ZENworks 2017 Update 4
Endpoint Security Agent Reference

January 2019

Legal Notice

Contents

About This Guide

The *ZENworks Endpoint Security Agent Reference* provides information to help you manage the Endpoint Security Agent.

Audience

This guide is intended for ZENworks administrators who need to configure, manage, and troubleshoot the Endpoint Security Agent.

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 Enabling and Disabling the Endpoint Security Agent

The Endpoint Security Agent is the ZENworks Agent module that is responsible for enforcing security policy settings on managed devices. Because it is a module, it can be installed, enabled, disabled, and uninstalled without affecting the other capabilities provided by the ZENworks Agent. The following operational states are possible for the Endpoint Security Agent:

- **Installed and enabled:** All effective security policies are enforced.
- **Installed and disabled:** The Endpoint Security Agent remains installed but does not enforce any security policies assigned to the user or device.
- **Uninstalled:** The Endpoint Security Agent is removed from the device.

By default, the Endpoint Security Agent is installed and enabled on managed devices if ZENworks Endpoint Security Management is activated (license or evaluation). If you want to change the operational state of the agent, see the instructions in "Customizing the Agent Features" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

2 Moving a Managed Device From One Zone to Another Zone

The following sections provide instructions to help you move a managed device that has the Endpoint Security Agent installed from one zone to another zone:

Moving a Device to a Zone Where Endpoint Security Management Is Not Active

When you move a device to a zone where Endpoint Security Management is not active (or the Endpoint Security Agent feature is disabled or not installed with the ZENworks Agent), all security policies are cleared from the device and the Endpoint Security Agent is either uninstalled or disabled.

To move a device:

1. If a Data Encryption policy is applied to the device, have the device's user decrypt files by moving the encrypted files from encrypted removable storage devices to non-encrypted folders on the device.

   Alternately, you can move the device and then decrypt the files by using the ZENworks File Decryption Utility (Admin edition). For information about the utility, see "File Decryption Utility" in the *ZENworks Endpoint Security Utilities Reference*.
2. Unregister the device. See "Unregistering a Device" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

   This clears all security policies and removes the device as a registered device in the zone.
3. Register the device in the new zone. See "Manually Registering a Device" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

   After the device registers in the zone, the ZENworks Agent uninstalls or disables the Endpoint Security Agent. It is uninstalled if the Endpoint Security Management license is not active or if the Endpoint Security Agent is not configured as an installed feature of the ZENworks Agent. It is disabled if the license is active but the agent is configured as a disabled feature of the ZENworks Agent.

Moving a Device to a Zone Where Endpoint Security Management Is Active

To move a device to a zone where Endpoint Security Management is active and the Endpoint Security Agent is an enabled feature for the ZENworks Agent:

1. Unregister the device. See "Unregistering a Device" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

   This clears all security policies and removes the device as a registered device in the zone.

2 Register the device in the new zone. See “Manually Registering a Device” in the *ZENworks Discovery, Deployment, and Retirement Reference*.

3 If the device had a Data Encryption policy applied to it in the old zone, export the data encryption keys from the old zone and import them into the new zone. See *ZENworks Endpoint Security Policies Reference*.

3 Working with the Endpoint Security Agent

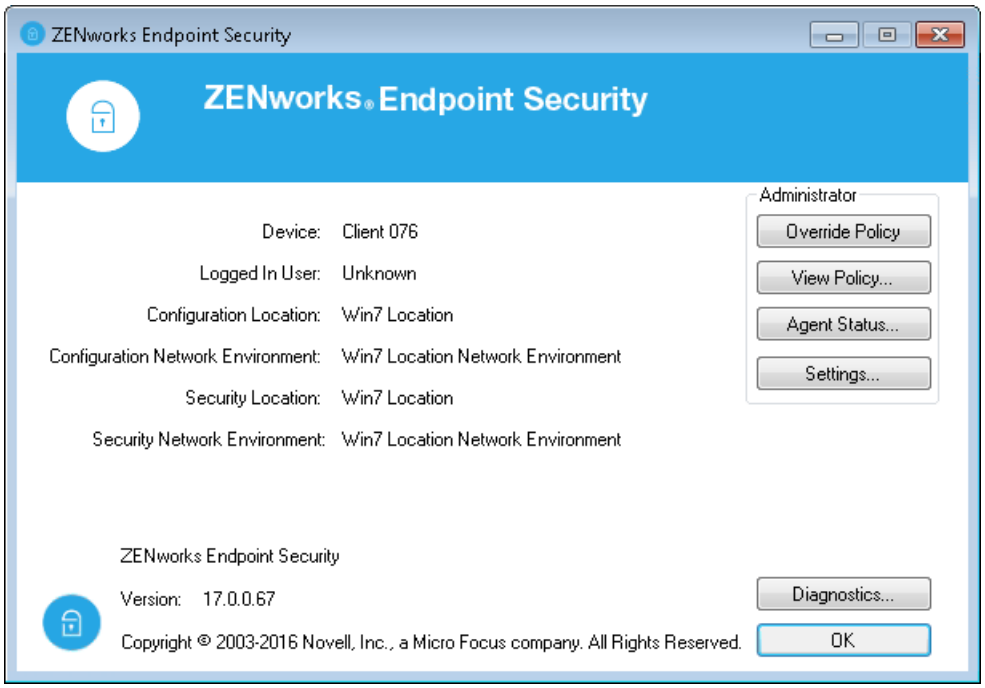
With the Endpoint Security Agent features on a managed device, you can make several configuration changes, create diagnostic packages, and view agent module, logging events, and policy assignments. Many of these features require an Administrator override password that is enabled in the ZENworks Control Center.

