



ZENworks 2020 Endpoint Security Management Evaluator's Guide

August 2021

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

© Copyright 2021 Micro Focus or one of its affiliates.

Contents

Welcome to ZENworks 2020 Endpoint Security Management	5
1 Install and Configure ZENworks	7
Download the ZENworks Software	7
Create a ZENworks System	13
Deploy the ZENworks Virtual Appliance	13
Install the ZENworks Software	14
Activate ZENworks Endpoint Security Management	15
Connect to a User Source	17
Register a Windows 10 Device	19
Create an Authorization Key	19
Register a Device	21
Define a Security Override Password	24
Set Up Security Locations	26
Create a Work Location	27
Create a Pre-VPN Location	29
Create a Location Assignment Policy	31
Enable Antimalware	34
2 Protect Against Malware Threats	39
Create an Antimalware Enforcement Policy	39
Assign the Policy	40
Verify the Policy	41
Explore More	43
Antimalware Test Files	44
Antimalware Enforcement Policy	44
Malware Scans -- Initiated from the Antimalware Agent	45
Malware Scans -- Initiated from the ZENworks Agent Command Line Utility (zac)	45
Malware Scans -- Initiated from ZENworks Control Center	46
Custom and Network Scan Policies	46
Scan Exclusions	47
Full and Quick Scan Schedules	47
User Interaction	48
Device Malware Status and Threat Monitoring	48
3 Protect Data	51
Encrypt Removable Drives	51
Create a Microsoft Data Encryption Policy	51
Assign the Policy	52
Verify the Policy	53
Encrypt Folders on Fixed Disks	56
Modify the Microsoft Data Encryption Policy	56
Verify the Policy	58
Control Access to Removable Drives	60

Create a Storage Device Control Policy	60
Assign the Policy	61
Verify the Policy	61
4 Secure Wireless Communication	63
Control Wireless Network Access	63
Create a Wi-Fi Policy	64
Assign the Policy	65
Verify the Policy	65
Enforce a VPN Connection	67
Create a VPN Enforcement Policy	68
Create a Firewall Policy	71
Assign the Policies	73
Verify the Policy	74
Unassign the Policies	75
5 Block Applications	77
Create an Application Control Policy	77
Assign the Policy	78
Verify the Policy	79
6 Control Device Hardware	81
Control Communication Hardware	81
Create a Communication Hardware Policy	81
Assign the Policy	82
Verify the Policy	83
Control USB Device Connectivity	85
Create a USB Connectivity Policy	85
Assign the Policy	86
Verify the Policy	86

Welcome to ZENworks 2020 Endpoint Security Management

Desktops and laptops are vital to the success of today's digital organizations, providing users with access to essential resources like tools and data. Their mobility and constant connection to the Internet, however, present security challenges not only to the individual endpoints but to an organization's entire network.

ZENworks 2020 Endpoint Security Management helps protect your Windows desktops and laptops against common events that compromise your organization's resources. Through a variety of device-based and user-based security policies, you can protect against malware threats, prevent execution of unwanted applications, secure USB and other hardware devices, control wireless network access, encrypt sensitive data, and more. And because ZENworks is location aware, you can tailor your security policies by location, making it easy to provide the most effective security measures for devices both internal and external to your organization's network.

But don't take our word for it. Use this *Evaluator's Guide* to check out ZENworks 2020 Endpoint Security Management yourself.

How to Evaluate ZENworks

1. [Review What You'll Need for the Evaluation \(page 6\)](#): Learn about the resources you'll need for the evaluation.
2. [Install and Configure ZENworks \(page 7\)](#): Install the ZENworks software and perform the configuration tasks needed to use the product.
3. [Protect Against Malware Threats \(page 39\)](#): Use ZENworks Endpoint Security Antimalware to protect devices and centrally monitor threats detected on those devices.
4. [Protect Data \(page 51\)](#): Encrypt data on both removable drives and fixed disks as well as control access to removable drives.
5. [Secure Wireless Communication \(page 63\)](#): Limit access to wireless networks based on access point identification or security. Enforce VPN connections on public wireless networks.
6. [Block Applications \(page 77\)](#): Protect against use of unauthorized or undesirable applications.
7. [Control Device Hardware \(page 81\)](#): Control access to communication hardware such as Bluetooth, parallel/serial ports, and network adapters. Restrict USB connectivity to approved types of devices.

Review What You'll Need for the Evaluation

Here's a heads up on some of the resources you'll need in order to run through this evaluation. More information about these requirements is provided in the sections that follow.

- ❑ **A Windows/Linux server or VM hypervisor.** The ZENworks software must be installed on a Windows or Linux server (physical or virtual). Or, the ZENworks Virtual Appliance (pre-configured with the ZENworks software) must be run on a supported hypervisor. For more information about supported servers and hypervisors, see [“Download the ZENworks Software” on page 7](#).

If you plan to evaluate the product's Antimalware capability:

- ◆ You must use the ZENworks Virtual Appliance or install the ZENworks software on a Linux server.
- ◆ The server/network hosting the ZENworks Primary Server must be configured to allow the Primary Server to access the following URL. This is the location from which malware signature updates (and Antimalware Agent updates) are retrieved:

```
https://microfocus-2dcb60a8-26c9-4560-9cc2-34a16ea5f6e6.2d7dd.cdn.bitdefender.net/
```

- ❑ **An LDAP directory.** To assign policies to users (rather than to devices only), you must connect ZENworks to an LDAP user directory. ZENworks synchronizes user data from the LDAP directory contexts you specify. After users log into ZENworks (using their LDAP credentials), the user-assigned policies are enforced on their devices.

This evaluation can be done with device policy assignments only. If you want to use user policy assignments, you'll need Microsoft Active Directory or NetIQ eDirectory.

- ❑ **A Windows 10 device.** This needs to be a physical desktop or laptop running windows 10. Do not use a virtual machine. To fully evaluate all of the ZENworks Endpoint Security capabilities, the device should have the following:
 - ◆ Wireless network hardware to test the wireless and VPN capabilities.
 - ◆ A VPN client to test the VPN capabilities.
 - ◆ One or more USB thumb drives that you can use for removable drive encryption and USB device control.

1 Install and Configure ZENworks

As a Unified Endpoint Management and Protection solution, all ZENworks Suite products (Asset Management, Configuration Management, Endpoint Security, Full Disk Encryption, and Patch Management) use the same ZENworks infrastructure. This means that when you complete the ZENworks installation, not only can you evaluate ZENworks Endpoint Security Management but you can also evaluate any of the other products. The products can then be purchased individually or as a Suite.

To set up a ZENworks system:

- ◆ “Download the ZENworks Software” on page 7
- ◆ “Create a ZENworks System” on page 13
- ◆ “Activate ZENworks Endpoint Security Management” on page 15
- ◆ “Connect to a User Source” on page 17
- ◆ “Register a Windows 10 Device” on page 19
- ◆ “Define a Security Override Password” on page 24
- ◆ “Set Up Security Locations” on page 26
- ◆ “Enable Antimalware” on page 34

Download the ZENworks Software

To download the ZENworks software, you need a Micro Focus account. If you don't already have an account, no worries, we'll help you easily create one through our free trial website. Not only does your Micro Focus account let you access the ZENworks software, it also gives you access to trials for other Micro Focus products and membership in the Micro Focus product communities.

- 1 Go to the [ZENworks 2020 Suite Trial Registration page \(https://www.microfocus.com/products/zenworks/free-trial\)](https://www.microfocus.com/products/zenworks/free-trial).

MICRO FOCUS
ZENworks Suite

Start Your Free 60-Day ZENworks Suite Now

NO CREDIT CARD REQUIRED

- Efficiency**
Easy, same-day installation.
- Complete Access**
Get all the benefits and functionality of the full-featured ZENworks Suite software.
- Collaboration**
Share and evaluate ZENworks Suite with your whole team.

Already have an account? [Sign In](#)

Complete the Form to Access Your Trial

* Required field

First name* Last name*

Email*

Username*

Password* [Show](#)

Country*
Select your Country

Phone* +1 Extension (optional)

Company name*

Job Title (optional)

Zip/Postal code*

[Start Free Trial](#)

By submitting this form, I agree to the [Micro Focus Website Terms of Use](#), [Privacy and Cookie Notice](#), and [EULA or Customer Terms for SaaS](#)

2 If you already have a Micro Focus account, click the **Sign In** link in the top right corner of the form and sign in to your account. Then continue with Step 3 below.

or

If you don't have a Micro Focus account:

2a Fill in the form to provide information for your account, then click **Start Free Trial**.

Your account is created and the following page is displayed.

MICRO FOCUS Solutions Products Support & Services Partners Events About Support Login Contact Us [My Micro Focus](#) [Free Trials](#)

Thank you for your interest in ZENworks Suite

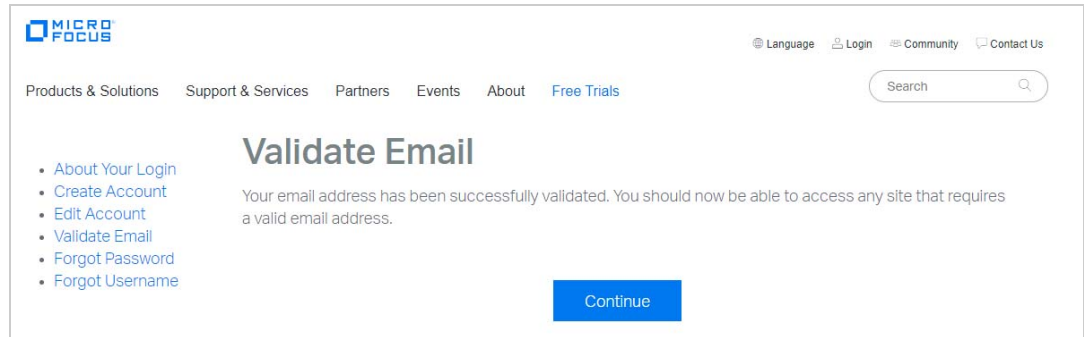
What happens next?

- 1 Validate your email**
Check your inbox for an email validation request. Didn't receive the email? Please check your spam folder.
- 2 Request a trial**
Complete the signup process on the trial page. Then you'll receive an email with the link to your free trial.
- 3 Access your product**
Click the link in the email and follow the instructions on the web page to access your trial.
- 4 Stay in touch**
Throughout your trial period, we'll reach out to you to see if you have any questions. But feel free to [contact us](#) at any point.

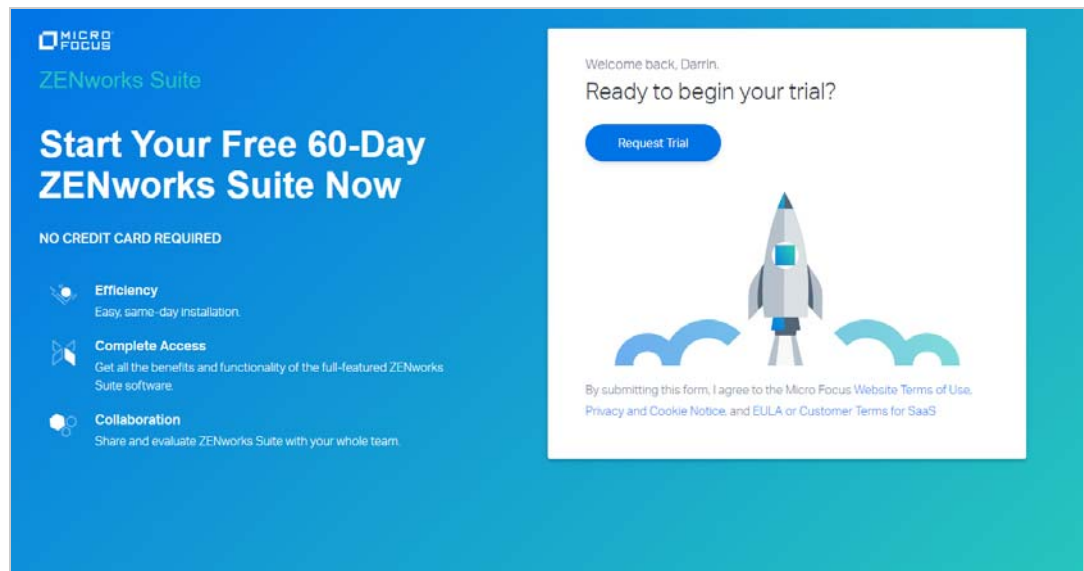
2b In your email account, open the Micro Focus Account email and click the **Validate Email** link.

2c Sign in with your Micro Focus account username and password.

After successful login, your email is validated and your Micro Focus account is activated.



2d Click **Continue** to return to the ZENworks Suite trial page.

