each time the ZENworks Agent performs a refresh on the device. If you want to delay the scan so that it does not happen immediately upon refresh, select the **Delay execution after refresh** option and specify the number of days, hours, or minutes you want to delay the scan.

Days of the Week

This schedule lets you specify the days during the week that you want the scan to run or to install updates. The action is run on these same days each week.

Select **Days of the Week**, then fill in the following fields:

- **Sun ... Sat:** Specifies the days of the week you want to execute the action.
- **Start Time:** Specifies the time you want to run the scan.
- **Process immediately if device unable to execute on schedule:** The action is considered past due if it is not executed on the configured schedule for some reason.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Start at a Random Time between Start Time and End Time:** Starts the action at a randomly selected time between the time you specify in the **Start Time** and **End Time** fields. You can use this option to avoid possible network overload from concurrently scheduled scans or updates.
- **Restrict Schedule Execution to the Following Date Range:** Limits executing the action to the time period specified by the starting and ending dates.

Monthly

This schedule lets you specify one or more days during the month to run the scan or install updates.

Select **Monthly**, then fill in the following fields:

- **Day of the Month:** Specifies the day of the month to execute the action. Valid entries are 1 through 31. If you specify 29, 30, or 31 and a month does not have those days, the action is not executed that month.
- **Last Day of the Month:** Executes the action on the last day of the month, regardless of its date (28, 30, or 31).
- ***First Sunday*:** Specifies a specific day of a week. For example, the first Monday or the third Tuesday. Click to add multiple days.
- **Start Time:** Specifies the time you want to execute the action.
- **Process Immediately if Device Unable to Execute on Schedule:** Any action is considered past due if it is not executed on the configured schedule for some reason.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Start at a Random Time between Start Time and End Time:** Executes the action at a randomly selected time between the time you specify in the Start Time and End Time boxes. You can use this option to avoid possible network overload from concurrently scheduled events.

- **Restrict Schedule Execution to the Following Date Range:** Limits executing the action to the time period specified by the starting and ending dates.

Fixed Interval

This schedule lets you specify an interval between days to run the scan or install updates. For example, you can execute the action every 14 days.

Select **Fixed Interval**, then fill in the following fields:

- **Months, Weeks, Days, Hours, Minutes:** Specifies the interval between times when the action is executed. You can use any combination of months, weeks, days, hours, and minutes. For example, both *7 days, 8 hours* and *1 week, 8 hours* provide the same schedule.
- **Start Date:** Specifies the initial start date for the interval.
- **Start Time:** Specifies the initial start time for the interval.
- **Process Immediately if Device Unable to Execute on Schedule:** A action is considered past due if it is not executed on the configured schedule for some reason. If you select this option:
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Restrict Schedule Execution to the Following Date Range:** Limits executing the action to the time period specified by the start date, end date, and end time.

Wake-on-LAN

If the device is not on at the scheduled time, this option attempts to use Wake-on-LAN technology to power on the device. The device must support Wake-on-LAN.

For information about Wake-on-LAN options or how it works, see "Wake-on-LAN in ZENworks Control Center" in the *ZENworks Using Wake-on-LAN* reference.

Creating a Scan Exclusions Policy

The Antimalware Scan Exclusions Policy is an optional policy that enables you to customize Antimalware scan exclusions of specified device files beyond what you may have already configured in other Antimalware policies. Once this policy is created, you can add the Scan Exclusions Policy option to the Custom Exclusions details of any of the three other Antimalware policies. The policy is then enforced based on the Scan Exclusions Policy and the Antimalware policy that this option is configured in having the same device or device folder assignment.

The following instructions assume that you are on the **Configure Scan Exclusions** page in the Create New Antimalware Scan Exclusions Policy wizard. For information about creating policies in general, see "Creating Security Policies" in the *ZENworks Endpoint Security Policies Reference*.

To configure Custom Exclusions, click **New** and save the configuration items in the New Exclusion dialog box for each exclusion that you add. The criteria required for the **Exclusion** field for each exclusion type is provided below:

NOTE: The **Process** exclusion type can only be used for the On-Access scan type.

- **File**, **Folder**, and **Process**:
  - Enter a path. For example:

    - Explicit: Used for exclusions in the on-demand scan types, Full, Quick, External Device, and Contextual, which are only applicable to local drives (fixed and removable), not to network mapped drives.
    - Folder: `C:\temp`
    - File: `E:\temp\Myfile.txt`

    - UNC path: Used for exclusions in the On-Access and Network scan types only. These path types are ignored if used for on-demand scans.
    - `\\hostName\shareName\filePath`
    - `\\IPaddress\shareName\filePath`

    NOTE: An exclusion path for an On-Access Scan can include any file path that the end user has rights to access.

  - Enter an environment variable. For example: `%ProgramFiles%`
  - Enter a wildcard. Use an asterisk (*) or double asterisk (**) to substitute for zero or more characters. Use a question mark (?) to substitute for exactly one character. Use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters. See the examples below. For example:
    - File exclusion in a location: `C:\Test\*` or `C:\Test\*.png`

      (excludes all files from the `Test` folder)
    - File exclusion in any location: `**\example.txt`

      (excludes any file named `example.txt` regardless of its location on the device)
    - Folder exclusion: `C:\Test\*`

      (excludes all folders from the `Test` folder)
    - Process exclusion:

      `C:\Program Files\WindowsApps\Microsoft.Not??.exe`

      (excludes the Microsoft Notes processes)

  NOTE: Process type exclusions require the name of the executable file, which can also include file names with wildcard characters.

- **Extension**: Enter one or more file extensions to be excluded from scanning, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example:

  `txt` or `.txt`

Assign and Publish the Policy

You can only assign Antimalware policies to devices. They cannot be assigned to users. For information about assigning and publishing Endpoint Security policies, see the topics below in the *ZENworks Endpoint Security Policies Reference*:

- "Assigning Security Policies"
- "Publishing Policies"

Antimalware Enforcement Policy

This section provides information about the settings you can view and modify in the Details page of a selected Antimalware Enforcement Policy. If you want to update settings on devices that already have the selected policy assigned, you need to republish the policy after making modifications, and then execute a refresh on those devices.

To open the Details page of the policy in ZENworks Control Center, navigate to **Policies**, select the policy in the Policies page or folder, click the policy name link, and select the **Details** tab.

On-Access Scan

On-access scans protect the device by preventing new malware threats from entering the system. This option scans local and network files when they are accessed (opened, moved, copied, or executed).

Scan Locations

You can configure which type of local files get scanned when they are accessed from the device. You can choose one of the three options below for each scan type, local or network as well as proscribe a limit on the size of files to be scanned. See the descriptions below to better understand what each option does:

- **All files:** Scans all files on the device or network except files excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement and Scan Exclusions Policy settings.

- **Applications only:** Scans only application files on the device except applications excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement Policy settings.

  For more information about the type of application files that get scanned or how to customize that list, see Application Only File Scans.

- **Defined file extensions only:** Scans only files that possess a file extension added in the Defined file extensions field for local files as applicable.

  Enter one or more file extensions to be scanned, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example: `txt` or `.txt`

- **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here (in MB). This option is provided to have some control on system performance related to scans. Since malware can also effect larger files, this option should be used with caution.

Scan Behavior

These settings provide some flexibility for configuring the behavior details of files to be scanned. Enable or disable as applicable to your desired protection in relation to system performance.

- **Scan only new or changed files:** This setting gives you an option that may improve system responsiveness with a minimum trade-off of security.
- **Scan boot sectors:** Boot sectors contain the required code to start the boot process. An infection could disable the drive and prevent the system from starting.
- **Scan for keyloggers:** Keyloggers record the input from the device's keyboard and can disclose sensitive information to hackers, including account numbers and passwords.
- **Scan for Potentially Unwanted Applications (PUA):** PUAs typically include undesirable programs that get installed on the device when bundled and downloaded with free software, often without the user's consent.
- **Scan archives:** Infected archive files are not an immediate threat and scanning them can be resource-intensive. Infected archive files are only a threat to the system if they are extracted from the archive and executed without having on-access scanning enabled.
  - **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here.
  - **Maximum depth (levels):** Defines the directory level depth that will be scanned, in increments of two.

  For information specific to scanning archived files, see About Scanned Archive Files.
- **Use deferred scanning:** Deferred scanning is selected by default and improves system performance by performing scans or copying scanned files when performance limitations are optimized.

Remediate Actions

Configure the default remediation action for infected files and suspect files. Each file type has a layered approach for the action taken, a default action and a secondary action if the default action fails. Configuration options are shown below:

File type	Default action	If default action fails:
Infected Files	◆ Deny Access ◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Deny Access ◆ Disinfect ◆ Delete ◆ Move to Quarantine
Suspect Files	◆ Deny Access ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Deny Access ◆ Delete ◆ Move to Quarantine

NOTE: For information about remediation of scanned archive files, see About Scanned Archive Files.

Full Scan

The Full Scan option is enabled by default. It is an on-demand scan that runs according to the schedule defined in the **Antimalware Agent Schedules** configuration. Full scans protect scan targets by checking for all types of malware threatening their security, such as viruses, spyware, adware, rootkits, and others.

Use this page to configure the types of files to scan, scan targets, scan behavior, and remediate actions, as defined below. You can also disable the feature entirely which might be needed temporarily when performing large scale operations such as migrations or software updates that use more resources.

- "User Rights" on page 47
- "Files to Scan" on page 48
- "Scan Targets" on page 48
- "Scan Behavior" on page 48
- "Remediate Actions" on page 49

User Rights

This setting enables you to configure rights for end users to initiate their own scans and pause, postpone, or cancel those scans as well as do the same for administrator-initiated scans, if so enabled.

The right for a user to cancel an administrator-initiated scan is disabled by default. The administrator can initiate a scan via a policy, quick task, or zac command.

NOTE: If the user pauses a scan and reboots the device before restarting the scan, the scan will resume on restart, but will no longer be visible to the user in the Agent Status Console.

Files to Scan

You can configure which type of files get scanned when the scheduled scan runs. See the descriptions below to better understand what each option does:

- **All files:** Scans all files on the device except files excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement and Scan Exclusions Policy settings.
- **Applications only:** Scans only application files on the device except applications excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement Policy settings.