You access options for the ZENworks Endpoint Security Agent beginning in the ZENworks Agent window on a managed device. Endpoint Security options other than file encryption and decryption are managed through the Agent About dialog box.

Accessing Endpoint Security

To open the Endpoint Security Agent About dialog box:

1. Access the client device with the ZENworks Agent installed and Endpoint Security Management enabled in the ZENworks Control Center.
2. On the device, right-click the ZENworks icon in the notification area, and select **Technician Application**.
3. In the ZENworks Agent navigation menu, click **Endpoint Security**.
4. In the **Endpoint Security Agent Actions** section, click **About** to display the Agent About dialog box.



Creating a Diagnostics Package

If Technical Support is helping you resolve an Endpoint Security Agent issue on one of your devices, you might be asked to generate a diagnostic package for Support to review. This package contains information about the device's Group Policy object, registry settings, system, and system events.

To create a diagnostics package:

1. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
2. Click **Diagnostics**.
3. Select the information to be included in the package.

   Group Policy Object: Captures the current GPO for the user/device as designated by your directory service.

   Last Memory Dump: Captures the last memory dump generated by the device.

   Registry Settings: Captures the device's current registry settings.

   System Information: Captures the device's system information.

   System Event Logs: Captures the device's current System Event logs.
4. Click **Create Package** to generate the package.

   The generated package (`ZESDiagnostics_YYYYMMDD_HHMMSS.zip.enc`) is saved on the desktop. This file is encrypted and can only be viewed by Micro Focus Support.

Viewing the List of Agent Modules

You can view a list of the Endpoint Security Agent modules that are currently loaded on a device. The list displays each module with its date and version.

1. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
2. Click **Diagnostics**.
3. Click **Module List**.
4. After you finish viewing the module list, click **Close** to exit the dialog box.

Logging Agent Events

The Endpoint Security Agent logs information to the device's local disk. This includes events related to application control, firewall management, hardware device control, data encryption, and much more.

By default, the logging level is set to Warning. If necessary, you can change it to Debug, Informational, or Error to gather more or less information. Log files, which are named `Log_YYYYMMDD_HHMMSS_NNNN.txt`, are located in the following hidden directory:

Windows 7/8/10: `c:\ProgramData\Novell\ZES\Logs`

For troubleshooting, you should set logging according to the directions of Micro Focus Support and re-create the circumstances that led to the error to see if it can be repeated.

To change the logging level:

1. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
2. Click **Diagnostics**.
3. Click **Logging**.
4. Change the logging levels as desired.

   By default, all logging events are set to **Warning**, but you can set each listed event to the following:

   Debug: Turns on every possible message and includes Informational, Warning, and Error messages.

   Informational: Records all events when they occur, such as when a network connection event begins and ends.

   Warning: Records errors that have occurred but are solvable and do not prevent the client from running.

   Error: Records errors that have occurred and prevent the client from running.
5. If you want to save the new settings as the default settings, select **Save as Defaults**.

   The settings become the new default settings. If you change the settings at a later time and then decide that you want to go back to the default settings, you can click **Restore Defaults**.
6. To insert a comment into the current log file, click **Add Comment**, type the comment, then click **OK**.
7. Click **OK** to exit the dialog box.