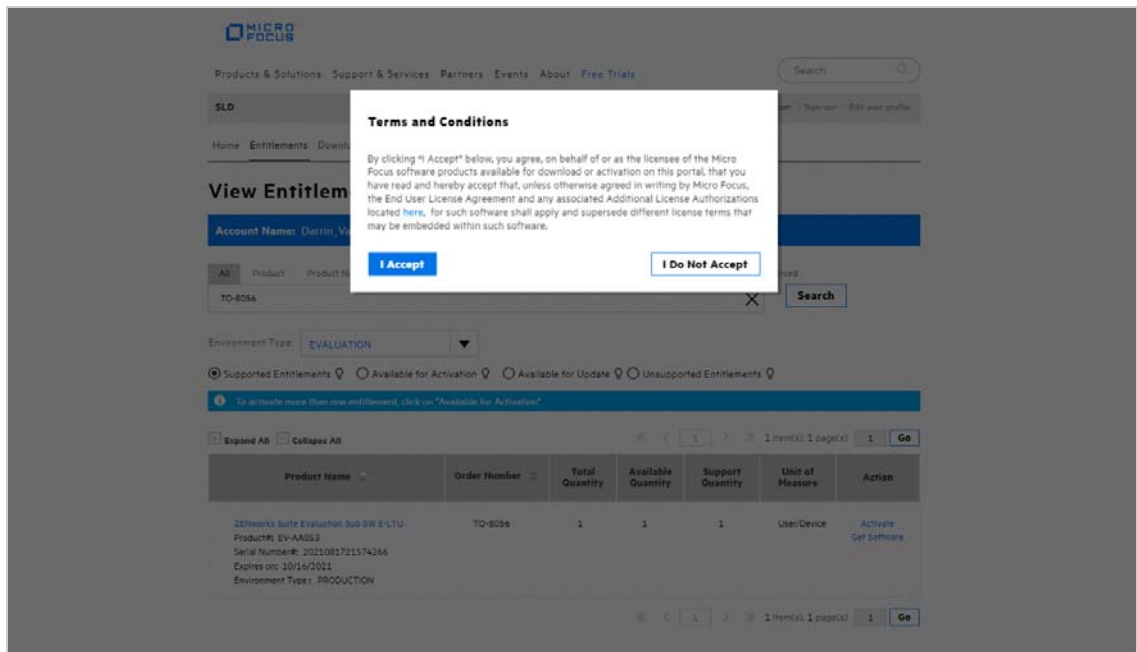


3 Click the **Request Trial** link.

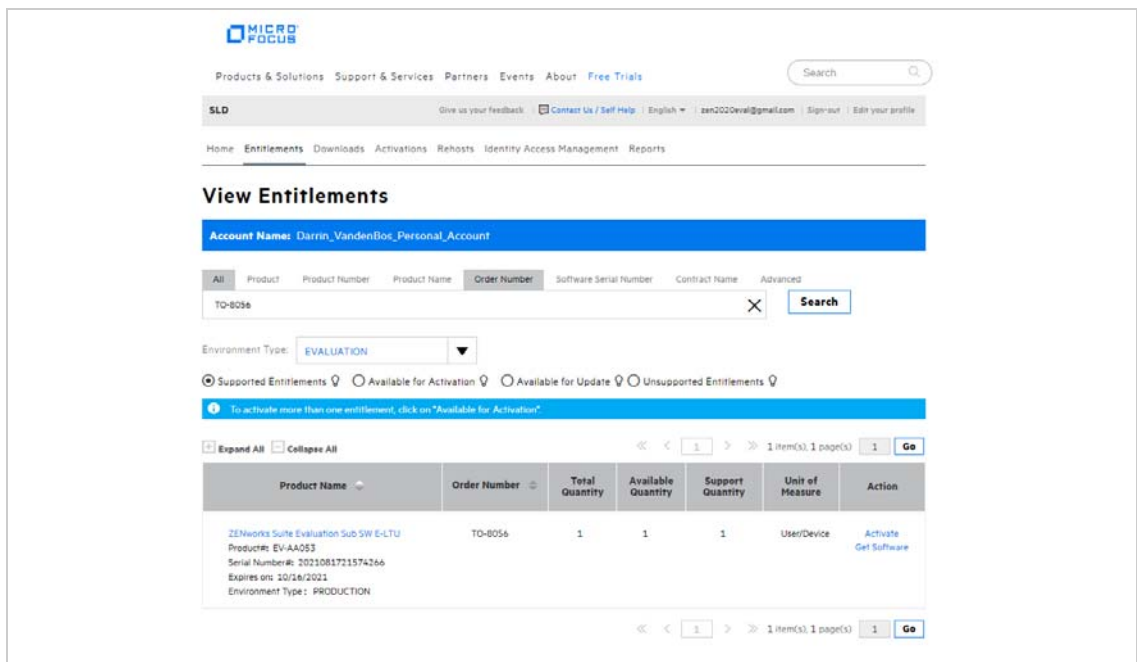
4 In your email account, open the MFI Trials and Eval email and click the **Sign in** link.

5 If prompted, sign in with your Micro Focus account username and password.

Your Micro Focus Software and License Distribution (SLD) portal is displayed.



- 6 Click **I Accept** to agree to the terms and conditions for Micro Focus software products.
- 7 Click **OK** to dismiss the *How to access your License Entitlements and Software Downloads* dialog.



- 8 Activate the product:
 - 8a In the product list, click the **Activate** link for the *ZENworks Suite Evaluation Sub SW-E-LTU* entry to display the License Activation page.

License Activation

Environment Type: PRODUCTION
Please enter the licensing locking information. Select the product and associated version and quantity to activate. Fields marked with an asterisk (*) are required.

Target Name * Auto-generate Name

Activation Notes

Email Confirmation Address

Product Name	Version *	Available Quantity	Quantity to Activate *
<input type="checkbox"/> ZENworks Suite Evaluation Sub SW E-LTU Product: EV-AA053	<input type="text" value="Select a version"/>	1	<input type="text"/>

[Previous](#) [Next](#)

8b In the Target Name field, enter ZENworks Server .

8c In the list, select ZENworks Suite Evaluation Sub SW E-LTU, select 2020.02 for the version, enter 1 as the quantity to activate, then click Next.

8d Click Submit to confirm the activation details and display the Activate Results page.

Activation Result

Target: ZENworks Server
Activated Date (mm/dd/yyyy): 08/17/2021 [Email All Details](#)

Product Name	Version	Activated Quantity	Status	Activation Notes
ZENworks Suite Evaluation Sub SW E-LTU	2020.02	1	Active	Get Software

Additional Instructions:
This evaluation product does not require a generated license key. The product software has a built-in evaluation period.

[View Certificate](#)

Email has been sent to: zen2020eval@gmail.com [Return to View Entitlements](#)

9 Click Get Software to display the Software Downloads page.

Micro Focus

Products & Solutions | Support & Services | Partners | Events | About | Free Trials

SLD | Give us your feedback | Contact Us / Self Help | English | zen2020eval@gmail.com | Sign-out | Edit your profile

Home | Entitlements | Downloads | Activations | Rehosts | Identity Access Management | Reports

Software Downloads

Account Name: Darrin_VandenBos_Personal_Account

Product: ZENworks Suite

Product Name: ZENworks Suite Evaluation Sub SW E-LTU

Version: 2020.02

Reset

Download Selected | Get Licenses

By downloading the software below, you agree, on behalf of or as the licensee of such software, that you have read and hereby accept that, unless otherwise agreed in writing by Micro Focus, the End User License Agreement and any associated Additional License Authorizations located [link], for such software shall apply and supersede different license terms that may be embedded within such software.

Description	Category	Platform	Language	File Type	Media Version	Created Date	Action
<input type="checkbox"/> ZENworks2020_Update2.iso	ZSUITE2020U2	***	***	Software	2020.02	2021-08-09	More Details Download
<input type="checkbox"/> ZENworks2020_Update2_Appliance-x86_64.ova	ZSUITE2020U2	***	***	Software	2020.02	2021-08-09	More Details Download
<input type="checkbox"/> ZENworks2020_Update2_Appliance-x86_64.zip.001	ZSUITE2020U2	***	***	Software	2020.02	2021-08-09	More Details Download
<input type="checkbox"/> ZENworks2020_Update2_Appliance-x86_64.zip.002	ZSUITE2020U2	***	***	Software	2020.02	2021-08-09	More Details Download
<input type="checkbox"/> ZENworks2020_Update2_Appliance-x86_64.zip.003	ZSUITE2020U2	***	***	Software	2020.02	2021-08-09	More Details Download

You'll quickly notice that there are a bunch of different download files. The files you need depend on whether you want to use the ZENworks Virtual Appliance or perform a traditional install.

Virtual Appliance: ZENworks is available as a virtual appliance that can be deployed to a supported virtual infrastructure. The appliance is built on a customized SUSE Linux Enterprise Server (64-bit) and comes pre-installed with ZENworks.

We strongly recommend that you use the appliance for the evaluation. Why? Because the appliance is convenient, easy to use, and doesn't require you to supply an operating system license. In addition, if you plan to evaluate the product's Antimalware capability, the ZENworks software must be installed on a Linux server (for reasons that will be explained in "Enable Antimalware" on page 34) and the appliance is Linux.

The appliance is supported on the following hypervisors.

Hypervisor	File to Download
VMware ESXi 6.x VMware Workstation 6.5 and newer (use in non-production environments only)	ZENworks2020_Update2_Appliance-x86_64.ova
Microsoft Hyper-V Server Windows 2012 2012 R2 2016 2019	ZENworks2020_Update2_Appliance-x86_64.vhd.zip ZENworks2020_Update2_Appliance-x86_64.vhdx.zip
XEN on SLES 12.x 15.x	ZENworks2020_Update2_Appliance-x86_64.xen.tar.gz
Citrix XenServer 7.x and Citrix Hypervisor 8.x	ZENworks2020_Update2_Appliance-x86_64.xva.tar.gz

Traditional Install: You can install the software on a server listed below.

Operating System	File to Download
Windows 2012 Server x86_64 Windows 2012 Server R2 x86_64 Windows 2016 Server x86_64 Windows 2019 Server x86_64	ZENworks_2020_Update2.iso
SLES 12 SP4 SP5 x86_64 SLES 15 SP1 SP2 x86_64	ZENworks_2020_Update2.iso

- 10 Click the **Download** link for the files you want to download.

Create a ZENworks System

After you've downloaded the ZENworks software, you are ready to install the ZENworks Primary Server and establish a management zone. The Primary Server manages the devices that register in the zone. For example, security configurations (referred to as security policies) are distributed by the Primary Server to the managed devices.

Refer to the appropriate section for installation instructions:

- ♦ [Deploy the ZENworks Virtual Appliance \(page 13\)](#)
- ♦ [Install the ZENworks Software \(page 14\)](#)

Deploy the ZENworks Virtual Appliance

- 1 Make sure the host machine has at least 16 GB RAM and 130 GB free disk space, and has a static IP address or a permanently leased dynamic (DHCP) IP address.
- 2 Import the ZENworks Virtual Appliance into your hypervisor to create a new virtual machine.

- 3 After the virtual machine has been created, add a second hard disk of size 40 GB. The first disk (90 MB) is used for the Appliance while the second disk (40 GB) will be used to store the ZENworks data.
- 4 Power on the new virtual machine.
- 5 Follow the prompts to configure the virtual machine and then the ZENworks Server and zone.

For this evaluation, we recommend the following:

- ♦ Create a new ZENworks Management Zone.
- ♦ Use the embedded PostgreSQL database. Even if you use Oracle or MSSQL database in your environment, using the embedded PostgreSQL database is more convenient and quicker.
- ♦ Use the internal Certificate Authority. Even if you use an external CA in your environment, using the internal CA is more convenient and quicker.

If you need more details, refer to the *ZENworks Appliance Deployment and Administration Reference* (https://www.novell.com/documentation/zenworks-2020-update-2/zen_ca_appliance).

Install the ZENworks Software

When using the ZENworks software on a physical server, remember that ZENworks Endpoint Security Antimalware requires that the ZENworks Primary Server be installed on a Linux server. The alternative is to use the ZENworks Virtual Appliance.

- 1 Make sure the target server has at least 16 GB RAM and 80 GB free disk space, and has a static IP address or a permanently leased dynamic (DHCP) IP address.
- 2 Log in to the server as a user with administrative rights.
- 3 Mount the ZENworks ISO and run the installation program:
 - ♦ **Windows:** Run `setup.exe`.
 - ♦ **Linux:** Run `setup.sh`.
- 4 Complete the installation wizard.

For this evaluation, we recommend the following:

- ♦ Create a new ZENworks Management Zone.
- ♦ Use the embedded PostgreSQL database. Even if you use Oracle or MSSQL database in your environment, using the embedded PostgreSQL database is more convenient and quicker.
- ♦ Use the internal Certificate Authority. Even if you use an external CA in your environment, using the internal CA is more convenient and quicker.

If you need more details, refer to the *ZENworks 2020 Server Installation Guide* (https://www.novell.com/documentation/zenworks-2020-update-2/zen_installation).

Activate ZENworks Endpoint Security Management

When you installed ZENworks, you created the ZENworks infrastructure (Primary Server and management zone) that supports the five main ZENworks Suite products: Asset Management, Configuration Management, Endpoint Security Management, Full Disk Encryption, and Patch Management.

To evaluate ZENworks Endpoint Security Management, you need to activate it. During the 60-day evaluation period you have access to the full product.