  For more information about the type of application files that get scanned or how to customize that list, see Application Only File Scans.
- **Defined file extensions only:** Scans only files that possess a file extension added in the Defined file extensions field for local files as applicable.

  Enter one or more file extensions to be scanned, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example: `txt` or `.txt`

Scan Targets

The default scan targets for Full Scan are **All Local Drives** and **All Removable Drives**, but you can delete these entries if not needed. Once you modify the configuration, whichever items you have selected in the Scan Targets configuration, including additional added items if that be the case, are the targets that will be scanned. When adding targets, you can specify either a drive path or an environment variable, for example:

- `D:\`
- `%WINDIR%\system32`

Scan Behavior

These settings provide flexibility for configuring the behavior details of files to be scanned. Enable or disable as applicable to your desired protection in relation to system performance.

- **Scan only new or changed files:** This setting gives you an option that may improve system responsiveness with a minimum trade-off of security.
- **Scan boot sectors:** Boot sectors contain the required code to start the boot process. An infection could disable the drive and prevent the system from starting.
- **Scan registry:** This option scans the Windows Registry database that stores settings for operating system components.
- **Scan memory:** This option scans programs that run in the system's memory.
- **Scan for keyloggers:** Keyloggers record the input from the device's keyboard and can disclose sensitive information to hackers, including account numbers and passwords.
- **Scan for rootkits:** Rootkits enable administrator-level access to the device with a primary function of hiding processes, files, logins, and logs. When combined with malware, they can be used to conceal the presence of intruders.
- **Scan cookies:** This option scans cookies stored by browsers installed on the device.

- **Scan for Potentially Unwanted Applications (PUA):** PUAs typically include undesirable programs that get installed on the device when bundled and downloaded with free software, often without the user's consent.
- **Scan archives:** Infected archive files are not an immediate threat and scanning them can be resource-intensive. Infected archive files are only a threat to the system if they are extracted from the archive and executed without having on-access scanning enabled.
  - **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here.
  - **Maximum depth (levels):** Defines the directory level depth that will be scanned, in increments of two.
- **Scan email archives:** This option scans email files and databases, including the file formats of .eml, .msg, .pst, .dbx, .mbx, .tbb, and others.

IMPORTANT: This scanning option is resource-intensive.

Remediate Actions

Configure the default remediation action for infected files, suspect files, and rootkits. Each file type, except rootkit, has a layered approach to configure for action taken, a default action and a secondary action if the default action fails. Configuration options are shown below:

File type	Default action	If default action fails:
Infected Files	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore
Suspect Files	◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Delete ◆ Move to Quarantine ◆ Ignore
Rootkits	◆ Disinfect ◆ Ignore	(not applicable)

NOTE: For information about remediation of scanned archive files, see About Scanned Archive Files.

Quick Scan

The Quick Scan option is enabled by default. It is a reduced-scope on-demand scan that runs according to the schedule defined in the **Antimalware Agent Schedules** configuration. A quick scan typically runs in less than a minute and uses a fraction of the resources needed to run a full scan.

Quick scans protect scan targets by scanning new and changed files on local drives and removable drives including rootkits and PUAs. It also checks boot sectors and memory. If files detected with malware cannot be disinfected, they are quarantined.

Use this page to configure the types of files to scan, scan targets, scan behavior, and remediate actions, as defined below. You can also disable the feature entirely.

User Rights

This setting enables you to configure rights for end users to initiate their own scans and pause, postpone, or cancel those scans as well as do the same for administrator-initiated scans, if so enabled.

The right for a user to cancel an administrator-initiated scan is disabled by default. The administrator can initiate a scan via a policy, quick task, or zac command.

NOTE: If the user pauses a scan and reboots the device before restarting the scan, the scan will resume on restart, but will no longer be visible to the user in the Agent Status Console.

Files to Scan

You can configure which type of files get scanned when the scheduled scan runs. See the descriptions below to better understand what each option does:

- **All files:** Scans all files on the device except files excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement and Scan Exclusions Policy settings.
- **Applications only:** Scans only application files on the device except applications excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement Policy settings.

  For more information about the type of application files that get scanned or how to customize that list, see Application Only File Scans.
- **Defined file extensions only:** Scans only files that possess a file extension added in the Defined file extensions field for local files as applicable.

  Enter one or more file extensions to be scanned, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example: `txt` or `.txt`

Scan Targets

The default scan targets for Quick Scan are **%WINDIR%\system32** and **%temp%**. Once you modify the configuration, whichever items you have selected in the Scan Targets configuration, including additional added items if that be the case, are the targets that will be scanned. When adding targets, you can specify either a drive path or an environment variable, for example:

- `D:\`
- `C:\%USERPROFILE%\`

Scan Behavior

These settings provide flexibility for configuring the behavior details of files to be scanned. Enable or disable as applicable to your desired protection in relation to system performance.

- **Scan only new or changed files:** This setting gives you an option that may improve system responsiveness with a minimum trade-off of security.
- **Scan boot sectors:** Boot sectors contain the required code to start the boot process. An infection could disable the drive and prevent the system from starting.
- **Scan registry:** This option scans the Windows Registry database that stores settings for operating system components.
- **Scan memory:** This option scans programs that run in the system's memory.
- **Scan for keyloggers:** Keyloggers record the input from the device's keyboard and can disclose sensitive information to hackers, including account numbers and passwords.
- **Scan for rootkits:** Rootkits enable administrator-level access to the device with a primary function of hiding processes, files, logins, and logs. When combined with malware, they can be used to conceal the presence of intruders.
- **Scan cookies:** This option scans cookies stored by browsers installed on the device.
- **Scan for Potentially Unwanted Applications (PUA):** PUAs typically include undesirable programs that get installed on the device when bundled and downloaded with free software, often without the user's consent.
- **Scan archives:** Infected archive files are not an immediate threat and scanning them can be resource-intensive. Infected archive files are only a threat to the system if they are extracted from the archive and executed without having on-access scanning enabled.
  - **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here.
  - **Maximum depth (levels):** Defines the directory level depth that will be scanned, in increments of two.
- **Scan email archives:** This option scans email files and databases, including the file formats of .eml, .msg, .pst, .dbx, .mbx, .tbb, and others.

IMPORTANT: This scanning option is resource-intensive.

Remediate Actions

Configure the default remediation action for infected files, suspect files, and rootkits. Each file type, except rootkit, has a layered approach to configure for action taken, a default action and a secondary action if the default action fails. Configuration options are shown below:

File type	Default action	If default action fails:
Infected Files	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore
Suspect Files	◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Delete ◆ Move to Quarantine ◆ Ignore
Rootkits	◆ Disinfect ◆ Ignore	(not applicable)

NOTE: For information about remediation of scanned archive files, see About Scanned Archive Files.

External Device Scan

External device scans are enabled by default. When enabled, they automatically detect and scan removable storage devices and media when they are connected to the system, unless the Display Security Alerts option is enabled in the Antimalware Agent Notifications settings, in which case users are prompted to scan the external drive. If an infected file is detected, a disinfection routine will run on the file. Files that cannot be disinfected are placed in quarantine.

- “Devices to Scan” on page 52
- “Files to Scan” on page 53
- “Scan Behavior” on page 53
- “Remediate Actions” on page 54

Devices to Scan

Devices and media that are detected as external include:

- CDs and DVDs
- USB storage devices, to include flash drives and external-hard drives
- Devices with more storage than specified when connected

NOTE: You can configure Antimalware Agent notifications, alerts, and other options for endpoint users in the Antimalware Agent Notifications configuration. For more information, see Antimalware Agent Notifications.

Files to Scan

You can configure which type of files get scanned when the scheduled scan runs. See the descriptions below to better understand what each option does:

- **All files:** Scans all files on the device except files excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement and Scan Exclusions Policy settings.
- **Applications only:** Scans only application files on the device except applications excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement Policy settings.

  For more information about the type of application files that get scanned or how to customize that list, see Application Only File Scans.
- **Defined file extensions only:** Scans only files that possess a file extension added in the Defined file extensions field for local files as applicable.

  Enter one or more file extensions to be scanned, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example: `txt` or `.txt`

Scan Behavior

These settings provide flexibility for configuring the behavior details of files to be scanned. Enable or disable as applicable to your desired protection in relation to system performance.

- **Scan only new or changed files:** This setting gives you an option that may improve system responsiveness with a minimum trade-off of security.
- **Scan boot sectors:** Boot sectors contain the required code to start the boot process. An infection could disable the drive and prevent the system from starting.
- **Scan registry:** This option scans the Windows Registry database that stores settings for operating system components.
- **Scan memory:** This option scans programs that run in the system's memory.
- **Scan for keyloggers:** Keyloggers record the input from the device's keyboard and can disclose sensitive information to hackers, including account numbers and passwords.
- **Scan for rootkits:** Rootkits enable administrator-level access to the device with a primary function of hiding processes, files, logins, and logs. When combined with malware, they can be used to conceal the presence of intruders.
- **Scan cookies:** This option scans cookies stored by browsers installed on the device.
- **Scan for Potentially Unwanted Applications (PUA):** PUAs typically include undesirable programs that get installed on the device when bundled and downloaded with free software, often without the user's consent.

- **Scan archives:** Infected archive files are not an immediate threat and scanning them can be resource-intensive. Infected archive files are only a threat to the system if they are extracted from the archive and executed without having on-access scanning enabled.
  - **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here.
  - **Maximum depth (levels):** Defines the directory level depth that will be scanned, in increments of two.
- **Scan email archives:** This option scans email files and databases, including the file formats of .eml, .msg, .pst, .dbx, .mbx, .tbb, and others.

  IMPORTANT: This scanning option is resource-intensive.

Remediate Actions

Configure the default remediation action for infected files, suspect files, and rootkits. Each file type, except rootkit, has a layered approach to configure for action taken, a default action and a secondary action if the default action fails. Configuration options are shown below:

File type	Default action	If default action fails:
Infected Files	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore
Suspect Files	◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Delete ◆ Move to Quarantine ◆ Ignore
Rootkits	◆ Disinfect ◆ Ignore	(not applicable)

NOTE: For information about remediation of scanned archive files, see About Scanned Archive Files.