Viewing Policy Assignments

You can view a list of the security policies that are assigned to the device. The list divides the security policies by assignment type: user, device, and zone.

1. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
2. Click **Diagnostics**.
3. Click **Policy List**.

   The list includes a tab for each assignment type: user, device, and zone. All user, device, and zone-assigned policies are displayed on these three tabs. If a policy type (such as a VPN Enforcement policy or Application Control policy) is not applied to the device through one of these three assignment types, the Endpoint Security agent applies its system (resource) policy to the device. The Other tab displays the policies for which the system (resource) policy is being applied, and also displays the management settings configured in the zone (ZSettings).
4. After you finish viewing the policy assignments, click **Close** to exit the dialog box.

Overriding Security Policies

The Endpoint Security Agent includes a policy override feature that disables the current security policies. All policies are disabled except for the Data Encryption policy, which continues to be enforced.

To override the security policies on a device:

1. Make sure you have enabled the device to accept an override password. For information, see Appendix A, “Override Password,” on page 19.
2. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
3. Click **Override Policy**.
4. Specify the override password or the override password key, and click **Override**.

   The **Override Policy** button changes to **Load Policy**.

   The override stays in effect until one of the following occurs:

   - The **Load Policy** button is clicked.
   - The device reboots.
   - If an override password key was used, the maximum override time expires or the key expires.

Viewing Effective Policies

Each policy type (Firewall, Application Control, USB Connectivity, and so forth) has one effective policy that is enforced on the device per location. The effective policy is created by merging all of the user, device, and zone assigned policies of that type according to established ordering and merging rules (see “How the Effective Policy is Determined” in the *ZENworks Endpoint Security Policies Reference*). The Endpoint Security Agent lets you view the effective policies for the device.

To view the effective policies in the Endpoint Security Agent:

1. Make sure you have enabled the device to accept an override password. For information, see Appendix A, “Override Password,” on page 19.
2. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
3. Click **View Policy**.
4. Specify the override password or the override password key, and click **OK**.

   The View Policy dialog box includes a tab for each policy type.

   Each policy type includes the following:

   Location list: All policies might not be available in all locations. Therefore, the effective policy can be different from one location to another. This list lets you select the location whose effective policy you want to view. The Data Encyption, Security Settings, VPN Enforcement, and Location Assignment policies are global-only policies; they do not have a location list because the effective policy is the same regardless of the location.

   Policy settings: The location’s effective policy settings are displayed in one or more sections after the location list. These settings are a result of the ordering and merging rules used to determine the effective policy.

Location Source: This section lists both the Location Assignment policies that are the source of the currently selected location and the policies that are the source of the effective policy settings.

The  icon identifies a global policy. The  icon identifies a location-based policy. This section is not displayed for policy types that support only global policies (Data Encyption, Security Settings, VPN Enforcement, and Location Assignment).

Merged Policies: This section lists all of the policies available for the available locations, regardless of the currently selected location (or no location for global-only policies). For example, if there are four available locations included in the Locations list, the policies that apply to any of the four locations are shown in the list. This list does not change when you change the location to view the effective policy for that location.

In addition to the tabs for each policy type, the **Report Settings** tab displays the report settings that are currently effective on the device. The **Location Relations** tab shows all available security locations for the device and the related network environments.

5 After you finish viewing the policy assignments, click **Close** to exit the dialog box.

Viewing Status Information

The Endpoint Security Agent provides a variety of status information related to the enforcement of security policies on the device. For example, the agent displays the current enforcement settings for the Firewall policy and resulting firewall activity. The agent also lists the detected USB devices and whether or not they can be accessed based on the USB Connectivity policy settings. This is just a small sample of the extensive status information available in the agent.

To view the Endpoint Security Agent status information:

1 Make sure you have enabled the device to accept an override password. For information, see Appendix A, “Override Password,” on page 19.

2 Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.

3 Click **Agent Status**.

4 Specify the override password or the override password key, and click **OK**.

The Agent Status dialog box includes a variety of tabs with different information. The displayed tabs can change depending on the policies assigned to the device.

5 After you finish viewing the status pages, click **Close** to exit the dialog box.

Clearing Security Policies

The Endpoint Security Agent allows you to clear assigned security policies. Clearing policies is different than overriding policies (see Overriding Security Policies). When you override policies, the policies can be reloaded during the current session and the Data Encryption policy is not affected. When you clear policies, all policies, including the Data Encryption policy, are removed and are not replaced until the Windows device reboots and the Endpoint Security Agent refreshes its information from the ZENworks Server.