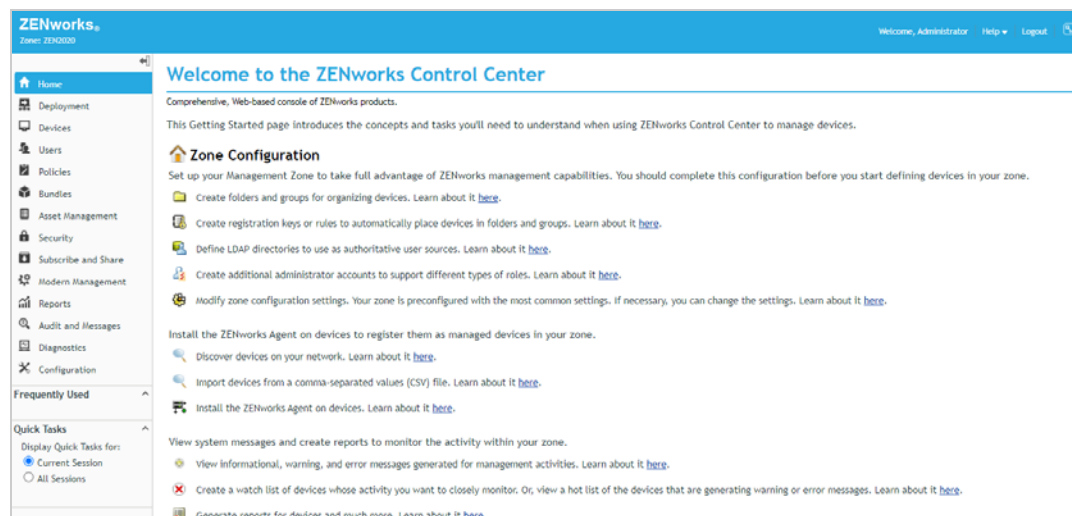
1 Log in to ZENworks Control Center:

1a In a web browser, enter the following URL:

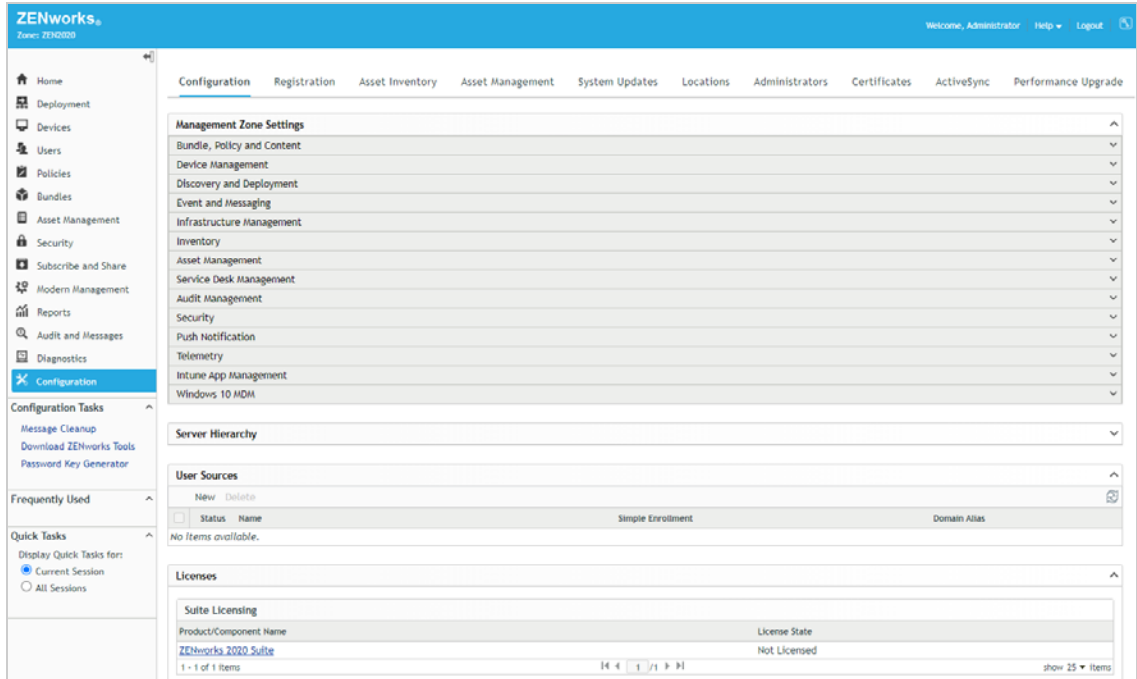
`https://ZENworks_Server_Address`

Replace `ZENworks_Server_Address` with the IP address or DNS name of the ZENworks Primary Server.

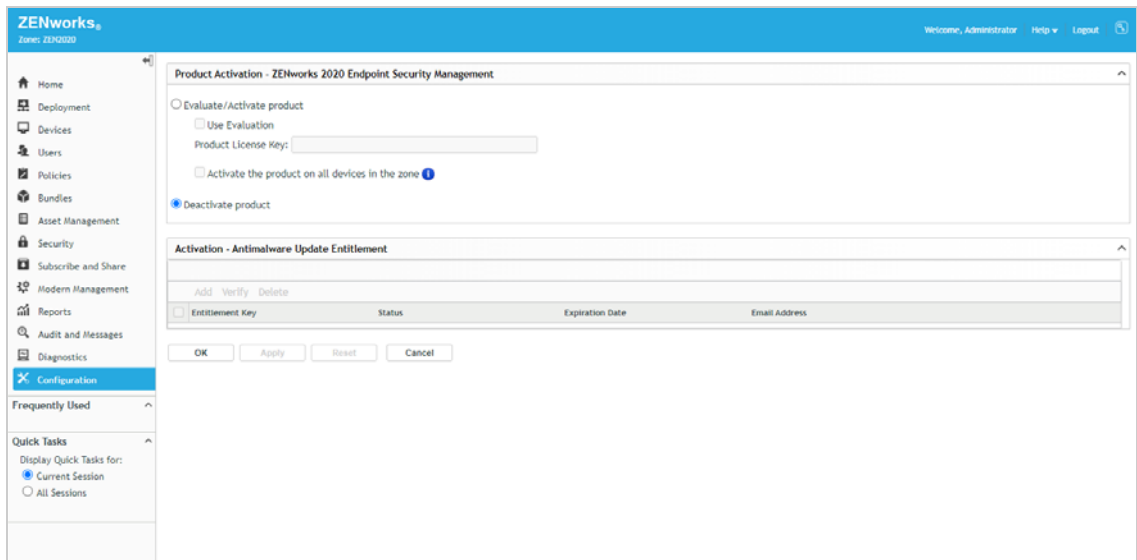
1b Specify *Administrator* as the username, specify the password you defined during installation, then click **Login** to display the Welcome page.



2 Click **Configuration** (in the left navigation pane).

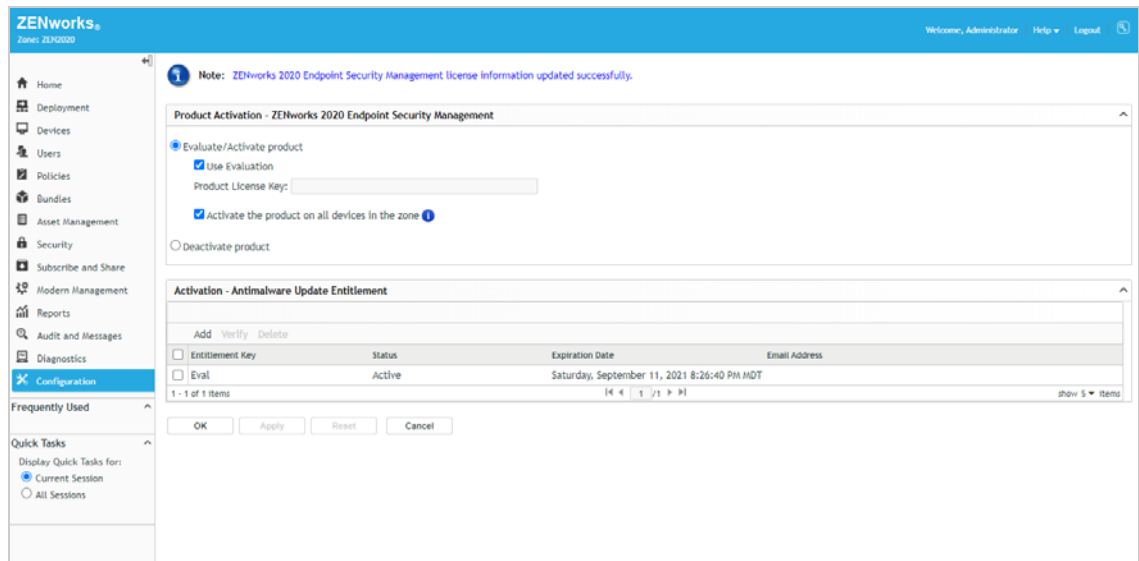


3 In the Licenses section, click **ZENworks 2020 Endpoint Security Management** to display the Product Activation - ZENworks 2020 Endpoint Security Management page.



4 Select **Evaluate/Activate product**, select the **Use Evaluation** option, select **Activate the product on all devices in the zone** option, then click **Apply**.

The product is activated for a 60-day evaluation period. As part of the evaluation period, the Antimalware Update Entitlement is also activated. The entitlement enables your ZENworks system to download malware signature updates and scan engine updates after you have enabled Antimalware in the zone. You'll do this in ["Enable Antimalware"](#) on page 34.



5 Click **OK** to close the Product Activation page.

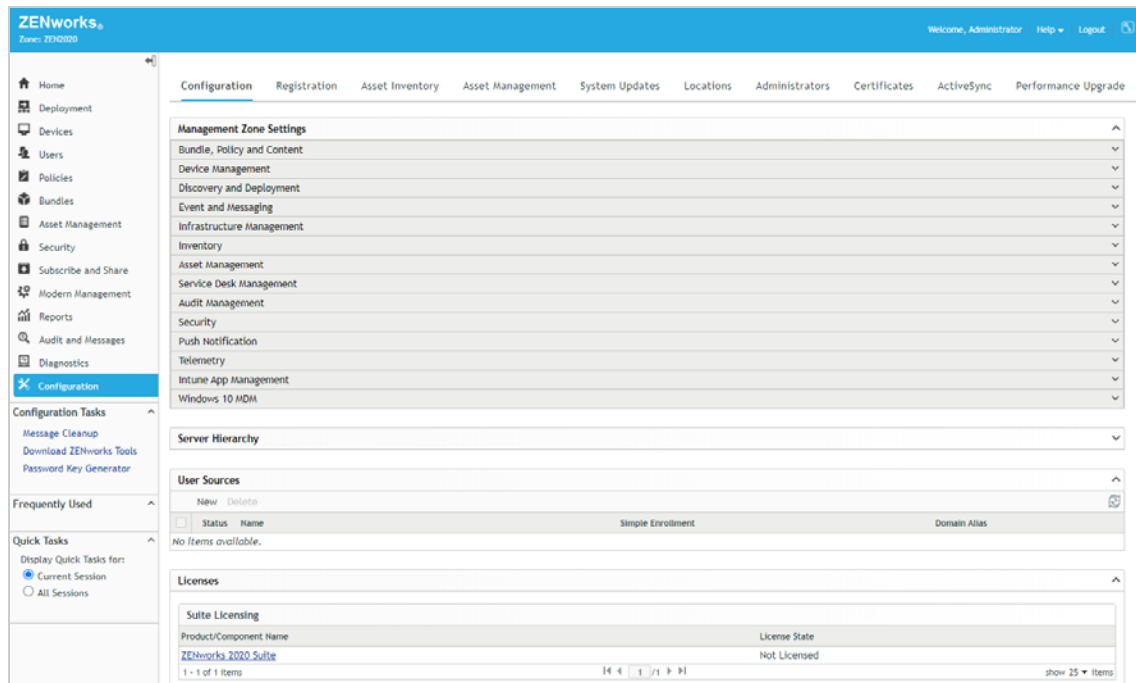
Connect to a User Source

You configure the security settings on endpoint devices through the use of security policies. Security policies can be assigned to devices or to users. Device-assigned policies are enforced on the device regardless of which user logs in. User-assigned policies are enforced on any device where the user logs in.

When a Windows device registers in the ZENworks management zone, the device is added to the ZENworks database and becomes eligible to be assigned policies. However, to be able to assign policies to users, you must connect ZENworks to your LDAP user directory (Microsoft Active Directory or NetIQ eDirectory). ZENworks then synchronizes user data from the LDAP directory contexts you specify to the ZENworks database. This allows policies to be assigned to users; then, when a user logs into ZENworks (using their LDAP credentials), the policies are enforced on the device.

All security policies can be assigned to devices, which means that connecting to a user source is not required. However, if you want to see how user assignments work, complete the following steps to connect to a user source:

- 1 In ZENworks Control Center, click **Configuration** (in the left navigation pane).



- 2 In the User Sources panel, click **New** to launch the Create New User Source wizard.