Contextual Scan

The Contextual Scan option is always enabled in the policy. However, Antimalware Agent Notifications must be enabled with the **Show icon in notification area** setting also enabled. With these options enabled, endpoint users can run scans on folders in File Explorer via the right-click menu. If either option is disabled, the option is not present in the right-click menu.

For more information about these notification settings, see Agent Notifications and End User Options.

- "Scan Behavior" on page 55
- "Remediate Actions" on page 56

Scan Behavior

These settings provide flexibility for configuring the behavior details of files to be scanned. Enable or disable as applicable to your desired protection in relation to system performance.

- **Scan only new or changed files:** This setting gives you an option that may improve system responsiveness with a minimum trade-off of security.
- **Scan boot sectors:** Boot sectors contain the required code to start the boot process. An infection could disable the drive and prevent the system from starting.
- **Scan registry:** This option scans the Windows Registry database that stores settings for operating system components.
- **Scan memory:** This option scans programs that run in the system's memory.
- **Scan for keyloggers:** Keyloggers record the input from the device's keyboard and can disclose sensitive information to hackers, including account numbers and passwords.
- **Scan for rootkits:** Rootkits enable administrator-level access to the device with a primary function of hiding processes, files, logins, and logs. When combined with malware, they can be used to conceal the presence of intruders.
- **Scan cookies:** This option scans cookies stored by browsers installed on the device.
- **Scan for Potentially Unwanted Applications (PUA):** PUAs typically include undesirable programs that get installed on the device when bundled and downloaded with free software, often without the user's consent.
- **Scan archives:** Infected archive files are not an immediate threat and scanning them can be resource-intensive. Infected archive files are only a threat to the system if they are extracted from the archive and executed without having on-access scanning enabled.
  - **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here.
  - **Maximum depth (levels):** Defines the directory level depth that will be scanned, in increments of two.
- **Scan email archives:** This option scans email files and databases, including the file formats of .eml, .msg, .pst, .dbx, .mbx, .tbb, and others.

IMPORTANT: This scanning option is resource-intensive.

Remediate Actions

Configure the default remediation action for infected files, suspect files, and rootkits. Each file type, except rootkit, has a layered approach to configure for action taken, a default action and a secondary action if the default action fails. Configuration options are shown below:

File type	Default action	If default action fails:
Infected Files	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore
Suspect Files	◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Delete ◆ Move to Quarantine ◆ Ignore
Rootkits	◆ Disinfect ◆ Ignore	(not applicable)

NOTE: For information about remediation of scanned archive files, see About Scanned Archive Files.

Quarantine

Each device has a local quarantine. The quarantine is an encrypted folder that contains malware-infected or malware-suspected files that have been detected by a scan. Quarantined files cannot do any harm because they cannot be executed or read.

Files are moved to quarantine based upon the scan remediation actions defined in the policies assigned to a device.

Quarantined files are sent to the Malware Research Lab on a regular basis to analyze and create routines for disinfection. If new signatures are created that can disinfect these types of files, those signatures will be included in the malware signature update, whereupon, the quarantined file will get disinfected and removed from quarantine.

All configurable options are enabled by default. For information about each option, see below:

- **Delete quarantined files older than (days):** This setting is provided to delete files that stay in quarantine for an extended period of time because the malware signatures updates have not provided a routine to disinfect the quarantined files. It cannot be disabled. The default setting to delete files is 30 days. The range for configuration is in increments from 1 to 180 days.
- **Submit quarantined files and critical threat data to Malware Research Lab every (hours):** You may want to configure this setting based on the amount of activity you get for quarantined files, while also considering conserving resources. Disabling this setting is not recommended. The default setting is every hour. The range for configuration is incremental from 1 to every 24 hours.

- **Rescan quarantine after malware signature updates:** This option is provided to disinfect quarantined files that could not be disinfected previously after a fix is included in a content update. Disabling this setting is not recommended. However, if your dashboard consistently shows low volume of quarantined files or the quarantined files are not essential to your daily operations, the flexibility is provided to disable the feature.
- **Copy files to quarantine before applying the disinfect action:** This option is provided to prevent data loss in case of false positives. You can restore legitimate files from quarantine from the Antimalware page on a selected device.
- **Allow users to take action on local quarantine:** Enables endpoint users to restore or delete files quarantined on their devices via Endpoint Security Agent Actions in the ZENworks Agent.

Exclusions

Scan exclusions can include both built-in file exclusions and custom exclusions. Built-in exclusions include Windows directories recommended for exclusion by Microsoft and some ZENworks directories. However, ZENworks built-in exclusions are not controlled by this setting. These built-in items will not be scanned for the scan types you configure in the policy. Scan types include, On-Access, Full, Quick, and Contextual scans.

For information about Microsoft recommended exclusions for Windows, see Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows.

Custom exclusions can include file exclusions added directly in the Custom Exclusions panel, exclusions implemented by assigned Antimalware Exclusion policies, or a combination of both. Scan types include, On-Access, Full, Quick, External Device, and Contextual scans. Scan Exclusion types are designated as File, Folder, Extension, or Process.

- **Built-in Exclusions:** Select the types of scans for which the built-in exclusions apply.
- **Custom Exclusions:** Select whether to apply Antimalware Exclusion policies assigned to the device, custom exclusions, or both.

  To add custom exclusions, click **New** after enabling custom exclusions and complete and save the configuration items in the New Exclusion dialog box for each exclusion that you add. The criteria required for the **Exclusion** field for each exclusion type is provided below:

  - **File**, **Folder**, and **Process**:
    - Enter a path. For example:

      - Explicit: Used for exclusions in the on-demand scan types, Full, Quick, External Device, and Contextual, which are only applicable to local drives (fixed and removable), not on network mapped drives.

      - Folder: `C:\temp`
      - File: `E:\temp\Myfile.txt`

      - UNC path: Used for exclusions in the On-Access and Network scan types only. These path types are ignored if used for on-demand scans. To ensure the path works in all environments, it is recommended that you enter the path using both formats.

      - `\\hostName\shareName\filePath`
      - `\\IPaddress\shareName\filePath`

NOTE: An exclusion path for an On-Access Scan can include any file path the end user has rights to access.

- Enter an environment variable. For example: `%ProgramFiles%`
- Enter a wildcard. Use an asterisk (*) or double asterisk (**) to substitute for zero or more characters. Use a question mark (?) to substitute for exactly one character. Use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters. See the examples below. For example:
  - File exclusion in a location: `C:\Test\*` or `C:\Test\*.png`

    (excludes all files from the `Test` folder)
  - File exclusion in any location: `**\example.txt`

    (excludes any file named `example.txt` regardless of its location on the device)
  - Folder exclusion: `C:\Test\*`

    (excludes all folders from the `Test` folder)
  - Process exclusion:

    `C:\Program Files\WindowsApps\Microsoft.Not??.exe`

    (excludes the Microsoft Notes processes)

NOTE: Process type exclusions require the name of the executable file, which can also include file names with wildcard characters.

- **Extension**: Enter one or more file extensions to be excluded from scanning, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example:

  `txt` or `.txt`

Custom Scan Policy

This section provides information about the settings you can view and modify in the Details page of a selected Antimalware Custom Scan Policy. If you want to update settings on devices that already have the selected policy assigned, you need to republish the policy after making modifications, and then execute a refresh on those devices.

The Custom Scan Policy is optional, but it gives you the capability to target specific threats that may not be covered in the regularly scheduled scans using the Antimalware Enforcement Policy. This policy enables you to define and schedule scans on local drives, other than the Full and Quick scans already defined in the Antimalware Enforcement Policy.

To open the Details page of the policy in ZENworks Control Center, navigate to **Policies**, select the policy in the Policies page or folder, click the policy name link, and select the **Details** tab.

Scan Settings

For the most part, the Scan Settings in the Custom Scan Policy mirrors several of the settings you can configure in the Antimalware Enforcement Policy, depending on the scan type. When you deploy this policy, it runs on the schedule you set in the Schedule tab of the policy, as opposed to the Antimalware Enforcement Policy, which runs on the zone Antimalware schedule. Reference the sections below for more information about these settings.

User Rights

This setting enables you to configure rights for end users to initiate their own scans and pause, postpone, or cancel those scans as well as do the same for administrator-initiated scans, if so enabled.

The right for a user to cancel an administrator-initiated scan is disabled by default. The administrator can initiate a scan via a policy, quick task, or zac command.

NOTE: If the user pauses a scan and reboots the device before restarting the scan, the scan will resume on restart, but will no longer be visible to the user in the Agent Status Console.

Files to Scan

You can configure which type of files get scanned when the scheduled scan runs. See the descriptions below to better understand what each option does:

- **All files:** Scans all files on the device except files excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement and Scan Exclusions Policy settings.
- **Applications only:** Scans only application files on the device except applications excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement Policy settings.

  For more information about the type of application files that get scanned or how to customize that list, see Application Only File Scans.
- **Defined file extensions only:** Scans only files that possess a file extension added in the Defined file extensions field for local files as applicable.

  Enter one or more file extensions to be scanned, separated by a semicolon “;”. You can enter extensions with or without the preceding dot. For example: `txt` or `.txt`

Scan Behavior

These settings provide flexibility for configuring the behavior details of files to be scanned. Enable or disable as applicable to your desired protection in relation to system performance.

- **Scan only new or changed files:** This setting gives you an option that may improve system responsiveness with a minimum trade-off of security.
- **Scan boot sectors:** Boot sectors contain the required code to start the boot process. An infection could disable the drive and prevent the system from starting.
- **Scan registry:** This option scans the Windows Registry database that stores settings for operating system components.