When you clear policies, you can choose to clear all policies, device-assigned policies, user-assigned policies, zone-assigned policies, and system (or resource) policies. This, in combination with viewing the effective policies (see Viewing Effective Policies) and the status information (see Viewing Status Information), can provide important information as you troubleshoot issues with policy enforcement.

To clear security policies from a device:

1. Make sure you have enabled the device to accept an override password. For information, see Appendix A, “Override Password,” on page 19.
2. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
3. Click **Settings**.
4. In the Policy section, select the policies you want to clear:

   Device: Clears all device-assigned policies.

   User: Clears all user-assigned policies.

   Zone: Clears all zone-assigned policies.

   System: Clears the Endpoint Security Agent’s internal (resource) policies.

   All: Clears all policies.
5. Click **Clear Policy**.
6. After you finish clearing policies, click **Close** to exit the dialog box.

Configuring Agent Self Defense

The Endpoint Security Agent includes self-defense functionality that can prevent it from being shut down, disabled, or tampered with in any way. If a user performs any of the following activities, the device is automatically rebooted to restore the correct system configuration:

- Using Windows Task Manager to terminate any Endpoint Security Agent processes.
- Stopping or pausing any Endpoint Security Agent services.
- Removing critical files and registry entries. If a change is made to any registry keys or values associated with the Endpoint Security Agent, the registry keys or values are immediately reset.
- Disabling NDIS filter driver binding to adapters.

By default, agent self defense is not enabled.

Enable Self Defense

Agent self defense is enabled or disabled through the Agent Security settings in ZENworks Control Center.

1. In ZENworks Control Center, click **Configuration**.
2. In the **Management Zone Settings** section, click **Device Management,** then click **ZENworks Agent**.
3. In the **Agent Security** section, turn on the **Enable self defense for the ZENworks Agent** option.
4. Click **OK** (at the bottom of the page) to save the changes.

Configure the Local Setting

By default, the Endpoint Security Agent is configured to use the Agent Security setting configured in ZENworks Control Center. However, the Endpoint Security Agent also provides a local setting that you can use to enable or disable self defense. This local setting overrides the agent self defense setting configured in ZENworks Control Center.

1. Make sure you have enabled the device to accept an override password. For information, see Appendix A, “Override Password,” on page 19.
2. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
3. Click **Settings**.
4. In the Agent Self Defense section, select from the following settings:

   Enabled: Enables Client Self Defense.

   Disabled: Disables Client Self Defense.

   Policy: Uses the agent self defense setting configured in ZENworks Control Center.
5. Click **Set**.
6. Click **Close** to exit the dialog box.

Configuring Security Center Integration

Security Center Integration enables the Endpoint Security Agent to register the Endpoint Security firewall (defined through a Firewall policy assigned to the device) with the Windows Security Center and disable the Windows firewall.

Security Center Integration is enabled or disabled through the **Disable Windows Firewall and register Endpoint Security Management Firewall in Windows Security Center** setting in the Firewall policy. By default, the Endpoint Security Agent is configured to use the policy setting. However, the Endpoint Security Agent also provides a local setting that you can use to enable or disable Security Center Integration. This local setting enables you to override the policy setting or enable/disable Security Center Integration if no Firewall policy is assigned.

Configure the Local Setting

1. Make sure you have enabled the device to accept an override password. For information, see Appendix A, “Override Password,” on page 19.
2. Open the **Endpoint Security Agent About** dialog box. See Working with the Endpoint Security Agent.
3. Click **Settings**.
4. In the Security Center Integration section, select from the following settings:

   Enabled: Enables Security Center Integration. The Endpoint Security firewall is enabled and the Windows firewall is disabled.

   Disabled: Disables Security Center Integration. The Windows firewall is enabled and the Endpoint Security firewall is disabled.

   Policy: Uses the Security Center Integration setting from the enforced Security Settings policy.
5. Click **Set**.
6. Click **Close** to exit the dialog box.