- 3 On the Connection Information page, define the following connection information, then click **Next**:

- ◆ **Connection Name:** Specify a descriptive name for the connection to the LDAP directory.
- ◆ **Address:** Specify the IP address or DNS hostname of the LDAP directory server.
- ◆ **Use SSL:** Disable the option if the LDAP server does not support SSL.
- ◆ **Port:** If the LDAP server is not listening on a default port (636 or 389), specify the correct port number.

- ♦ **Root LDAP Context:** The root context establishes the ZENworks entry point into the directory. If you don't specify a root context, the directory's root container is used.
 - ♦ **Ignore Dynamic Groups in eDirectory:** Leave this option unchecked.
- 4 (Conditional) On the Certificate page (which is displayed only if the connection is using SSL), verify the certificate information, then click **Next**.
 - 5 On the Credentials page, specify a Read-only username and password that ZENworks can use to access the directory, then click **Next**.
 - 6 On the Authentication Mechanisms page, select **Username/Password**, then click **Next**.
 - 7 On the User Containers page, add the container where the user accounts reside that you will use during the evaluation, then click **Next**.
 - 8 Complete the wizard.

Register a Windows 10 Device

A device must register with the ZENworks management zone in order for it to be managed. To register a Windows device, you install the ZENworks Agent on the device. The agent then contacts the ZENworks Primary Server and completes the registration process.

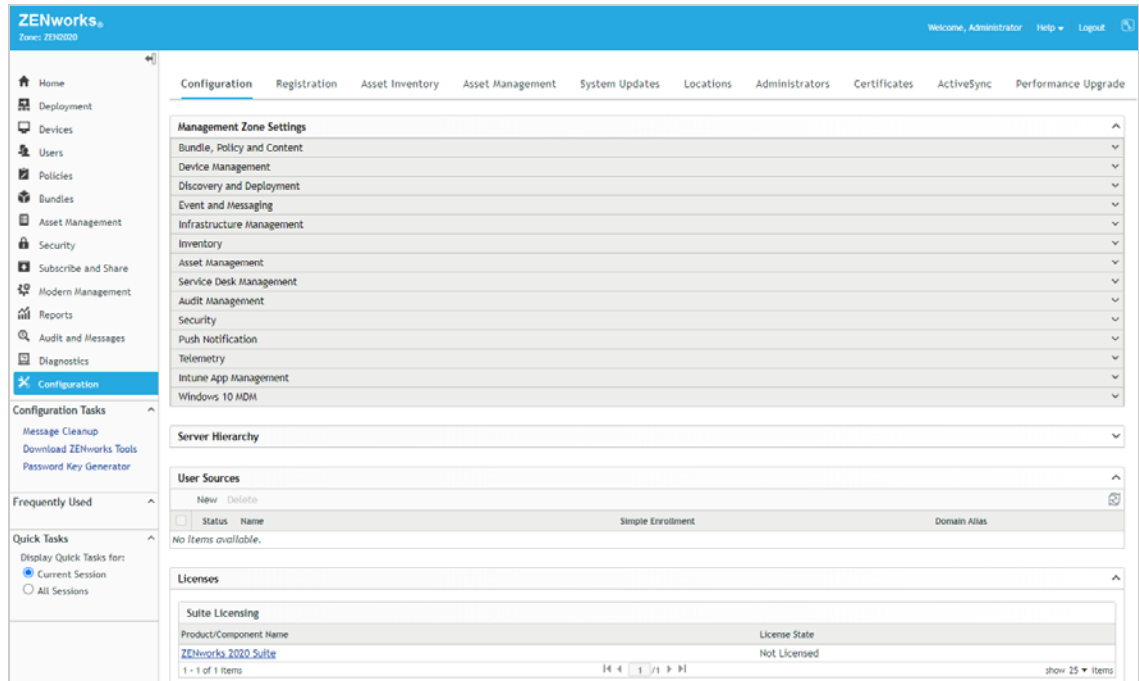
- ♦ [“Create an Authorization Key” on page 19](#)
- ♦ [“Register a Device” on page 21](#)

Create an Authorization Key

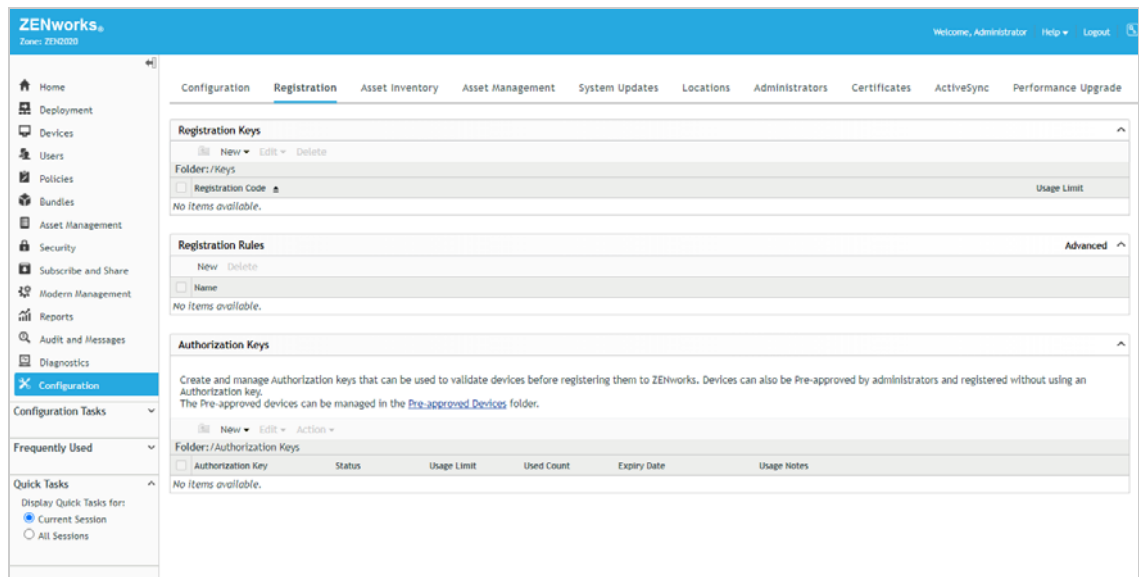
When you install the ZENworks Agent on a device, it has the information required to connect back to your ZENworks Primary Server and register in your zone. To secure your ZENworks system against access by rogue devices, ZENworks allows only authorized devices to register. One way to authorize a

device is to issue an authorization key that must be entered during installation of the ZENworks Agent on the device. This is the method we'll have you use, which means you first need to create an authorization key.

- 1 In ZENworks Control Center, click **Configuration** (in the left navigation pane).



- 2 Click the **Registration** tab (top of page).



- 3 In the Authorization Keys panel, click **Configure > Authorization Key** to display the New Authorization Key dialog box.

4 Configure the settings as follows, then click **Add** to create the key.

- ◆ **Authorization Key:** Enter an 8 - 10 character key of your choice, or click **Generate** to automatically generate one. You'll need to remember the key so write it down if necessary.
- ◆ **Usage Limit:** Select the limit for the number of times this key can be used, or select **Unlimited** to remove the usage limit for this evaluation. Security best practices dictate that you not allow unlimited uses in a production environment.
- ◆ **Expiry:** Select an expiration date for the key, or select **Does Not Expire** for this evaluation. As with the usage limit, security best practice in a production environment would be to use an expiration date.

5 Click **Add** to create the key and add it to the list.

Register a Device

There are several ways you can distribute the ZENworks Agent to the device, including using discovery and deployment tasks in ZENworks Control Center to push the agent to devices, but we'll just have you manually download the agent from your ZENworks Primary Server and start the installation.

1 On the Windows 10 device that you want to register, enter the following URL:

`https://ZENworks_Server_Address/zenworks-setup`

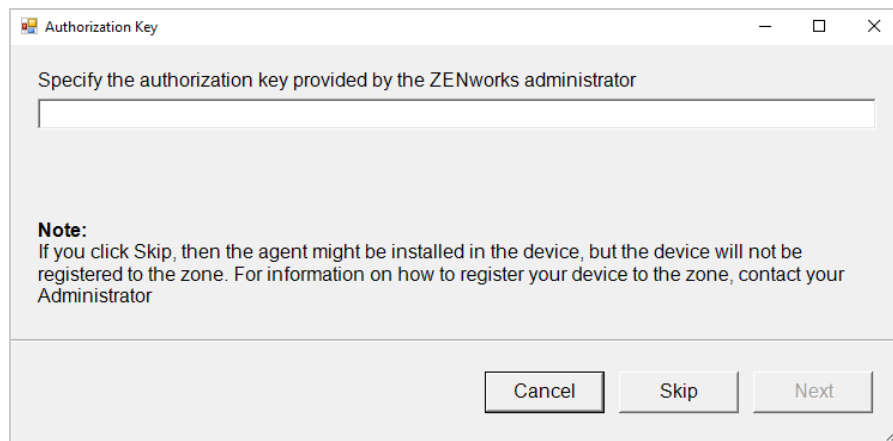
The ZENworks Agent download list is displayed.


Package Name	Target Platform	Target Architecture	Install Type	Size
Default Agent (x86_Network)	Linux	x86 Architecture (32 bit)	Network	48.8 MB
Default Agent (x86_Complete)	Linux	x86 Architecture (32 bit)	Standalone	178.4 MB
Default Agent (x86_64_Network)	Linux	x86_64 Architecture (64 bit)	Network	46.7 MB
Default Agent (x86_64_Complete)	Linux	x86_64 Architecture (64 bit)	Standalone	197.4 MB
Default Agent (x86_64_Complete)	Macintosh	x86_64 Architecture (64 bit)	Standalone	253.2 MB
Default Agent (x86_Network)	Microsoft Windows	x86 Architecture (32 bit)	Network (.NET 4.5 required)	2.3 MB
Default Agent (x86_Complete)	Microsoft Windows	x86 Architecture (32 bit)	Standalone	637.7 MB
Default Agent (x86_Complete)	Microsoft Windows	x86 Architecture (32 bit)	Standalone (.NET 4.5 required)	570.9 MB
Default Agent (x86_64_Network)	Microsoft Windows	x86_64 Architecture (64 bit)	Network (.NET 4.5 required)	2.3 MB
Default Agent (x86_64_Complete)	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone	663.1 MB
Default Agent (x86_64_Complete)	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone (.NET 4.5 required)	596.3 MB

- 2 In the list, click the installation package you want to download to the device, then follow the prompts to download it.

You want the Microsoft Windows package that is the **Standalone** install type. If you know that the target device has .NET 4.5 or newer installed, you can use the **Standalone (.NET 4.5 required)** install type instead.

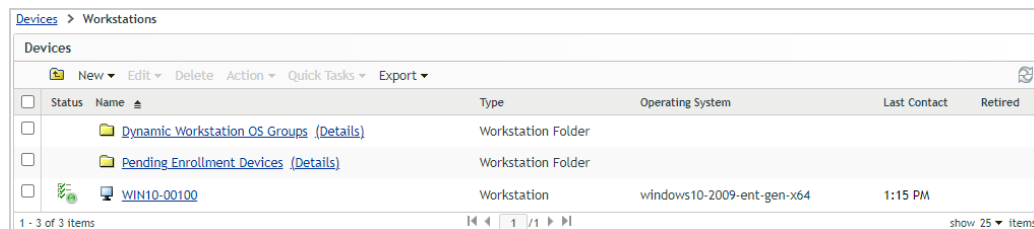
- ♦ **32 bit:** *Default Agent (x86_Complete)* Microsoft Windows x86 Architecture (32 bit) Standalone package
 - ♦ **64 bit:** *Default Agent (x86_64_Complete)* Microsoft Windows x86_64 Architecture (64 bit) Standalone package
- 3 After the ZENworks Agent download completes, double-click the agent to start the installation.
 - 4 When prompted, enter the authorization key you created, then click **Next** to continue the installation.




The installation can take a few minutes. You can track the progress through the ZENworks icon  located in the notification area.

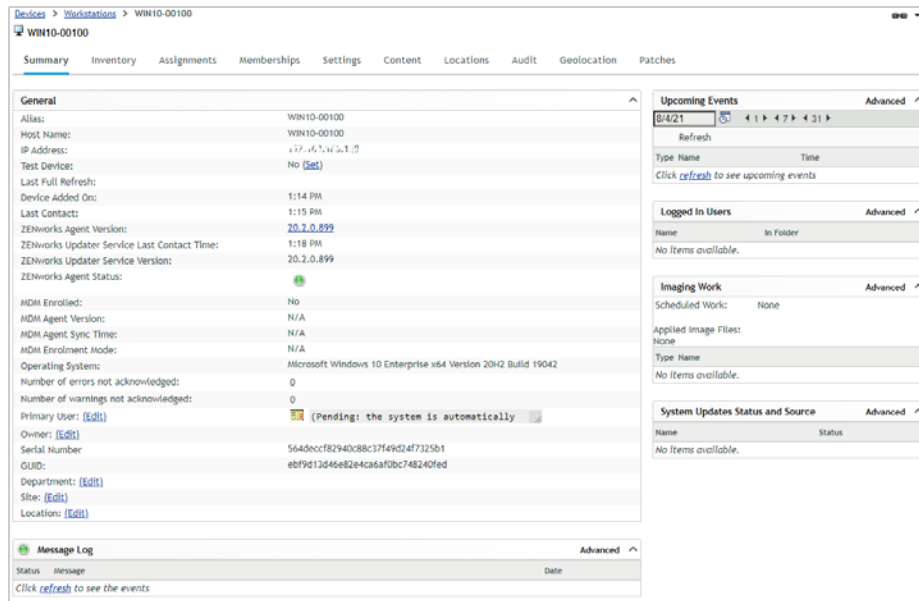
- 5 When installation is complete, reboot the device as prompted.
- 6 In ZENworks Control Center, go to the **Devices > Workstations** list to confirm that the device is enrolled in the zone.