- **Scan memory:** This option scans programs that run in the system's memory.
- **Scan for keyloggers:** Keyloggers record the input from the device's keyboard and can disclose sensitive information to hackers, including account numbers and passwords.
- **Scan for rootkits:** Rootkits enable administrator-level access to the device with a primary function of hiding processes, files, logins, and logs. When combined with malware, they can be used to conceal the presence of intruders.
- **Scan cookies:** This option scans cookies stored by browsers installed on the device.
- **Scan for Potentially Unwanted Applications (PUA):** PUAs typically include undesirable programs that get installed on the device when bundled and downloaded with free software, often without the user's consent.
- **Scan archives:** Infected archive files are not an immediate threat and scanning them can be resource-intensive. Infected archive files are only a threat to the system if they are extracted from the archive and executed without having on-access scanning enabled.
  - **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here.
  - **Maximum depth (levels):** Defines the directory level depth that will be scanned, in increments of two.
- **Scan email archives:** This option scans email files and databases, including the file formats of .eml, .msg, .pst, .dbx, .mbx, .tbb, and others.

IMPORTANT: This scanning option is resource-intensive.

Remediate Actions

Configure the default remediation action for infected files, suspect files, and rootkits. Each file type, except rootkit, has a layered approach to configure for action taken, a default action and a secondary action if the default action fails. Configuration options are shown below:

File type	Default action	If default action fails:
Infected Files	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore
Suspect Files	◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Delete ◆ Move to Quarantine ◆ Ignore
Rootkits	◆ Disinfect ◆ Ignore	(not applicable)

NOTE: For information about remediation of scanned archive files, see About Scanned Archive Files.

Add the Scan Targets

Click **New** to add a scan target. Built-in options include **All Local Drives** or **All Removable Drives**, or you can adding a specific target and enter either a drive path or an environment variable, for example:

- `C:\Windows`
- `%WINDIR%\system32`

Once you add to or update the Scan Targets list, whichever items you have listed in the configuration are the targets that will be scanned.

NOTE: Ensure the paths or variables that you enter for scan targets are valid on the devices you assign the policy to. The policy does not validate these paths. In like manner, when the scan is run on devices, the Antimalware Agent runs the scan irrespective of a valid path. Invalid targets are simply logged as no malware detected.

Schedule

If you have a need to modify the schedule for when the scan runs and need more information, reference the configuration options below:

- **No Schedule:** Select this scheduling option if you do not want the scan to run automatically. This option has no preset to kickoff a scan. It is designed to allow the flexibility for running scans via the **Initiate Malware Scan** quick task, which you can initiate on a selected device when you select the option in the quick task list or by entering a **zac command** in the Windows Command Prompt on the agent device. For more information about these options, see the following references:
  - Antimalware Quick Tasks
  - "Antimalware Commands" in the *ZENworks Command Line Utilities Reference*
- **Date Specific:** This schedule is designed to run a scan one or more times on the specified date(s) and time. For information about configuring this schedule, see Configure a Date Specific Schedule.
- **Recurring:** This schedule enables you to configure scans to run at a specified interval. For information about configuring this schedule, see Configure a Recurring Schedule.
- **Wake-on-LAN:** If the device is not on at the scheduled time, this option attempts to use Wake on LAN (WoL) technology to power on the device. The device must support Wake on LAN.

  For information about Wake-on-LAN options or how it works, see "Wake-on-LAN in ZENworks Control Center" in the *ZENworks Using Wake-on-LAN* reference.

Exclusions

Scan exclusions can include both built-in file exclusions and folders, files, and applications you designate for exclusion (custom). Built-in exclusions include Windows directories recommended for exclusion by Microsoft and some ZENworks directories, which can vary for Windows directories depending on the operating system. However, ZENworks built-in exclusions are not controlled by this setting. These items will not be scanned for the scan types you configure after the policy is created.

Custom exclusions can include exclusions added directly in the Exclusions tab of policy Details, exclusions implemented by selected Antimalware Scan Exclusion policies, or a combination of both. Exclusion types are designated as File, Folder, or Extension.

- **Built-in Exclusions:** This option is recommended and selected by default, but you can disable it.
- **Custom Exclusions:** Select whether to apply Antimalware Scan Exclusion policies assigned to the device, custom exclusions, or both.

  To add custom exclusions, click **New** after enabling custom exclusions and complete and save the configuration items in the New Exclusion dialog box for each exclusion that you add. The criteria required for the **Exclusion** field for each exclusion type is provided below:

  - **File** and **Folder**:
    - Enter a path. For example:
      - Folder: `C:\temp`
      - File: `C:\temp\Myfile.txt`
    - Enter an environment variable. For example: `%ProgramFiles%`
    - Enter a wildcard. Use an asterisk (*) or double asterisk (**) to substitute for zero or more characters. Use a question mark (?) to substitute for exactly one character. Use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters. See the examples below. For example:
      - File exclusion in a location: `C:\Test\*` or `C:\Test\*.png`

        (excludes all files from the `Test` folder)
      - File exclusion in any location: `**\example.txt`

        (excludes any file named `example.txt` regardless of its location on the device)
      - Folder exclusion: `C:\Test\*`

        (excludes all folders from the `Test` folder)
  - **Extension**: Enter one or more file extensions to be excluded from scanning, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example:

    `txt` or `.txt`

Network Scan Policy

This section provides information about the settings you can view and modify in the Details page of a selected Antimalware Network Scan Policy. If you want to update settings on devices that already have the selected policy assigned, you need to republish the policy after making modifications, and then execute a refresh on those devices.

To open the Details page of the policy in ZENworks Control Center, navigate to **Policies**, select the policy in the Policies page or folder, click the policy name link, and select the **Details** tab.

Scan Settings

For the most part, the Scan Settings in the Custom Scan and Network Scan policies mirror several of the settings you can configure in the Antimalware Enforcement Policy, depending on the scan type. When you deploy either of these policies, they run on the schedule you set in the Schedule tab of the policy, as opposed to the Antimalware Enforcement Policy, which runs on the zone Antimalware schedule. Reference the sections below for more information about these settings.

User Rights

This setting enables you to configure rights for end users to initiate their own scans and pause, postpone, or cancel those scans as well as do the same for administrator-initiated scans, if so enabled.

The right for a user to cancel an administrator-initiated scan is disabled by default. The administrator can initiate a scan via a policy, quick task, or zac command.

NOTE: If the user pauses a scan and reboots the device before restarting the scan, the scan will resume on restart, but will no longer be visible to the user in the Agent Status Console.

Files to Scan

You can configure which type of files get scanned when the scheduled scan runs. See the descriptions below to better understand what each option does:

- **All files:** Scans all files on the specified network path except files excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement Policy settings.
- **Applications only:** Scans only application files on the specified network path except applications excluded from scans by built-in and custom exclusion settings defined in the Antimalware Enforcement Policy settings.

  For more information about the type of application files that get scanned or how to customize that list, see Application Only File Scans.

- **Defined file extensions only:** Scans only files that possess a file extension added in the Defined file extensions field for local files as applicable.

  Enter one or more file extensions to be scanned, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example: `txt` or `.txt`

Scan Behavior

These settings provide flexibility for configuring the behavior details of files to be scanned. Enable or disable as applicable to your desired protection in relation to system performance.

- **Scan only new or changed files:** This setting gives you an option that may improve system responsiveness with a minimum trade-off of security.
- **Scan boot sectors:** Boot sectors contain the required code to start the boot process. An infection could disable the drive and prevent the system from starting.
- **Scan registry:** This option scans the Windows Registry database that stores settings for operating system components.
- **Scan memory:** This option scans programs that run in the system's memory.
- **Scan for keyloggers:** Keyloggers record the input from the device's keyboard and can disclose sensitive information to hackers, including account numbers and passwords.
- **Scan for rootkits:** Rootkits enable administrator-level access to the device with a primary function of hiding processes, files, logins, and logs. When combined with malware, they can be used to conceal the presence of intruders.
- **Scan cookies:** This option scans cookies stored by browsers installed on the device.
- **Scan for Potentially Unwanted Applications (PUA):** PUAs typically include undesirable programs that get installed on the device when bundled and downloaded with free software, often without the user's consent.
- **Scan archives:** Infected archive files are not an immediate threat and scanning them can be resource-intensive. Infected archive files are only a threat to the system if they are extracted from the archive and executed without having on-access scanning enabled.
  - **Skip files larger than (MB):** Only scans files that are equal to or smaller than the size proscribed here.
  - **Maximum depth (levels):** Defines the directory level depth that will be scanned, in increments of two.
- **Scan email archives:** This option scans email files and databases, including the file formats of .eml, .msg, .pst, .dbx, .mbx, .tbb, and others.

  IMPORTANT: This scanning option is resource-intensive.

Remediate Actions

Configure the default remediation action for infected files, suspect files, and rootkits. Each file type, except rootkit, has a layered approach to configure for action taken, a default action and a secondary action if the default action fails. Configuration options are shown below:

File type	Default action	If default action fails:
Infected Files	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Disinfect ◆ Delete ◆ Move to Quarantine ◆ Ignore
Suspect Files	◆ Delete ◆ Move to Quarantine ◆ Ignore	◆ Delete ◆ Move to Quarantine ◆ Ignore
Rootkits	◆ Disinfect ◆ Ignore	(not applicable)

NOTE: For information about remediation of scanned archive files, see About Scanned Archive Files.

Add the Scan Targets

Click **New** to add a scan target. The target path must use IP address or FQDN format. As a best practice for a single network directory and file you should enter both the IP and FQDN paths. For example:

- `\\hostName\shareName\filePaths`
- `\\IPaddress\shareName\filePath`

Once you add to or update the Scan Targets list, whichever items you have listed in the configuration are the targets that will be scanned.

Network Scan File Credentials: To enable scans on network files, click  to browse and locate the applicable credential from the Credential Vault, and add the credentials in the `domain\user format`. For more information, see Network Credentials.