Clear the Local Setting through ZENworks Control Center

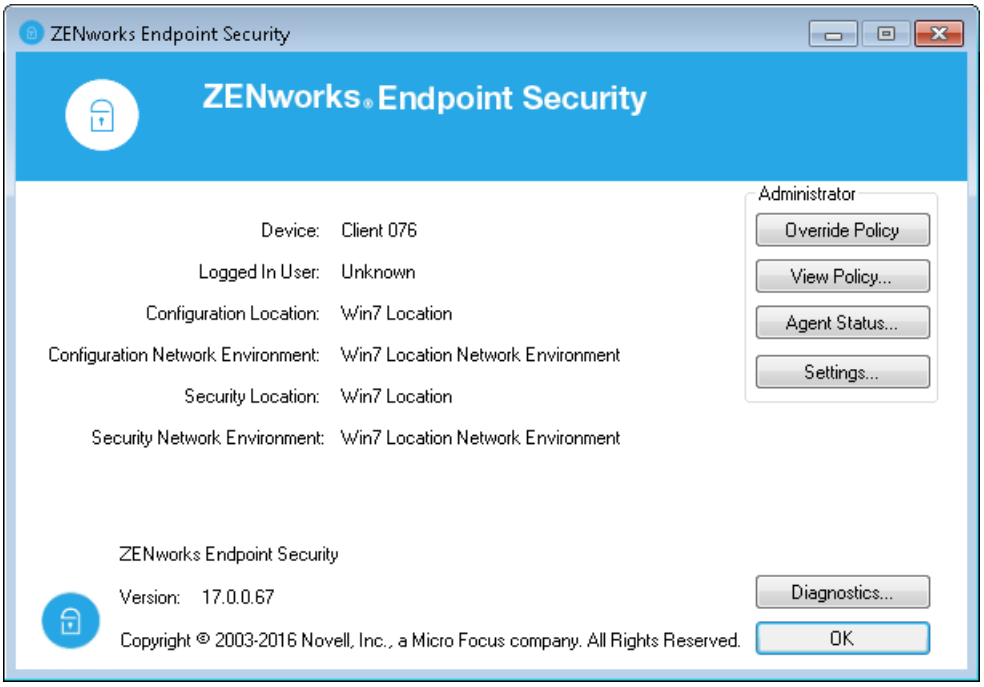
You can use ZENworks Control Center to clear the Security Center Integration local setting on a device. Clearing the setting resets it to the **Policy** option, causing the Endpoint Security Agent to enforce the policy setting rather than the local setting.

1. In ZENworks Control Center, click the **Devices** tab.
2. In the Devices list, locate the device whose local setting you want to clear.
3. Select the check box next to the device, then click **Quick Tasks** > **Clear ZESM Local Firewall Registration Settings**.
4. If you want to change any of the Quick Task options, do so. Otherwise, click **Start** to initiate the task and display the Quick Task Status dialog box.

   When the status for the device changes to **Done**, the local setting has been reset on the device.

A Override Password

The Endpoint Security Agent provides several features that are intended for use only by a ZENworks administrator or by a user under the direction of a ZENworks administrator. These features are grouped together in the Endpoint Security Agent's About dialog box.



In order for these Administrator features to be available, a ZENworks Agent override password must be configured in ZENworks Control Center. To configure the password:

1. In ZENworks Control Center, click **Configuration**.
2. In the **Management Zone Settings** section, click **Device Management,** then click **ZENworks Agent**.
3. In the **Agent Security** section, turn on the **Enable an override password for the ZENworks Agent** option, then click **Change** to set the password.
4. After setting the password, click **OK** (at the bottom of the page) to save the changes.

When you use an override password on a device, we recommend the following practice:

- If you are the one using the override password on a device, you can use the password as defined in the Agent Security settings.
- If you are allowing a user to access the Administrator options, you should generate a password key for the user. The key functions like the override password but allows you to specify who can use the key, what device it can be used on, and when the key expires. Using a key enables you to maintain the security of your override password and impose restrictions on the key. For information about generating a key for the override password, see "Password Key Generator" in the *ZENworks Endpoint Security Utilities Reference*.

B Interoperability Support

The ZENworks Endpoint Security Agent is officially listed as WHQL certified by Microsoft, ensuring current and ongoing compatibility with Microsoft Windows operating systems. Because the solution runs at the NDIS layer, we have taken extreme care to ensure that we are fully compatible with, and take advantage of, Windows infrastructure.

Windows Hardware Quality Labs (WHQL) is a Microsoft procedure for certifying that the hardware for peripherals and other components is compatible (works as expected) with Microsoft Windows operating systems. WHQL provides test kits to third-party developers so that they can test their product's compatibility. Products that are submitted to and meet the tests at Microsoft are allowed to display the Microsoft Windows logo on their marketing materials and are included in Microsoft's Hardware Compatibility List (HCL).