The Windows device is listed after the predefined device folders. In this example, we enrolled a Windows device named *WIN10-00100*.



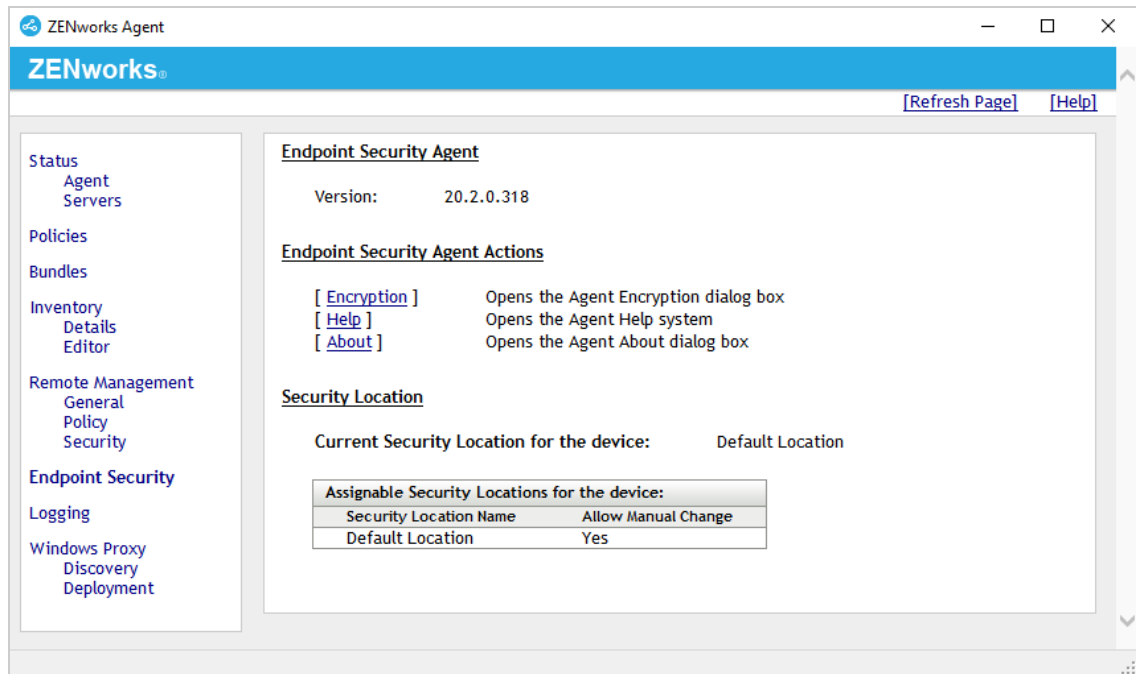
Status	Name	Type	Operating System	Last Contact	Retired
<input type="checkbox"/>	Dynamic Workstation OS Groups (Details)	Workstation Folder			
<input type="checkbox"/>	Pending Enrollment Devices (Details)	Workstation Folder			
<input type="checkbox"/>	 WIN10-00100	Workstation	windows10-2009-ent-gen-x64	1:15 PM	

- 7 (Optional) In the list, click the Windows device to display its Summary page. The Summary page provides details about the device.



- 8 On the device, right-click the ZENworks icon in the Notification area, then click Technician Application to display the ZENworks Agent window.

The ZENworks Agent window provides details about the agent and the ZENworks server to which it is connected. It also provides information such as assigned policies and bundles. Typically, users don't need to access the ZENworks Agent windows, but we wanted to introduce it because we'll refer to it several times throughout this evaluation to verify policy assignments.



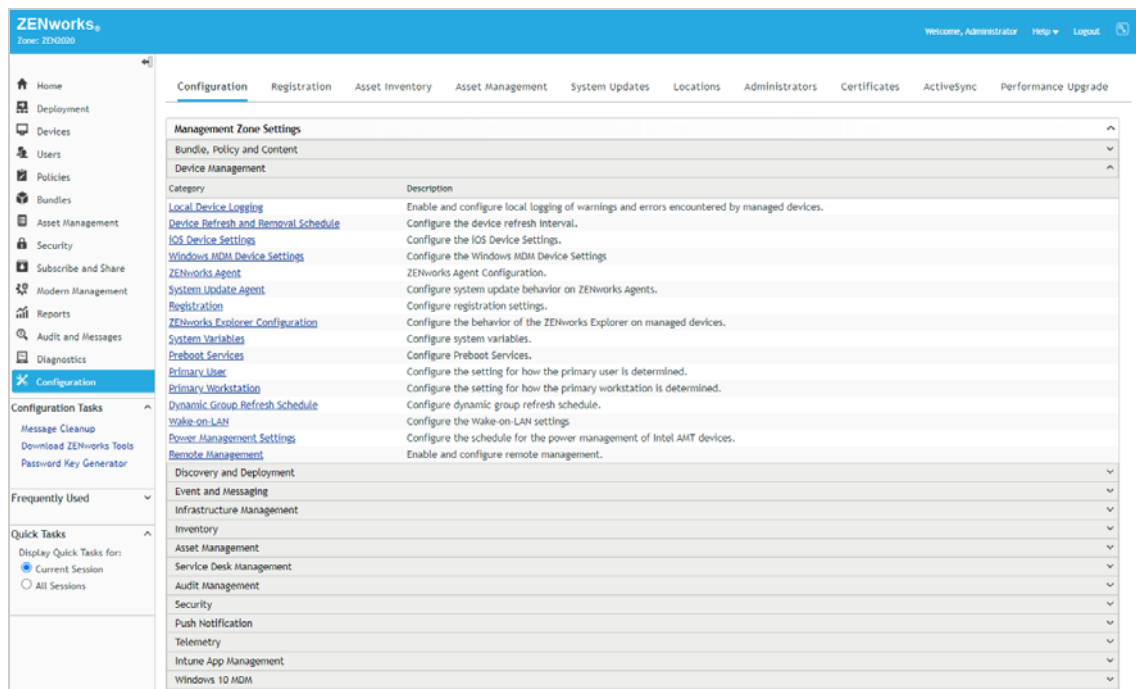
You now have a device that you can use for the rest of this evaluation. One device is sufficient, but you can register additional Windows 10 devices if you'd like to apply security policies to multiple devices. And, if you plan to evaluate the Antimalware capability, additional devices will provide more data for the Security dashlets.

Define a Security Override Password

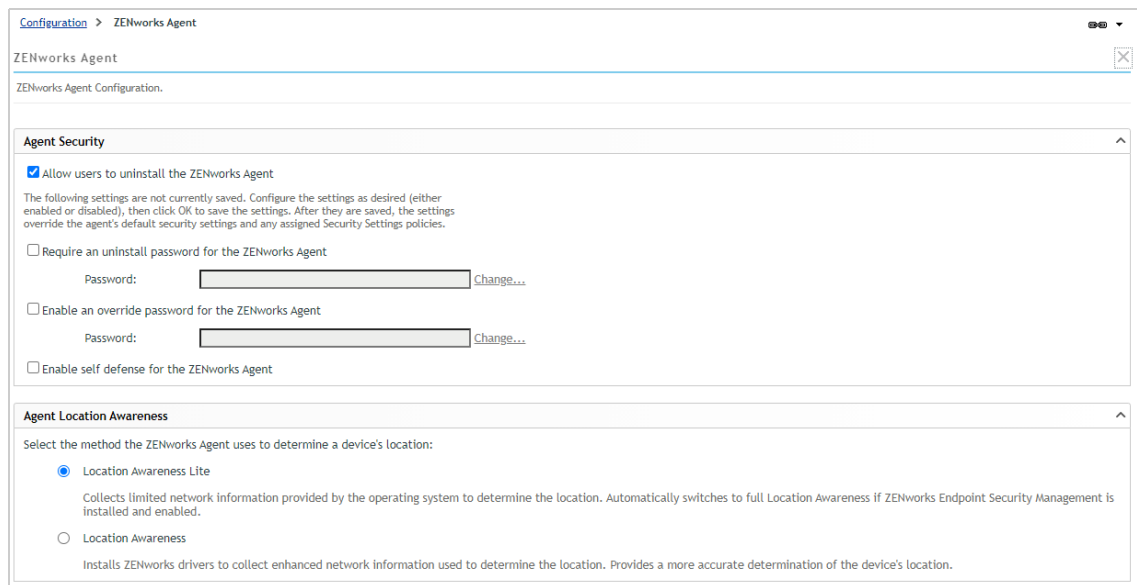
The ZENworks Agent consists of multiple modules with the Endpoint Security Agent being the one that handles security related tasks and enforcement. You can define an override password that disables the Endpoint Security Agent's enforcement of security policies (excluding encryption and Antimalware policies) on a device. The override password can also be used to unlock other administrator-level information on the device that can be helpful when troubleshooting security policies.


We strongly recommend and encourage (and even implore) you to set an override password!

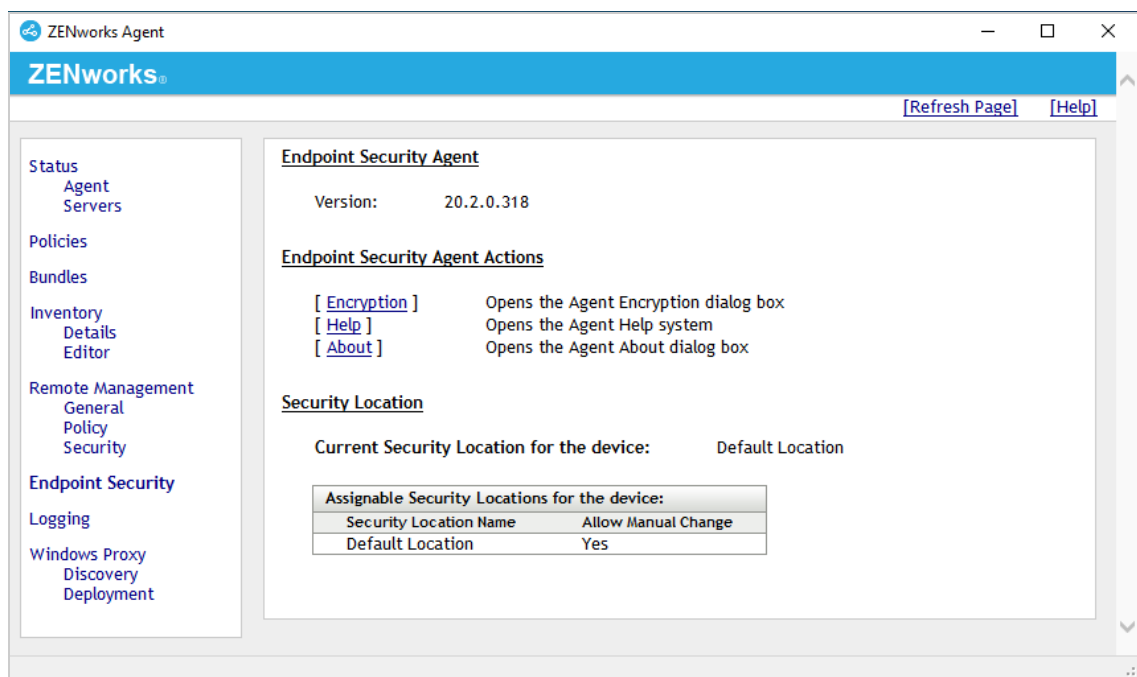
- 1 In ZENworks Control Center, click **Configuration** (in the left navigation pane).



- 2 In Management Zone Settings, click **Device Management** to expand the section, then click **ZENworks Agent** to display the ZENworks Agent configuration settings.