Schedule

If you have a need to modify the schedule for when the scan runs and need more information, reference the configuration options below:

- **No Schedule:** Select this scheduling option if you do not want the scan to run automatically. This option has no preset to kickoff a scan. It is designed to allow the flexibility for running scans via the **Initiate Malware Scan** quick task, which you can initiate on a selected device when you

select the option in the quick task list or by entering a **zac command** in the Windows Command Prompt on the agent device. For more information about these options, see the following references:

- Antimalware Quick Tasks
- "Antimalware Commands" in the *ZENworks Command Line Utilities Reference*

- **Date Specific:** This schedule is designed to run a scan one or more times on the specified date(s) and time. For information about configuring this schedule, see Configure a Date Specific Schedule.
- **Recurring:** This schedule enables you to configure scans to run at a specified interval. For information about configuring this schedule, see Configure a Recurring Schedule.
- **Wake-on-LAN:** If the device is not on at the scheduled time, this option attempts to use Wake on LAN (WoL) technology to power on the device. The device must support Wake on LAN.

  For information about Wake-on-LAN options or how it works, see "Wake-on-LAN in ZENworks Control Center" in the *ZENworks Using Wake-on-LAN* reference.

Exclusions

Scan exclusions can include both built-in file exclusions and folders, files, and applications you designate for exclusion (custom). Built-in exclusions include Windows directories recommended for exclusion by Microsoft and some ZENworks directories, which can vary for Windows directories depending on the operating system. However, ZENworks built-in exclusions are not controlled by this setting. These items will not be scanned for the scan types you configure after the policy is created.

Custom exclusions can include exclusions added directly in the Exclusions tab of policy Details, exclusions implemented by selected Antimalware Scan Exclusion policies, or a combination of both. Exclusion types are designated as File, Folder, or Extension.

- **Built-in Exclusions:** This option is recommended and selected by default, but you can disable it.
- **Custom Exclusions:** Select whether to apply Antimalware Scan Exclusion policies assigned to the device, custom exclusions, or both.

  To add custom exclusions, click **New** after enabling custom exclusions and complete and save the configuration items in the New Exclusion dialog box for each exclusion that you add. The criteria required for the **Exclusion** field for each exclusion type is provided below:

  - **File** and **Folder**:
    - Enter a path. The target path must use IP address or FQDN format. For example:
      - `\\hostName\shareName\filePath`
      - `\\IPaddress\shareName\filePath`
    - Enter an environment variable. For example: `%ProgramFiles%`
    - Enter a wildcard. Use an asterisk (*) or double asterisk (**) to substitute for zero or more characters. Use a question mark (?) to substitute for exactly one character. Use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters. See the examples below. For example:
      - File exclusion in a location: `\\IPaddress\shareName\Test\*` .png

        `\\IPaddress\shareName\Test\*.png`

(excludes all files from the `Test` folder)

- File exclusion in any location: `**\example.txt`

  (excludes any file named `example.txt` regardless of its location on the device)

- Folder exclusion: `\\IPaddress\shareName\Test\*`

  (excludes all folders from the `Test` folder)

- **Extension**: Enter one or more file extensions to be excluded from scanning, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example:

  `txt` or `.txt`

Scan Exclusions Policy

This section provides information about the settings you can view and modify in the Details page of a selected Antimalware Scan Exclusions Policy. If you want to update settings on devices that already have the selected policy assigned, you need to republish the policy after making modifications, and then execute a refresh on those devices.

To open the Details page of the policy in ZENworks Control Center, navigate to **Policies**, select the policy in the Policies page or folder, click the policy name link, and select the **Details** tab.

The **Custom Exclusions** configuration in the Antimalware Scan Exclusions Policy gives you the most comprehensive options for applying custom exclusions in the Antimalware Agent. You can tailor each exclusion that you add by one of the exclusion types (File, Folder, Extension, or Process), and by one or more scan types (On-Access, Full, Quick, External Device, Contextual, Network, and Custom).

When you assign both the Antimalware Scan Exclusions Policy and one or more of the Antimalware scan policies to a device with the **Use Antimalware Exclusions policies assigned to device** option selected under Custom Exclusions in the scan policy, the settings in the Antimalware Scan Exclusions Policy will be enforced.

To configure Custom Exclusions, click **New** and save the configuration items in the New Exclusion dialog box for each exclusion that you add. The criteria required for the **Exclusion** field for each exclusion type is provided below:

NOTE: The **Process** exclusion type can only be used for the On-Access and Full scan types.

- **File**, **Folder**, and **Process**:
  - Enter a path. For example:

    - Explicit: Used for exclusions in the on-demand scan types, Full, Quick, External Device, and Contextual, which are only applicable to local drives (fixed and removable), not on network mapped drives.

    - Folder: `C:\temp`
    - File: `E:\temp\Myfile.txt`

- UNC path: Used for exclusions in the On-Access and Network scan types only. These path types are ignored if used for on-demand scans. To ensure the path works in all environments, it is recommended that you enter the path using both formats.

- `\\hostName\shareName\filePath`
- `\\IPaddress\shareName\filePath`

NOTE: An exclusion path for an On-Access Scan can include any file path the end user has rights to access.

- Enter an environment variable. For example: `%ProgramFiles%`
- Enter a wildcard. Use an asterisk (*) or double asterisk (**) to substitute for zero or more characters. Use a question mark (?) to substitute for exactly one character. Use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters. See the examples below. For example:
  - File exclusion in a location: `C:\Test\*` or `C:\Test\*.png`

    (excludes all files from the `Test` folder)
  - File exclusion in any location: `**\example.txt`

    (excludes any file named `example.txt` regardless of its location on the device)
  - Folder exclusion: `C:\Test\*`

    (excludes all folders from the `Test` folder)
  - Process exclusion:

    `C:\Program Files\WindowsApps\Microsoft.Not??.exe`

    (excludes the Microsoft Notes processes)

NOTE: Process type exclusions require the name of the executable file, which can also include file names with wildcard characters.

- **Extension**: Enter one or more file extensions to be excluded from scanning, separated by a semicolon ";". You can enter extensions with or without the preceding dot. For example:

  `txt` or `.txt`

4 Running Scans

Antimalware scans are either on-access or on-demand scans. On-demand scans are automated using zone, override, and policy schedules, but can also be run by the administrator, and if so configured, also by end users. This section provides details about the different types of scans and the different options for running them.

On-Access Scans

On-access scans occur anytime an endpoint user opens, moves, copies or executes a local or network file, and in accordance with the On-Access settings in the Antimalware Enforcement Policy. This can include boot sectors and potentially unwanted applications (PUA).

On-Demand Scans

On-demand scans include all the scans described below:

- **Full Scan:** This scan is configured in the Antimalware Enforcement Policy. Full scans protect scan targets by checking for all types of malware threatening their security, such as viruses, spyware, adware, rootkits and others. The scan runs as follows:
  - According to the Antimalware Agent Schedule or override thereof on a device folder or device
  - When started from a quick task in ZENworks Control Center
  - When started from a zac command on the device
  - When started by an endpoint user from the Agent Status Console (if enabled in ZENworks Control Center)
- **Quick Scan:** This scan is configured in the Antimalware Enforcement Policy. This is a reduced-scope on-demand scan that typically runs in less than a minute and uses a fraction of the resources needed to run a full scan. The scan runs as follows:
  - According to the Antimalware Agent Schedule or override thereof on a device folder or device
  - When started from a quick task in ZENworks Control Center
  - When started from a zac command on the device
  - When started by an endpoint user from the Agent Status Console (if enabled in ZENworks Control Center)

- **Custom Scan:** This scan requires a Custom Scan Policy and gives you the capability to target specific threats that may not be covered in the regularly scheduled scans using the Antimalware Enforcement Policy.
  - According to the schedule set in the Custom Scan Policy
  - When started from a quick task in ZENworks Control Center
  - When started from a zac command on the device
- **Network Scan:** This scan requires a Network Scan Policy and gives you the capability to scan network drives, which you cannot do with the Enforcement or Custom Scan policies.
  - According to the schedule set in the Network Scan Policy
  - When started from a quick task in ZENworks Control Center
  - When started from a zac command on the device
- **External Device Scan:** When enabled, this scan automatically detects and scans removable storage devices and media when they are connected to the system, unless the Display Security Alerts option is enabled in the Antimalware Agent Notifications settings, in which case users are prompted to scan the external drive.
- **Contextual Scan:** When the **Show icon in notification area** setting is enabled Antimalware Agent Notifications, endpoint users can run scans on folders in File Explorer via the right-click menu and also using the Custom Scan option in the Agent Status Console.

Scan Type	Scheduled Scans	Quick Task Scans	zac Command Scans	User Initiated Scans
Full Scan	Yes	Yes	Yes	Yes (conditional)
Quick Scan	Yes	Yes	Yes	Yes (conditional)
Custom Scan	Yes	Yes	Yes	No
Network Scan	Yes	Yes	Yes	No
External Device Scan	No	No	No	Yes (conditional)
Contextual Scan	No	No	No	Yes (conditional)

NOTE: You cannot initiate another scan of the same type, Full or Quick, or of the same policy for a Custom Scan or Network Scan, until that scan completes or is stopped on the device in the Agent Status Console.

For information about running scans from a quick task or zac command, see the following:

- Quick task: Initiate Malware Scan
- zac command: "Antimalware Commands" in the *ZENworks Command Line Utilities Reference*.

For information about configuring scheduled scans or controlling end user scan options on devices with the Antimalware Agent installed, see the following sections:

- Antimalware Agent Schedules
- Antimalware Agent Notifications
- Policy Management

5 Monitoring Antimalware Status

If you have the Antimalware Database configured, you can monitor malware threats and Antimalware activity via dashlets in the Security Dashboard as well as view activity on a selected device from the Antimalware page, to include viewing specific details about detected malware threats. This section provides information about these two monitoring features and malware threat details.

Antimalware Dashlets

When ZENworks Endpoint Security is active in the zone, the ZENworks Control Center displays four Antimalware dashlets in the Security Dashboard by default. These dashlets give you the capability to monitor malware scans and threats and updates to the Antimalware Agent on devices that have the Antimalware Enforcement Policy enforced. You can also initiate scans and malware signature updates to those devices from specific dashlets. When you click **Security** in the ZENworks Control Center navigation panel, it takes you directly to the Security Dashboard.

Device Last Malware Scan

This dashlet displays scan activities for devices in your zone to monitor malware threats. By default, it displays information about any type of scan that was performed on devices for a specified time period. You can change the selected time periods based on your requirements. When you mouse over the chart, the time period and the number of threats detected during that time period are displayed.