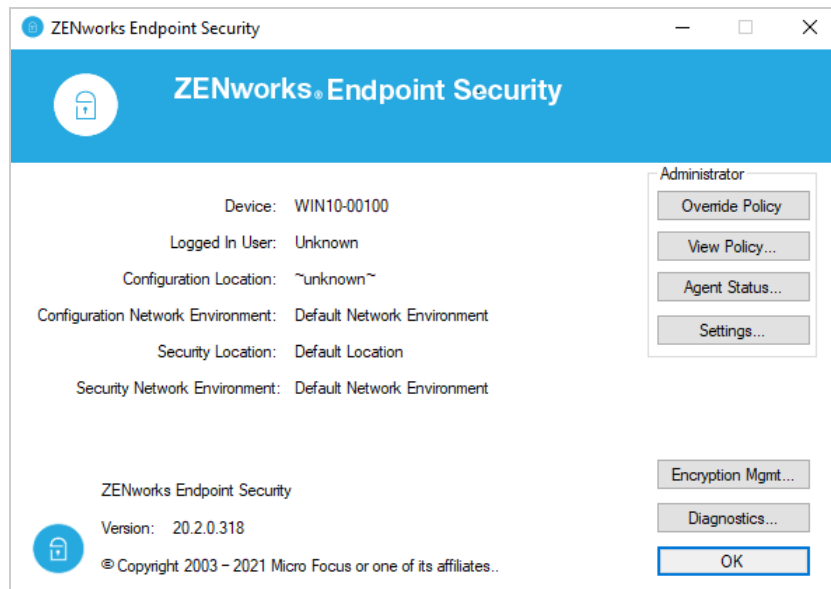


- 3 In the Agent Security section, select **Enable an override password for the ZENworks Agent**, then click **Change** and enter a password of your preference.
- 4 Click **OK** at the bottom of the page to save the changes.
- 5 Wait about 10 minutes for the ZENworks Primary Server's settings cache to be updated.
For performance reasons, the cache is refreshed every 10 minutes with configuration setting updates.
- 6 On your Windows 10 device, right-click the ZENworks icon , then click **Refresh**.
- 7 Once the ZENworks icon stops spinning, right-click the icon, then click **Technician Application** to display the ZENworks Agent window.
- 8 Click **Endpoint Security** (in the left-navigation pane) to display the Endpoint Security page.



- 9 Under Endpoint Security Agent Actions, click **About** to display the Endpoint Security Agent dialog.

The Administrator buttons are only displayed when an override password is set. If you do not see them, close the dialog, wait a few more minutes, and then refresh the device again.



- 10 To disable enforced security policies, click **Override Policy** and enter the override password.

All security policies other than encryption and Antimalware policies are overridden until you click the **Load Policy** button.

Set Up Security Locations

ZENworks provides location awareness to optimize a device's security. For example, you could apply one set of security policies to a device while it is in the office on your private network and another set when it is in a less secure remote location such as a public network.

A device determines its location by evaluating the current network environment against a defined set of network criteria. If the device's current network environment matches the criteria defined for a location, the device uses that location. If the network environment does not match to a location, the predefined Unknown location is used.

You can skip setting up locations if:

- ♦ They do not interest you. Instead, you can designate policies as global, meaning that they apply everywhere and don't rely on locations.
- ♦ You don't want to evaluate the VPN Enforcement policy (see [“Enforce a VPN Connection” on page 67](#)). This policy relies on locations.

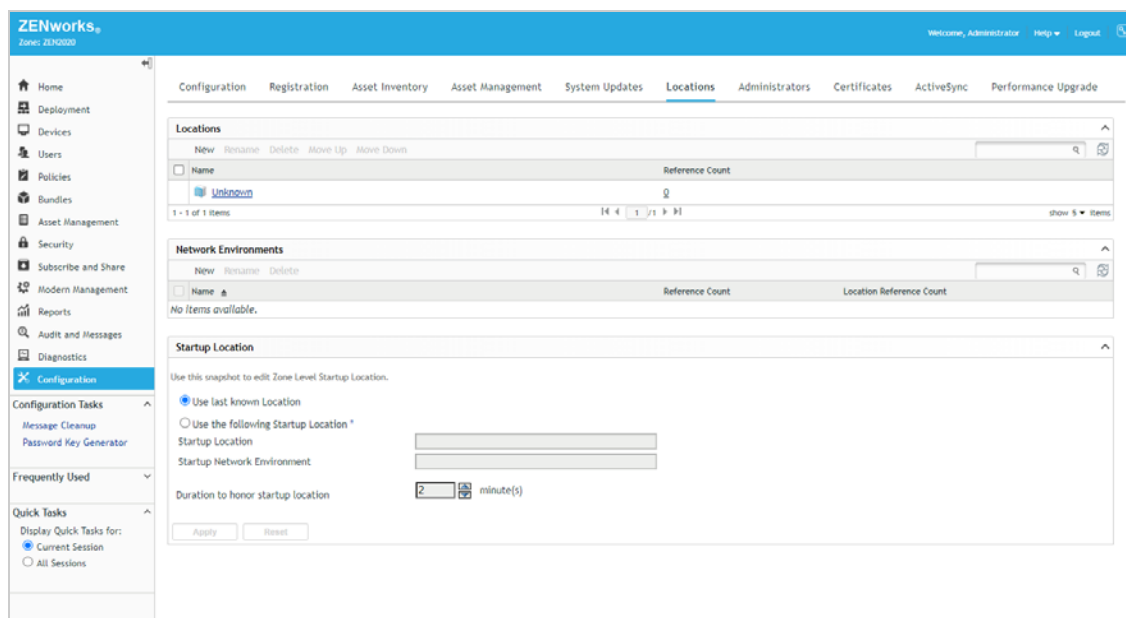
The following sections explain how to define two locations. You'll also create a Location Assignment policy and add the locations to the policy. The Location Assignment policy lets a device know which defined locations to consider for matching against its current network environment.

- ◆ [“Create a Work Location” on page 27](#)
- ◆ [“Create a Pre-VPN Location” on page 29](#)
- ◆ [“Create a Location Assignment Policy” on page 31](#)

Create a Work Location


We'll create a Work location that represents your organization's private network.

- 1 In ZENworks Control Center, click **Configuration** > **Locations** to display the Locations page.



- 2 In the Locations list, click **New** to launch the Create New Location wizard.

Create New Location

 **Step 1: Define Details**
Enter the Location details.

Location Name: *

Description:

Download Throttle Rate (in KB/s): *

Upload Throttle Rate (in KB/s): *

Preferred Protocol for Communication:(Inherited) [Override Setting](#)
By default, the value is inherited from Zone setting.

Audit Data Upload: ▼

CIFS Server:

Fields marked with an asterisk are required.

3 Complete the wizard:

- ◆ **Step 1: Define Details:** Name the location **Work**. Ignore the rest of the fields. (Note: You can name the location whatever you want, but for clarity we'll refer to this location as Work throughout the rest of the evaluation.)
- ◆ **Step 2: Location HTTP Proxy Details:** Ignore these fields.
- ◆ **Step 3: Assign Network Environments:** Keep the **Create and assign Network Environment to the Location** selection.
- ◆ **Step 4: Define Details:** The words **Network Environment** are automatically appended to your location name (for example, **Work Network Environment**). Keep the default and ignore the rest of the fields.
- ◆ **Step 5: Network Environment HTTP Proxy Details:** Ignore these fields.
- ◆ **Step 6: Network Environment Details:** This is where you add the network criteria that define the location. There is a wide range of network services you can use for the criteria in order to refine the location, but for our purposes we'll keep it simple. Select **Client IP Address**, click **Add**, specify your Windows 10 device's IP address, then click **OK** to save it to the list. If you've registered more than one device in ZENworks for the evaluation, repeat this to add that device's IP address as well. You can also use CIDR notation to specify a range of addresses.
- ◆ **Step 7: Summary:** Click **Finish** to create the location.

The location is saved in the Locations list.

Success: The Location has been created successfully.

Configuration Registration Asset Inventory Asset Management System Updates **Locations** Administrators Certificates ActiveSync Performance Upgrade

Locations

New Rename Delete Move Up Move Down

Name	Reference Count
Work	0
Unknown	0

1 - 2 of 2 items show 5 Items

Network Environments

New Rename Delete

Name	Reference Count	Location Reference Count
Work Network Environment	0	1

1 - 1 of 1 items show 5 Items

Startup Location

Use this snapshot to edit Zone Level Startup Location.

Use last known Location
 Use the following Startup Location *

Startup Location:

Startup Network Environment:

Duration to honor startup location: minute(s)

Apply Reset


- 4 Keep the Locations page open and continue with the next section, [Create a Pre-VPN Location](#).

Create a Pre-VPN Location

The VPN Enforcement policy lets you enforce a VPN connection whenever a device switches to the Unknown location (or another “trigger” location). You can use a pre-VPN location to enforce policies, such as a restrictive firewall, until the VPN connection is established. We’ll go ahead and create a pre-VPN location at this time since we’ll need it in [“Enforce a VPN Connection” on page 67](#).

- 1 Make sure you are still on the Locations page.
- 2 In the Locations list, click **New** to launch the Create New Location wizard.

Create New Location

 **Step 1: Define Details**
Enter the Location details.

Location Name: *

Description:

Download Throttle Rate (in KB/s): *

Upload Throttle Rate (in KB/s): *

Preferred Protocol for Communication: (Inherited) [Override Setting](#)
By default, the value is inherited from Zone setting.

Audit Data Upload: Enabled Disabled Disabled

CIFS Server:

Fields marked with an asterisk are required.

3 Complete the wizard:

- ◆ **Step 1: Define Details:** Name the location **Pre-VPN**. Ignore the rest of the fields. (Note: You can name the location whatever you want, but for clarity we'll refer to this location as Pre-VPN throughout the rest of the evaluation.)
- ◆ **Step 2: Location HTTP Proxy Details:** Ignore these fields.
- ◆ **Step 3: Assign Network Environments:** Select the **Do not create and assign Network Environment to this Location** selection. The Pre-VPN location does not need a network environment because the VPN Enforcement policy automatically switches the device to the Pre-VPN location when the policy is triggered from the Unknown location.
- ◆ **Step 4: Summary:** Click **Finish** to create the location.

The location is saved in the Locations list.

Success: The Location has been created successfully.

Configuration Registration Asset Inventory Asset Management System Updates **Locations** Administrators Certificates ActiveSync Performance Upgrade

Locations

New Rename Delete Move Up Move Down

Name	Reference Count
<input type="checkbox"/> Work	0
<input type="checkbox"/> Pre-VPN	0
<input type="checkbox"/> Unknown	0

1 - 3 of 3 items

Network Environments

New Rename Delete

Name	Reference Count	Location Reference Count
<input type="checkbox"/> Work Network Environment	0	1

1 - 1 of 1 items

Startup Location

Use this snapshot to edit Zone Level Startup Location.

Use last known Location

Use the following Startup Location *

Startup Location:

Startup Network Environment:

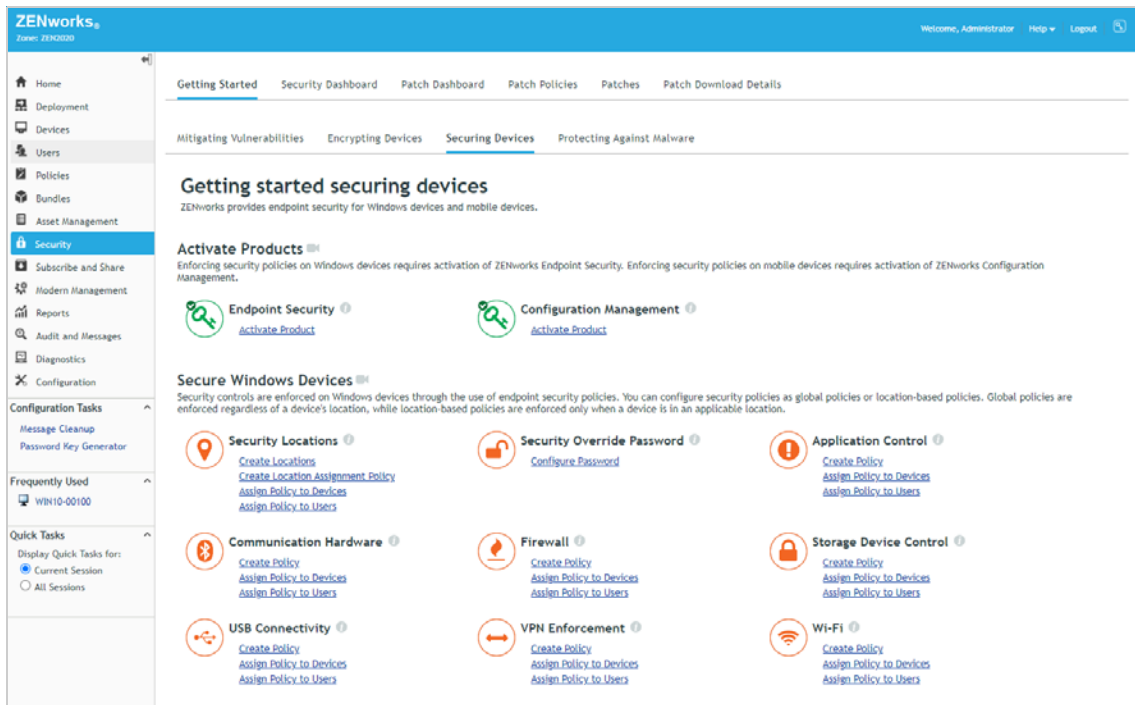
Duration to honor startup location: minute(s)

Apply Reset

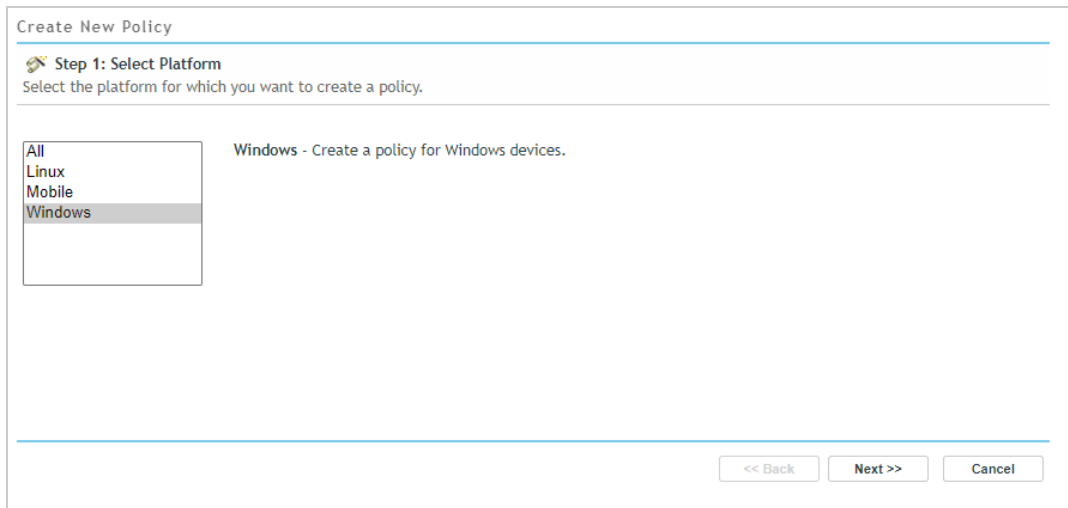
Create a Location Assignment Policy

The Location Assignment policy determines the available security locations for devices. We'll create a Location Assignment policy that includes the Work, Pre-VPN, and Unknown locations and then assign the policy to your Windows 10 device.

- 1 In ZENworks Control Center, click **Security** (in the left navigation pane), then click the **Getting Started** tab.
- 2 Click the **Securing Devices** subtab.



- 3 Under Security Locations, click **Create Location Assignment Policy** to launch the Create New Policy wizard.

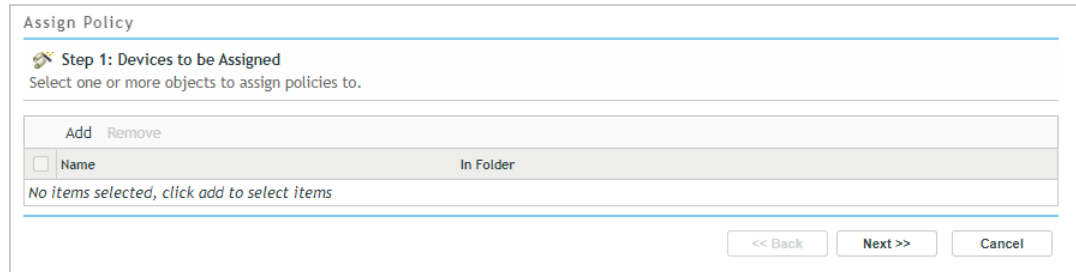


- 4 Complete the wizard:
 - ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
 - ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
 - ◆ **Step 3: Select Policy Type:** Keep the **Location Assignment Policy** selection.
 - ◆ **Step 4: Define Details:** Name the policy **Location Assignment**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as Location Assignment throughout the rest of the evaluation.)

- ◆ **Step 5: Configure Allowed Locations:** In the Allowed Locations list, click **Add**, select the Work and Pre-VPN locations and click **OK** to add them to the list. Keep the Unknown location in the list as well.
- ◆ **Step 6: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

5 Assign the policy:

- 5a In the Security Locations section of the Getting Started Securing Devices page, click **Assign Policy to Devices** to launch the Assign Policy wizard.



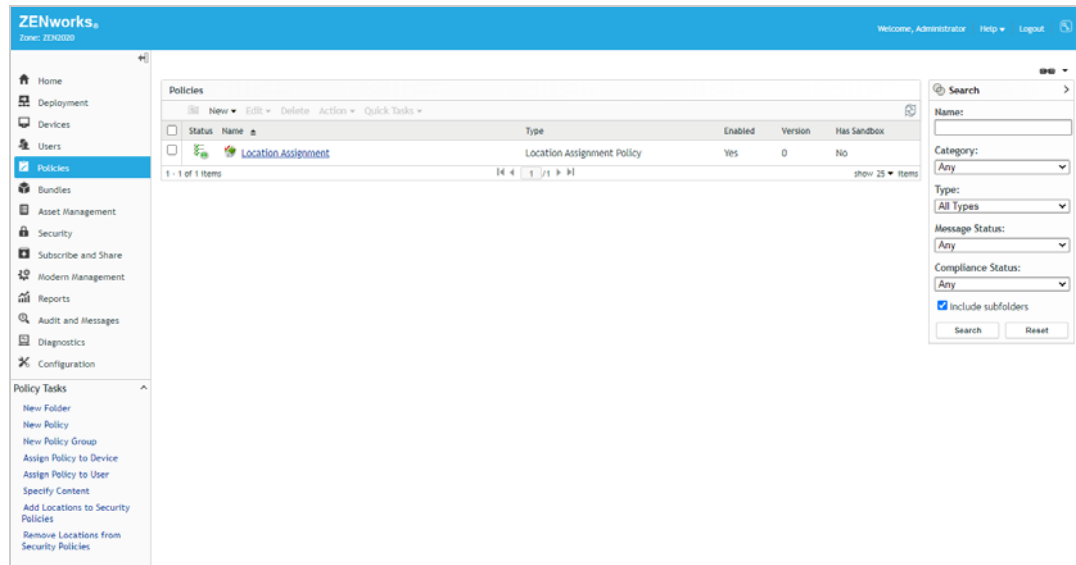
5b Complete the wizard:

- ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
- ◆ **Step 2: Policies to be Assigned:** Select the Location Assignment policy, then click **OK** to add it to the list.
- ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
- ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

6 View the policy:

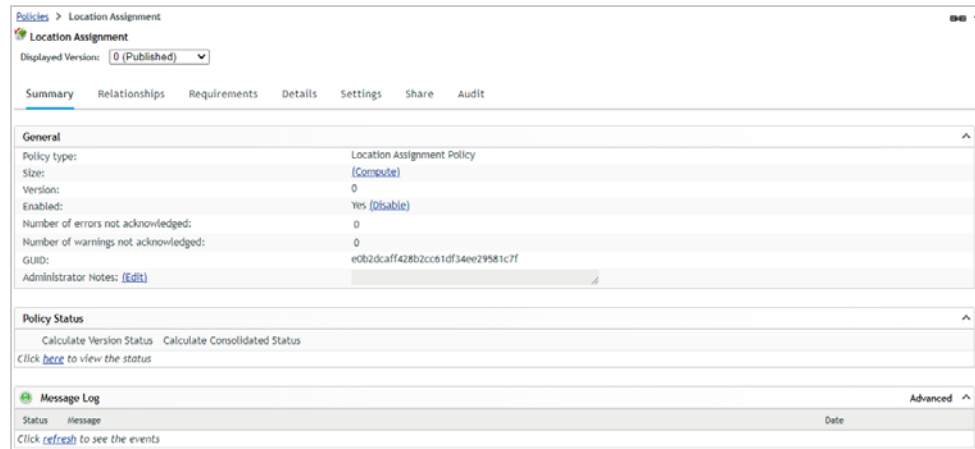
We've used the Getting Started to create the Location Assignment policy, but policies can be created, edited, and deleted using the Policies list. This includes assigning the policy to additional devices or users.


- 6a Click Policies (in the left navigation pane) to display the Policies list.



6b Click the Location Assignment policy to display its details.

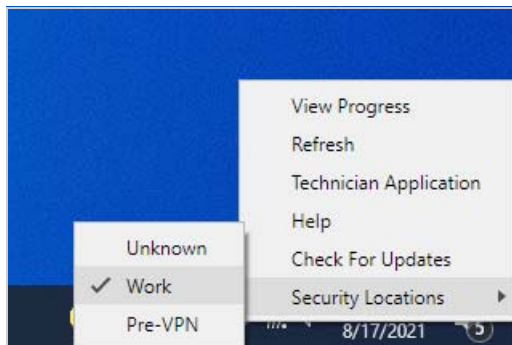
You use the Details tab to change the policy settings and the Relationships tab to add and remove assignments.



7 On your Windows 10 device, right-click the ZENworks icon , then click **Refresh** to enforce the Location Assignment policy.

8 After the ZENworks icon stops spinning, right-click the icon, then click **Security Locations** to display the assigned locations.

For now, it is enough to verify the locations are showing up. We'll do more with them later.

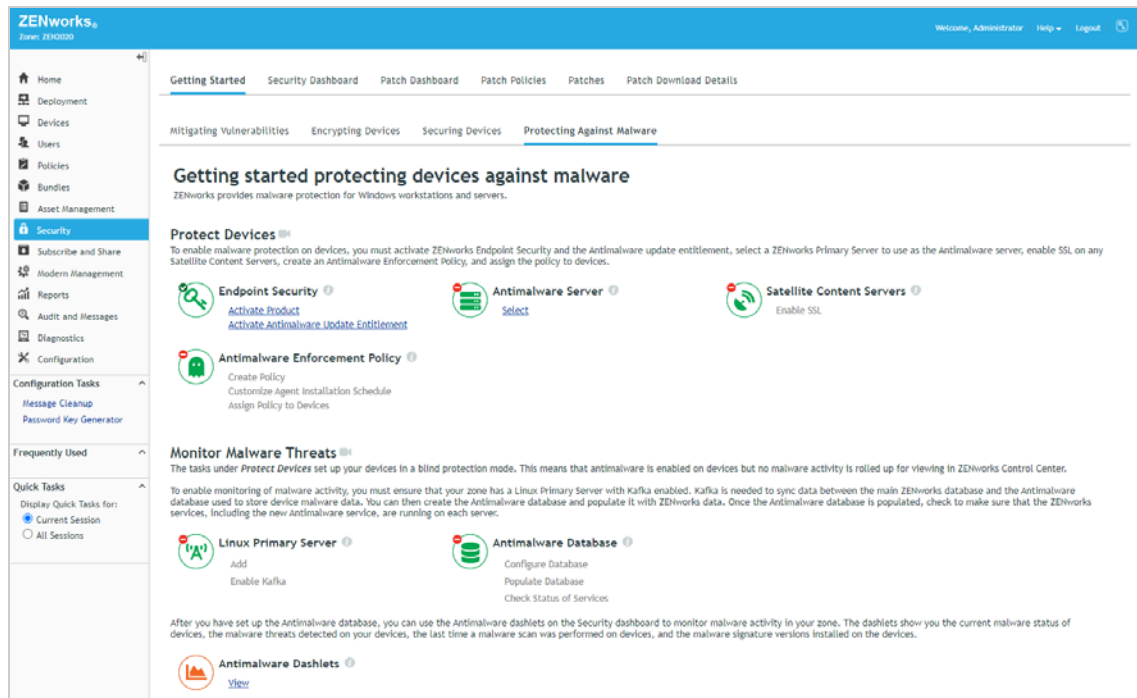


Enable Antimalware

If you plan to evaluate ZENworks Endpoint Security Antimalware, you must enable it in your zone. If not, you can skip this section.

IMPORTANT: Antimalware requires a ZENworks Primary Server that is running on Linux. If you didn't use the ZENworks Virtual Appliance or install your ZENworks Primary Server on a Linux server, you need to do so before you can enable Antimalware. Refer to "[Create a ZENworks System](#)" on page 13 and, when prompted, add the new Linux Primary Server to your existing management zone.

- 1** In ZENworks Control Center, click **Security** (in the left navigation pane), then click the **Getting Started** tab.
- 2** Click the **Protecting Against Malware** subtab.



3 In the Protect Devices section, the Endpoint Security icon should have a green check mark from being activated earlier. If it does not, see [“Activate ZENworks Endpoint Security Management” on page 15.](#)

4 Configure the ZENworks Primary Server as an Antimalware Server.

The Antimalware Server creates the software bundle that installs the Antimalware Agent on devices, initiates maintenance tasks on the Antimalware database, and functions as an Ondemand Content Master to download malware signatures and agent updates from the external service. To access this external service, the server must be able to reach the URL below. If you haven’t configured your environment to allow this, you need to do so before continuing.

`https://microfocus-2dcb60a8-26c9-4560-9cc2-34a16ea5f6e6.2d7dd.cdn.bitdefender.net/`

4a Under Antimalware Server, click **Select**.

4b In the Antimalware Server section, select your Primary Server to function as the Antimalware Server.

4c Click **OK** to save the settings and initiate the creation of the Antimalware Agent bundle.

Notice that there is now a green check mark on the Antimalware Server icon to indicate that this setup task is complete.

5 Ignore the Satellite Content Servers section. This setup task is already marked complete because there are no Satellites in your zone.

Satellites are ZENworks-managed devices that perform roles, such as serving Antimalware content, that are normally done by ZENworks Primary Servers. A device’s Antimalware Agent communicates with ZENworks Primary Servers and Satellites using a secure (SSL) connection to request malware signature updates and agent updates. By default, Primary Servers are configured to serve content via SSL but Satellites are not. If you were to add Satellites to function as Content Servers, you would need to enable them for SSL in order for them to serve Antimalware content to managed devices.