Modify the Data Displayed

To filter the data displayed by the dashlet, expand and modify any of the sections in the following panels and apply the changes:

- **Filter Tab:** Enables you to view information about the last malware scan that was performed on the devices in the zone, based on filters such as the scan type, device folders, device groups, and operating system.
- **Time Filter Tab:** Enables you to filter the data based on the following time periods:

NOTE: Ensure that the time periods do not overlap with each other.

Duration	Time Period	Description	Additional Information
Up to	**Days**	This includes the time elapsed from now until 0:00 hours of the selected day. For example, if you configure this time filter Up to 1 Day at 5:30 PM on 16 April, all devices that were scanned from 12:00 AM, 15 April to 5:30 PM, 16 April are displayed.	◆ When you select the **Up to** filter, the From field is disabled. ◆ If you configure the time filter in weeks or months, each week is calculated as 7 days and each month is calculated from the selected day to the same day in the following month.
	Weeks	This includes the time elapsed from now until 0:00 hours of the selected week. For example, if you configure this time filter Up to 1 Week at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 9 April to 5:30 PM, 16 April will be displayed.	
	Months	This includes the time elapsed from now until 0:00 hours of the selected month. For example, if you configure this time filter Up to 1 Month at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 16 March to 5:30 PM, 16 April will be displayed.	

Duration	Time Period	Description	Additional Information
Between	**Days**	This includes the time elapsed between the two specified days. For example, if you specify the duration as 1 day to 7 days, and configure this time filter at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 9 April to 23:59 PM, 15 April.	◆ The **From** field should be less than the **To** field. ◆ If you configure the time filter in weeks/months, then each week is calculated as 7 days and each month is calculated as the same day on which the time filter was configured in the selected month.
	Weeks	This includes the time elapsed between two specified weeks. For example, if you specify the duration as 1 Week to 3 Weeks, and configure this time filter at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 26 March to 23:59 PM, 9 April will be displayed.	
	Months	This includes the time elapsed between two specified months. For example, if you specify the duration as 1 Month to 3 Months, and configure this time filter at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 16 January to 23:59 PM, 16 March will be displayed.	
More than	**Days**	This includes the time elapsed beyond the specified days. For example, if you configure the time filter as More than 30 days, at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 16 March and before will be displayed.	If you configure the time filter in weeks/months, then each week is calculated as 7 days and each month is calculated as the same day on which the time filter was configured in the selected month.
	Weeks	This includes the time elapsed beyond the specified weeks. If you configure the time filter as More than 3 Weeks, at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 27 March and before will be displayed.	
	Months	This includes the time elapsed beyond the specified months. If you configure the time filter as more than 2 Months, at 5:30 PM on 16 April, all devices that contacted the server from 12:00 AM, 16 February and before will be displayed.	

Execute Actions from the Device Panel

The Devices panel displays the scan details based on the selected filters. It provides information about the device, the scan type and the time at which the scan was run. The following actions can be performed on the filtered content, within the Devices panel:

Task	Description
Scan Now	Performs the selected type of scan on the selected devices. The scan options include Full, Quick, Custom, and Network. If you select Custom or Network, you need to browse and select the relevant Custom or Network Scan policy. **NOTE:** Custom Scan and Network Scan policies in the selection list are not filtered for device assignments when you select a policy for a Custom or Network scan, so you need to ensure the selected policy is assigned to the device.
Update Malware Signature	Forces a Malware Signature update on the selected devices if the signature is out dated.
Update Antimalware Agent	Forces an Antimalware Agent update on the selected devices if the Antimalware Agent is outdated on the selected devices.
Refresh	To update the scan related information in the dashlet.
Show or Hide columns	Click  to show or hide columns within the Devices panel.
Search	Filters the data displayed in the table by specifying the device name or the user name in the search field.

For general information about using the ZENworks Dashboard, reference the Help at Home > Dashboard.

Device Malware Status

This dashlet displays the malware status for individual devices in the zone, for a selected detection period. The malware status options include:

- Resolved: Displays the details of devices on which all the identified threats are resolved. The threats are resolved by placing them in quarantine, or by disinfecting or deleting them.
- Unresolved: Displays the details of devices on which, at least one threat has not been resolved as yet, meaning the file was ignored or blocked. Blocked files only occur with On-Access scans, in which case all access to the file is denied by the Antimalware Agent.
- No Threats: Displays the details of devices that do not have any threats.
- Unknown: Displays the details of devices that have not contacted the server in the last three days. This value can be configured based on your requirement. For more information, see Security Dashboard Configuration.

By default, this dashlet displays the device malware status for the last 24 hours. However, you can change the filters to view the malware status for the last 7 or 30 days. When you hover over the chart, the malware status and the associated number of devices are displayed.

Modify the Data Displayed

To modify the data that is displayed, expand the sections in the filter panel, modify the required filters and apply the changes. The data can be filtered based on the device folders, device groups, device type, operating system, threat status, and detection period.

Execute Actions from the Devices Panel

The Devices panel displays the scan details based on the selected filters. It provides information about the device, the scan type and the time at which the scan was run. Actions that can be performed within the Devices panel include:

Task	Description
Scan Now	Performs the selected type of scan on the selected devices. The scan options include full, quick, custom and network. If you select custom or network, you need to browse and select the relevant custom or network scan policy.
Update Malware Signature	Forces a Malware Signature update on the selected devices, if the signature is out dated.
Update Antimalware Agent	Forces an Antimalware Agent update on the selected devices if the Antimalware Agent is outdated on the selected devices.
Refresh	Updates the scan-related information in the dashlet.
Show or Hide columns	Click  to show or hide columns within the Devices panel.
Search	Filters the data displayed in the table by specifying the device name or the user name in the search field.

For general information about using the ZENworks Dashboard, reference the Help at Home > Dashboard.

Top Malware Threats

This dashlet displays the list of top malware threats in the zone. By default, the top malware threats are displayed based on the number of infected devices. You can modify the filters to display the top malware threats based on the most number of devices with unresolved threats or the most recently detected malware threats. You can also filter the data based on a particular threat type. The threat types include, Adware, Application, Archive Bomb, Dialer, Rootkit, Spyware and Virus. When you hover over each list item, the type of threat and the number of infected devices are displayed.

This dashlet can be customized to best fit your needs. You can also create multiple custom dashlets, if required. For example, you can create a dashlet for the Windrows 10 devices in the zone with the most number of threats or, you can create a dashlet to identity the top virus threat based on the number of devices impacted by it.

Modify the Data Displayed

To modify the data that is displayed, expand the sections in the filter panel, modify the required filters and apply the changes. The data can be filtered based on the device folders, device groups, device type, operating system, detection period and threat type.

Execute Actions from the Threats Panel

The Threats panel displays the threats based on the criteria defined in the filter panel. It provides information about the threat name, the number of devices impacted by the threat, the number of devices on which the threat is still unresolved and when the threat was first and last detected.

When you click a link in one of the applicable columns (Name, Total Devices, or Unresolved Devices), it will take you to a page that shows details for the threat on that row. Here you can view specific details about the threat and the devices it has infected. Links in the Name and Total Device column will display threat details that include all infected devices regardless of the Threat Status. Links in the Unresolved Devices column will display the threat details, but will only list infected devices that have an “Unresolved” threat status.

Other actions that can be performed within the Threats panel include:

Task	Description
Show or Hide columns	Click  to show or hide columns within the Threats panel.
Search	Filters the data displayed in the table by specifying the device name or the user name in the search field.

Device Malware Signature Version

This dashlet displays the list of Malware Signature versions that are installed on devices in the zone. The data is displayed by default in the form of a bar chart. You can apply the relevant filters to display the Malware Signature versions based on device folders, device groups, device types, operating systems and specific versions. When you hover over each list item, the type of threat and the number of infected devices are displayed.

If you want to view data for Antimalware Agent versions installed on devices, you can create a custom dashlet by selecting and applying the **Antimalware Agent Version** option under Primary or Secondary Grouping in the Group Data panel.

Modify the Data Displayed

To modify the data that is displayed, expand and modify any of the sections in the Filter panel or the Group Data panel and then apply your changes.

Filter Panel

The Filter panel enables you to view data based on device folders, device groups, device type, operating system, malware signature version and Antimalware Agent version.

Group Data Panel

To group the data and stack it in the chart, select the required options from the Primary Grouping and Secondary Grouping fields. When the Primary and Secondary data are grouped, the information is displayed as a stacked bar graph, else it is displayed as a bar graph.

Execute Actions from the Devices Panel

The Devices panel displays the devices that meet the criteria defined in the dashlet filter panel. You can also filter the list by searching for a particular device name in the search field.

For information about other actions and options you have in the Devices panel, see the following table:

Task	Description
Scan Now	Performs the selected type of scan on the selected devices. The scan options include Full, Quick, Custom, and Network. If you select Custom or Network, you need to browse and select the relevant Custom or Network Scan policy. **NOTE:** Custom Scan and Network Scan policies in the selection list are not filtered for device assignments when you select a policy for a Custom or Network scan, so you need to ensure the selected policy is assigned to the device.
Update Malware Signature	Forces a Malware Signature update on the selected devices if the signature is out dated.
Update Antimalware Agent	Forces an Antimalware Agent update on the selected devices if the Antimalware Agent is outdated on the selected devices.
Show or Hide columns	Click  to show or hide columns within the Devices panel.
Search	Filters the data displayed in the table by specifying the device name or the user name in the search field.

Antimalware Page

If you have the Antimalware Database configured, this page provides a snapshot status of malware threats, the scan schedule, and quarantined file information for the selected computer. You can also take specific actions on files, kickoff scans, and update the Antimalware Agent and Malware Signature versions on the computer. For more detailed information, see the topics for each section on the page.

- "Device Status" on page 77
- "Scan Schedule" on page 78
- "Malware Threats" on page 79
- "Files" on page 79

Device Status

The Device Status section enables you to quickly do the following for the selected device:

View malware threat status

The charts display data for three different time periods based on the last time the device reported its status. If the device last reported 12 hours ago, the 24 hour status is for the 24 hours prior to that report and so forth for 7 and 30 days.

The status indicators relate to the overall status of threats on the device by status level. For example, for a given time period, you could have a status of **Unresolved Threats** with 3 threats detected. However, only one of those threats would need to be unresolved to display that status.

A different color is associated with each status level:

- Unresolved Threats = Red
- Resolved Threats = Blue
- No Threats = Green

If the device has not reported within the last 3 days, the status is reported as **Unknown** by default. You can change the Unknown threshold using the **Security Dashboard** setting. For more information see, Security Dashboard Configuration.

View and update the Antimalware Agent or Malware Signature

Under Antimalware Agent and Malware Signature, respectively, you can view the version information and the last time either item was updated. You can also check for an update for either item by clicking **Update Now** under its respective heading. Each option opens the Quick Task Status window where you can start the task.

View quarantine file count and delete or restore them in bulk

The Quarantine section displays the total count of files placed in quarantine during the last 30 days. The options to **Delete All** or **Restore All** quarantine files is done in mass using a quick task. To delete or restore quarantine files by individual file selection, go to the Files panel on the Antimalware page. For information about the Files panel, see Files.

Scan Schedule

Lists the device's scan schedule for Full and Quick scans from the assigned Enforcement policy and from and all custom and network scans from the assigned Custom Scan and Network Scan policies. The Schedule link will automatically take you to where the schedule for the device is set, either the zone, device folder, or device.

NOTE: The time zone for Next Scan entries is based on the time zone of the browser used to log into the ZENworks Control Center. This time zone can be different on the actual device based on its location. To see if the two are different, mouse over the time displayed for **Last Contact** in the Summary page of the selected device, where a popup displays the time zone for both.

You can kick off any of the scans shown for the device, at will, by selecting the scan in the Scan Type column, and clicking **Run Scan**. This will open a quick task dialog box for the scan.

Malware Threats

The Malware Threats section enables you to view the status of malware events. You can filter the malware events by threat name or click on a specific threat in the Threat Name column to see details about the threat.

For information about threat details when you click a specific threat in the table, see Malware Threat Details.

Files

Shows the status (Disinfected, Quarantined, Deleted, Denied Access, Ignored) of both infected and suspicious files associated with the detected malware threats. Quarantined files can be restored or deleted if necessary, using a quick task. You can filter the list by either file name or threat name.

NOTE: If you remove the Antimalware Enforcement Policy from the device, the files shown in this list will persist for 30 days, at which point the history data will be cleaned up. There may also be a disparity from the Files count provided in the Malware Threats pane and the number of files in the list during this 30 day period.

Restore Files from Quarantine

To restore a file from quarantine:

1. Select the file in the Files list.
2. Click **Restore File from Quarantine** at the top of the table.
3. If you want to restore the file to a location different than the one shown in the table, select **New Location**, and enter the location using one of the formats below:
   - Local directory:

     `C:\Windows`

     `%WINDIR%\system32`
   - Network directory:

     `\\hostName\shareName\filePaths`

     `\\IPaddress\shareName\filePath`
4. Select the desired option boxes as defined below:
   - **Exclude restored file from future On-Access** or **On-demand scans**

     You might select either or both of these options if you continue to get the same file displaying as “suspicious” in the quarantine list.
   - **Overwrite if file exists in restore location**
5. Click **OK** to advance to the Quick Task Status window, and then click **Start** to execute the operation. You can leave the Quick Task Status open until the process completes, or click **Hide** and monitor the status from the Quick Tasks section under the ZENworks Control Center navigation panel.

Delete Files from Quarantine

To delete one or more files from quarantine:

1. Select the file or files in the Files list for deletion.
2. Click **Delete File from Quarantine** at the top of the table.
3. Click **Start** to execute the operation in the Quick Task Status window.

About Scanned Archive Files

When you have the **Scan archives** option enabled in Scan Behavior settings for any of the policies that run scans, Antimalware scans all types of archives (including email file formats). If the Antimalware Agent unzips the archive and finds an infected or suspicious file, it will perform the policy-configured remediation actions on the file, such as disinfecting or quarantining the file. It will then rezip the file.

If the agent cannot perform the configured remediation actions, it will take whatever actions it can to safeguard against the malware threat. This could include denying access to the entire archive.

If the agent cannot unzip the archive, it will ignore it.

While the list below is by no means inclusive of all supported archive formats, these are the most common:

```
7z; ace; alz; ar; arc; arj; boo; bz; bz2; bzip2; cab; chm; cpio; dbx; deb
(with gzip, bzip2, xz); dmg (with HFS); docfile; eml; esh; exe; ezs; fky;
frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hqx; hta; htm;
html; htt; iaf; icd; ico; img; inf; ini; inno; instyler; inx; ipf; iso;
installshield; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb;
lha; lzh; lnk; maf; mam; maq; mar; mat; mbx; mcr; mda; mdb; mde; mdt; mdw;
mem; mhtml; mid; mime; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms;
mscompress; msg; msi; mso; msp; mst; msu; nsis; nws; oab; obd; obi; obs;
obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak;
pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd;
psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram;
rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf;
scar; scr; script; sct; sdr; sfx; sh3; shb; shs; shw; sis; sit; sldm; sldx;
smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbb; tbz2;
td0; tgz; thebat; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url;
uuencode; vb; vbe; vbs; vbscript; vise; vwp; vxd; wav; wbk; wbt; wcm; wdm;
wise; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf;
wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt;
xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo
```

Malware Threat Details

This page provides detailed information about the threat and details of the devices that have been infected with the threat. The page is accessed by clicking a specific threat link in either the Antimalware page for a selected device or in the Top Malware Threats dashlet. Using the options in this page, you can perform scans, update the malware signature and update the Antimalware Agent on selected and infected devices.

Threat Information

This section displays the following information:

- Type: The type of threat. For example, virus, adware, spyware, application, archive bomb, application, rootkit or dialer.
- First Detected On: Date on which the threat was first detected on a device in the zone.
- Device First Detected On: Name of the device on which the threat was first detected. You must have rights to the device to display the name. Click the device name link to view the device details page.
- Last Detected On: Date on which the threat was last detected on a device in the zone.

Infected Devices

This section lists the names of devices that are infected with the selected threat along with the following information:

- Device details such as the device name, the device type (workstation or server), device status (normal, retired, lost), operating system, user associated with the device, when was the device last refreshed and when did the device last contact the server.
- Threat details such as the type of threat and when it was last detected on the device.
- File details such as the number of suspicious or infected files and the full path to these files. Click the files link, to view the files section within the device Antimalware page. This section provides information about the status of the infected or suspicious files. The threat status includes, Disinfected, Quarantined, Deleted, Denied Access, and Ignored.
- Scan details such as the types of scans, the scan schedule, which lists the details of the current schedule, the scan status (last and next scans) for the selected device, as well as the scan policy that will be implemented by each scheduled scan. To view the schedule configuration for a specific scan, click the link in the relevant scan schedule column.
- Other details such as the department and site associated with the device.

Actions

Using this page, you can perform the following actions:

- **Scan Now:** Performs the selected type of scan on the selected devices. The scan options include full, quick, custom and network. If you select custom or network, you need to browse and select the relevant custom or network scan policy.
- **Update Malware Signature:** Forces a Malware Signature update on the selected devices if the signature is out dated.
- **Update Antimalware Agent:** Forces an Antimalware Agent update on the selected devices if the Antimalware Agent is outdated on the selected devices.
- **Show or Hide columns:** Click to select the columns that you want to display or hide in the grid.
- **Filter panel:** Displays devices based on the selected filters. The filter options include Device Folders, Device Groups, Device Type, Operating System, Threat Status, Detection Period.

6 Antimalware Quick Tasks

You can initiate a variety of malware scans on devices or groups selected in the ZENworks Control Center via a quick task depending on the Antimalware policies deployed on those devices. You can also run quick tasks to update the Malware Signature or Antimalware Agent on devices that have the Antimalware Agent installed.

NOTE: Quick tasks on dynamic groups is conditional based on which group members have the Antimalware Agent installed. For this reason, even though a quick task may be enabled on a dynamic group, running the quick task will have no affect on unsupported group members.

Initiate Malware Scan

You can run the following scans on devices using the **Initiate Malware Scan** quick task when the Antimalware Enforcement Policy is deployed to those devices.

- Full Scan
- Quick Scan
- Custom Scan (Also requires Custom Scan Policy assignment)
- Network Scan (Also requires Network Scan Policy assignment)

You cannot initiate another scan of the same type, Full or Quick, or of the same policy for a Custom Scan or Network Scan, until that scan completes or is stopped on the device in the Agent Status Console.

To run the Initiate Malware Scan quick task:

1. Select the device(s) in **Devices** > **Workstations** (and sub-folder if applicable), and select **Initiate Malware Scan** in the Quick Tasks pull-down menu.
2. Choose the type of scan to run and click **OK**. If you are running a Custom or Network scan, use the browse feature to locate and select the applicable policy before clicking OK.

   NOTE: Custom Scan and Network Scan policies in the selection list are not filtered for device assignments when you select a policy for a Custom or Network scan, so you need to ensure the selected policy is assigned to the device.

   ---
3. Click **Start** in the Quick Task Status window to initiate the scan.

You can also initiate a Full or Quick Scan quick task from the Scan Schedule panel in the Antimalware page on a selected Device.

Update Malware Signature

Use the Update Malware Signature quick task on selected devices that have Antimalware enforced to ensure those devices have the latest malware signature content. Malware signature content is used to detect and disinfect files that are infected with malware.

To run the Update Malware Signature quick task:

1. Select the device(s) in **Devices** > **Workstations** (and sub-folder if applicable) and select **Update Malware Signature** in the Quick Tasks pull-down menu.
2. Click **Start** in the Quick Task Status window to start the signature update.

You can also run this quick task from the Device Status panel in the Antimalware page on a selected Device.

Update Antimalware Agent

Use the Update Antimalware Agent quick task on selected devices that have Antimalware enforced to ensure those devices have the latest software update for the Antimalware Agent.

To run the Update Antimalware Agent quick task:

1. Select the device(s) in **Devices** > **Workstations** (and sub-folder if applicable) and select **Update Antimalware Agent** in the Quick Tasks pull-down menu.
2. Click **Start** in the Quick Task Status window to start the agent update

You can also run this quick task from the Device Status panel in the Antimalware page on a selected Device.

Restore or Delete Files from Malware Quarantine

Two additional quick tasks, **Restore Files from Malware Quarantine** and **Delete Files from Malware Quarantine** can be executed on a specific device by accessing the Antimalware page for the device in the ZENworks Control Center. From this page you can restore or delete files in mass or select individual files in malware quarantine for restoration or deletion on the device.

For more information, reference the topics for “Device Status ”and “Files” in the Antimalware Page.

7 Antimalware Agent Details

The ZENworks Endpoint Security Antimalware Agent is installed on managed devices when you assign the Antimalware Enforcement Policy to those devices. This section provides information specific to the Antimalware Agent, including installation requirements, agent updates, end user options associated with agent notifications, uninstalling the agent, and lookup for error codes that could be encountered.

Agent Installation Requirements

The following prerequisites are required to install the Antimalware Agent on managed devices:

IMPORTANT: Ensure that the Policy Management agent feature is enabled and installed.

ZENworks no longer supports Windows Server as a Primary Server from version 24.2 onwards. For more information, see End of Windows Primary Server Support.

- Ensure that the managed device is supported (see Managed Device Requirements in ZENworks System Requirements) and is:
  - Windows 10 or newer
  - Windows Server 2012 or newer
- Ensure that managed devices have the recommended disk space and memory for the installation:
  - Disk space: 3 GB
  - RAM: 4 GB
- Activate ZENworks Endpoint Security Management and the Antimalware Entitlement.
- Remove any preexisting antimalware or antivirus programs from the devices. This includes completing any required reboots from software removal. Otherwise, the Antimalware Agent installation could require multiple reboots.

  The program will prohibit installation on Windows 10 devices that have antimalware or antivirus software installed, but this capability is not available on Windows Server operating systems.

NOTE: Microsoft Defender Antivirus is one exception to this requirement. The agent installation package removes this program from both Windows 10 and Windows Server operating systems prior to installation.

- Configure the Antimalware Server settings.
- Make any required changes to the installation schedule. The default setting is “at policy enforcement.”

  When assigning the policy to many devices at one time, care should be taken to minimize the impact of the agent download and installation on your Content Servers and network. best practice would be to ensure that assigned devices are on different refresh schedules (Configuration > Device Management > Device Refresh and Removal Schedule) or have different Antimalware Agent installation schedules (Configuration > Security > Antimalware Agent Schedules). You can randomize these settings by customizing them on the Settings tab of device folders and individual devices.
- Create an Antimalware Enforcement Policy.
- Assign the Antimalware Enforcement Policy to the devices and publish the policy.
- Follow up on Antimalware Agent installation status. In some cases (system dependent) end users may be prompted to reboot their devices to complete the installation.

For more information, see Antimalware Configuration.

Agent Updates

Updates to the Antimalware Agent are released periodically and the check for updates is built into the zone update schedule, which can be configured for a fixed interval or specific days and times during the week. There are also override options for this schedule at the device folder and device level. The default setting uses the fixed interval and checks for changes to the Antimalware Agent every 4 hours. When an update to the agent is detected, it is downloaded from the Antimalware Cloud Service through content servers and installed on the device. If a reboot is required, there are postpone reboot and enforce reboot settings that you can modify in the same schedule.

For information about modifying current settings in the update schedule, see Antimalware Agent Schedules.

If you have indication of an Antimalware Agent update failing to install, there could be one of several different causes, including a communication issue between the OCM and the CDN, inadequate disk space on the OCM or other content servers, an error downloading content, and so forth. To troubleshoot for a potential Antimalware issue, look for a cause in the ondemand-content-servlet log in the upstream OCM that communicates with the CDN. To troubleshoot for a potential issue with the update bundle, see “Troubleshooting” in the *ZENworks Software Distribution Reference*.

NOTE: Antimalware Agent updates can be similar in size to the original installation and the same recommendations for disk space, RAM, and scheduled distribution apply to updates. For more information, see Agent Installation Requirements.

Agent Notifications and End User Options

In the Antimalware Agent Notifications configuration, the **Show icon in notification area** option is enabled be default. If you leave this feature enabled, end users will have access to the Agent Status Console and all its features on the device when the Antimalware Enforcement policy is in effect. This includes the options to run Full, Quick, Custom, and Contextual scans on device folders and files. The latter scan option is run from the right-click menu in File Explorer, while the other three scans are run from the console.

NOTE: You can disable the user capability to run Full and Quick scans, without disabling the **Show icon in notification area** option, via the User Rights settings for Full Scan and Quick Scan in the Antimalware Enforcement Policy > Details page. Contextual scans can only be disabled from the **Show icon in notification area** option.

Agent Status Console

The Antimalware Agent Status Console is accessed by double-clicking the Antimalware Agent icon in the Windows notification area. The icon can also be added to the taskbar in Windows **Taskbar settings**. Accessing console features and console behavior is described below:

Icon	Description / Behavior
	**Antimalware Agent:** Located in the Windows notification area. Opens the Agent Status Console. When the Agent Status Console is opened on a device, an Event Log displays scan and update activity in the console.
	**Antimalware Issue:** If one or more issues are found from a scan, the Antimalware Agent icon is appended with a warning symbol.
	**Filter:** Opens a flyout panel in the Agent Status Console where filter options can filter which type of events show in the Event Log.
	**Scans:** Opens a flyout panel in the Agent Status Console where separate icons are provided to run Full, Quick, and Custom Scans, and to check for Antimalware Agent updates.
	**Modules:** Opens the modules panel where action can be taken on quarantined files.

NOTE: One of the options for end users in the Agent Status Console is the **View Log** link associated with scans displayed in the console. When clicked, data is displayed in the console in expandable groupings that show more details. While the events will still display in the console once policy changes are refreshed on the device, the logs of all events that predate a policy change will no longer be accessible to the end user.

Postpone Reboot Option

If you have **Postpone reboot** enabled in the Antimalware Agent Update Schedule and **Display restart notifications** enabled in the Antimalware Agent Notifications configuration, users will be notified of and have the option to postpone any reboots required from Antimalware Agent updates.

Disabling the Show Icon Option

If you disable the **Show icon in notification area** option in the Antimalware Agent Notifications configuration and refresh devices with the Antimalware Agent installed or before deploying the Antimalware Enforcement Policy, all the options above will be hidden from end users. Additionally, users will not receive notifications from Antimalware Agent activity.

All the settings in the Antimalware Agent Notifications configuration have detailed descriptions which you can read for more information.

Uninstalling the Antimalware Agent

There are three ways you can uninstall the Antimalware Agent from a managed device:

- Remove the Antimalware Enforcement Policy assignment from the device in ZENworks Control Center

  If you remove the policy assignment, there is a 10 minute delay before the removal starts. This delay provides a way to prevent the uninstall through policy removal if you want to replace the policy with another Antimalware Enforcement Policy. If a new policy is applied with a device refresh before the 10 minutes expire, removal of the Antimalware Agent will be ignored.
- Uninstall the ZENworks Agent
- Run the `zac malware-remove-agent` or `zac mr` command from the command line on the device

  The Antimalware Agent does display in the Windows Program and Features list as “ZENworks Endpoint Security”, but for security reasons, you cannot uninstall the agent using Windows.

For more in formation about Endpoint Security policy removal in general, see “Policy Removal” in the *ZENworks Endpoint Security Policies Reference*.

Unregistering a Device with the Antimalware Agent

If you unregister a device that has the Antimalware Agent installed, the agent remains on the device unless you reregister the device in another zone or the same zone with the Antimalware Policy not assigned to the device. This behavior precludes unnecessary removal of the agent when moving a device to another zone.

Error Code Lookup

The errors listed below are the ones you are most likely to see on the Antimalware Agent. In most cases subsequent updates will clear the error. If you encounter an error not shown here or have an issue that you cannot resolve, contact Micro Focus Support.

Error Code	Description
-1002	Could not resolve server.

Error Code	Description
-1008	This error is caused by the Antimalware Agent being unable to contact a Content Server for its updates.

Troubleshooting

Antimalware agent displays "You are at risk" alert message

An Antimalware agent device has access to the On-demand Content Master (OCM) server, and can successfully update its agent and signature versions. If the device has no direct access to the internet, then the following alert message is displayed:

"You are at risk"

"The connection to Cloud Services could not be established. You are not fully protected. Please contact your system administrator."

Cause: The Antimalware agent requires access to the following addresses:

nimbus.bitdefender.net

The agent will try to resolve this directly. If it cannot, the agent displays the "You are at risk" error.

Workaround:

In ZCC, go to Configuration > Security > Antimalware Agent Notifications and change the "Cloud Services unavailable" notification from "Critical" to "Warning", this will suppress the message.

This may affect detection rates, as access to Cloud Services provides an additional level of detection for suspicious files beyond what is available from the local scan engine heuristics.

OR

Allow agents to directly access nimbus.bitdefender.net on port 443

Unable to Install Antimalware Agent on Windows Devices

Unable to install Antimalware Agent on Windows devices without updating the custom platform support.

Workaround: Add the mapping entry for the windows version in windowsVersionMapping.properties file.

Antimalware Agent is installed even if another Antivirus is available on the Server

On a Server, ZENworks Antimalware agent is downloaded and installed even if another Antivirus is already available.

Workaround: Ensure that you uninstall the existing antivirus, and then install Antimalware.

An exception is Logged While Copying Data from Antimalware History Table

The following exception message is logged in the Antimalware log file while copying data from the Antimalware history table:

Failed to persist the data using bulk copy.

While configuring the Antimalware Database, ensure that you use public as the schema name for PostgreSQL and dbo as the schema name for MS SQL. If you have specified any other schema name, then you might face this issue.

Workaround: Ensure that you provide the above-mentioned schema names.

Antimalware Service Fails to Start as Port 61100 is used by Kafka

Unable to start the Antimalware service as the port 61100 is being used by Kafka.

Workaround: Restart the server.