6 Skip the Antimalware Enforcement Policy section for now.

At this point in the setup, you could create an Antimalware Enforcement Policy and assign it to a Windows 10 device. This would install the Antimalware Agent on the device and start protecting the device based on the policy settings. However, no device status or detected malware threats would be rolled up for viewing in the console because the components that support the monitoring functionality are not enabled yet. We'll do that now and have you create the Antimalware Enforcement policy when we get to [Chapter 2, "Protect Against Malware Threats,"](#) on page 39.

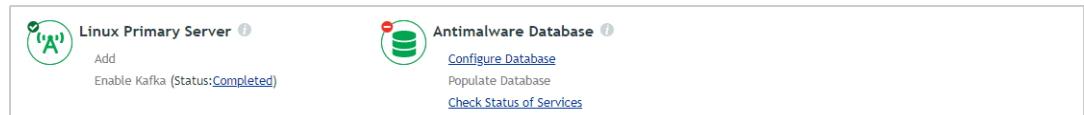
7 Enable Kafka on your Linux Primary Server.

Kafka is needed to sync data between the ZENworks database and the Antimalware database that you'll create in the next step. Kafka only runs on Linux.

7a Under Linux Primary Server, click **Enable Kafka**.

7b In the Linux Primary Server field, select your Primary Server, then click **Enable Kafka**.

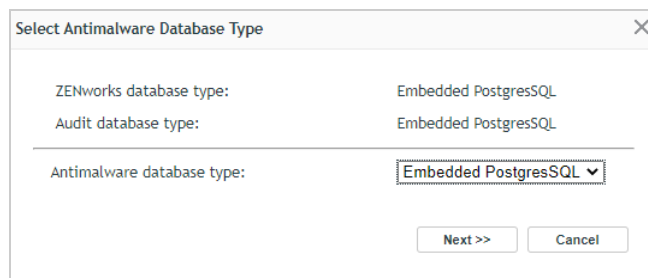
The dialog closes and the Enable Kafka status shows **In Progress**. It takes a minute or two for the task to complete, at which point the status changes to Completed and a green check mark is displayed on the Linux Primary Server icon. In addition, the **Configure Database** link (under Antimalware Database) is now available.



8 Configure the Antimalware database and populate it with data from the ZENworks database.

8a Under Antimalware Database, click **Configure Database** to launch the database configuration wizard and display the Select Antimalware Database Type dialog.

The Antimalware database must be the same database type as your ZENworks database. The selection defaults to that database type.



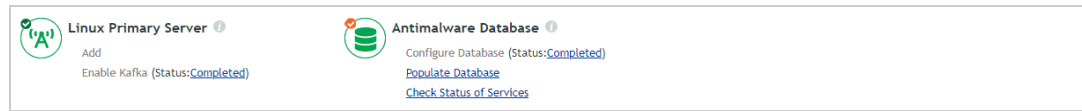
8b Leave the Antimalware database type set to the selected type, then click **Next**.

8c If your database is Embedded PostgreSQL, you don't need to provide any more information. Click **Configure** to start the configuration process.

or

If your database is Oracle or MSSQL, follow the prompts to provide the information needed to configure the database.

The dialog closes and the Configure Database status shows **In Progress**. Click the status to show the status dialog. It won't take long to configure the database in a new zone. Close the dialog and check the progress. Once it has completed, the Populate Database link is enabled.



- 8d** Click **Populate Database**, then click **Start** to populate the Antimalware database with the data it requires from the ZENworks database.

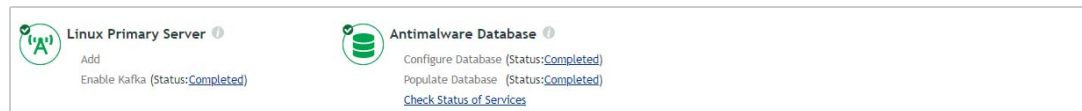
The dialog closes and the Populate Database status shows **In Progress**. It can take up to 15 minutes for the task to complete. During that time, ZENworks Control Center is not available because the ZENworks services shut down.

IMPORTANT: If you have multiple ZENworks servers in your management zone, the database population task can not be initiated from ZENworks Control Center as described above. In a multi-server zone, the dialog that is displayed provides instructions for completing the task. Follow the instructions to shut down your ZENworks servers and manually initiate the task.

- 8e** After 15 minutes, launch ZENworks Control Center again and log in. If you can't log in yet, wait a while longer for the database population process to finish and the ZENworks services to restart, then try again.

- 8f** Go to the Getting Started Protecting Against Malware page.

At this point, the Populate Database status has changed to Completed and a green check mark is displayed on the Antimalware database icon.



- 8g** Click the **Check Status of Services** link to display the Diagnostics page.

The Diagnostics page includes four sections that you'll want to look at. The first is the ZENworks Database section and it should show all three ZENworks databases.

ZENworks Databases						
Status	Database Size	Host	Type	Version	Schema	
✓	0.3 GB	137.65.59.29	PostgreSQL	12.4	ZENworks	
✓	0.02 GB	137.65.59.29	PostgreSQL	12.4	Audit	
✓	0.01 GB	137.65.59.29	PostgreSQL	12.4	Antimalware	

Database size last calculated at: 8:28 PM

The second is the Antimalware Service section that shows the status of the service on each ZENworks server.

Status	Database Size	Host	Type	Version	Schema
✓	0.3 GB	137.65.59.29	PostgreSQL	12.4	ZENworks
✓	0.02 GB	137.65.59.29	PostgreSQL	12.4	Audit
✓	0.01 GB	137.65.59.29	PostgreSQL	12.4	Antimalware

Database size last calculated at: 8:28 PM

The third section (Connector Status) and fourth section (Data Sync Status) shows the status of the Kafka connectors and consumers used to sync data from the ZENworks database to the Antimalware database.

Connector Name	Topic Name	Connector Status
ZENconnector-zdevicefolderrights	zentable_1-zdevicefolderrights	Running
ZENconnector-zpolicyfolderrights	zentable_1-zpolicyfolderrights	Running
ZENconnector-zdevice	zenview_1-zdevice	Running
ZENconnector-zdevicegroupings	zenview_1-zdevicegroupings	Running
ZENconnector-zeffectiveasettings	zenview_1-zeffectiveasettings	Running
ZENconnector-zpolicy	zenview_1-zpolicy	Running
ZENconnector-zsystemsetting	zenview_1-zsystemsetting	Running
ZENconnector-zzenobject	zenview_1-zzenobject	Running
ZENconnector-zzenobjecteq	zentable_1-zzenobjecteq	Running

1 - 9 of 9 items

Topic Name	Consumer Name	Server Name	Last Sync from Kafka	Last Sync to microservice	Consumer Status	Pending records
zentable_1-zdevicefolderrights	antimalware-zdevicefolderrights	zendoc2a-provo.nov...	Aug 09, 2021 08:24 PM	NA	Running	NA
zentable_1-zpolicyfolderrights	antimalware-zpolicyfolderrights	zendoc2a-provo.nov...	Aug 09, 2021 08:25 PM	NA	Running	NA
zenview_1-zdevice	antimalware-zdevice	zendoc2a-provo.nov...	Aug 09, 2021 08:25 PM	NA	Running	NA
zenview_1-zdevicegroupings	antimalware-zdevicegroupings	zendoc2a-provo.nov...	Aug 09, 2021 08:25 PM	NA	Running	NA
zenview_1-zeffectiveasettings	antimalware-zeffectiveasettings	zendoc2a-provo.nov...	Aug 09, 2021 08:24 PM	NA	Running	NA
zenview_1-zpolicy	antimalware-zpolicy	zendoc2a-provo.nov...	Aug 09, 2021 08:25 PM	NA	Running	NA
zenview_1-zsystemsetting	antimalware-zsystemsetting	zendoc2a-provo.nov...	Aug 09, 2021 08:25 PM	NA	Running	NA
zenview_1-zzenobject	antimalware-zzenobject	zendoc2a-provo.nov...	Aug 09, 2021 08:25 PM	NA	Running	NA

1 - 8 of 8 items

If any of the sections show issues, restart your ZENworks server. Restarting the server resolves most issues.

2 Protect Against Malware Threats

ZENworks Endpoint Security Antimalware provides real-time protection against both known and zero-day malware threats (viruses, worms, keyloggers, trojans, and more). The Antimalware Agent (scan engine) uses a variety of technologies—including signatures, file format analyzers and parsers, archive algorithms, emulation, and complex heuristic algorithms—to detect and remediate threats on local drives, removable drives, and network drives.

To protect your Windows 10 device against malware threats, you need to create an Antimalware Enforcement policy and assign it to the device. The policy installs the Antimalware Agent and defines agent behaviors such as on-access (real-time) scanning, on-demand (scheduled) scanning, threat remediation, and quarantine management.

- ♦ “Create an Antimalware Enforcement Policy” on page 39
- ♦ “Assign the Policy” on page 40
- ♦ “Verify the Policy” on page 41
- ♦ “Explore More” on page 43

Create an Antimalware Enforcement Policy

- 1 In ZENworks Control Center, go to the Getting Started Protecting Against Malware page.

The screenshot shows the ZENworks Control Center interface. The top navigation bar includes 'Getting Started', 'Security Dashboard', 'Patch Dashboard', 'Patch Policies', 'Patches', and 'Patch Download Details'. The left sidebar shows a navigation menu with 'Security' selected. The main content area is titled 'Getting started protecting devices against malware' and contains several sections:

- Protect Devices**: A section with a sub-header 'Protect Devices' and a description: 'To enable malware protection on devices, you must activate ZENworks Endpoint Security and the Antimalware update entitlement, select a ZENworks Primary Server to use as the Antimalware server, enable SSL on any Satellite Content Servers, create an Antimalware Enforcement Policy, and assign the policy to devices.' It includes three cards: 'Endpoint Security' (with links 'Activate Product' and 'Activate Antimalware Update Entitlement'), 'Antimalware Server' (with a 'Select' button), and 'Satellite Content Servers' (with an 'Enable SSL' button).
- Antimalware Enforcement Policy**: A card with a 'Create Policy' button and links 'Customize Agent Installation Schedule' and 'Assign Policy to Devices'.
- Monitor Malware Threats**: A section with a sub-header 'Monitor Malware Threats' and a description: 'The tasks under Protect Devices set up your devices in a blind protection mode. This means that antimalware is enabled on devices but no malware activity is rolled up for viewing in ZENworks Control Center. To enable monitoring of malware activity, you must ensure that your zone has a Linux Primary Server with Kafka enabled. Kafka is needed to sync data between the main ZENworks database and the Antimalware database used to store device malware data. You can then create the Antimalware database and populate it with ZENworks data. Once the Antimalware database is populated, check to make sure that the ZENworks services, including the new Antimalware service, are running on each server.' It includes two cards: 'Linux Primary Server' (with 'Add' button and 'Enable Kafka (Status:Completed)') and 'Antimalware Database' (with 'Configure Database (Status:Completed)', 'Populate Database (Status:Completed)', and 'Check Status of Services' buttons).
- Antimalware Dashlets**: A card with a 'View' button.

- 2 In the Antimalware Enforcement Policy section, click **Create Policy** to launch the Create New Policy wizard.
- 3 Complete the wizard:
 - ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
 - ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
 - ◆ **Step 3: Select Policy Type:** Keep the **Antimalware Enforcement Policy** selection.
 - ◆ **Step 4: Define Details:** Name the policy **Antimalware Enforcement**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as Antimalware Enforcement throughout the rest of the evaluation.)
 - ◆ **Step 5: Configure On-Access Scanning:** On-access scans occur when files are opened, copied, moved, or executed and provide real-time protection. The Normal level configures the on-access scan settings for typical coverage. Keep this default setting. After the policy is created, you can customize the individual on-access settings if needed.
 - ◆ **Step 6: Configure On-Demand Scanning:** The policy includes four on-demand scan types: Full, Quick, External Device, and Contextual. This page lets you enable or disable a scan type. For the evaluation, leave all of the scan types enabled. Each scan type includes individual settings that you can customize after the policy is created.
 - ◆ **Step 7: Configure Quarantine Behavior:** These settings configure the device's local quarantine. Keep the defaults.
 - ◆ **Step 8: Configure Scan Exclusions:** The **Use the built-in exclusions...** option enables the Microsoft recommended virus scan exclusions for Windows operating systems. Keep this option enabled. The **Use assigned Antimalware Scan Exclusions policies** option instructs the Antimalware Agent to merge exclusions from any Antimalware Scan Exclusions policies assigned to the device with the custom exclusions you can define in this policy (after creation). For now, keep this option disabled.
 - ◆ **Step 9: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policy

- 1 In the Antimalware Enforcement Policy section of the Getting Started Protecting Against Malware page, click **Assign Policy to Devices** to launch the Assign Policy wizard.

Assign Policy

Step 1: Devices to be Assigned
Select one or more objects to assign policies to.


Add Remove	
<input type="checkbox"/>	Name
	In Folder
No items selected, click add to select items	

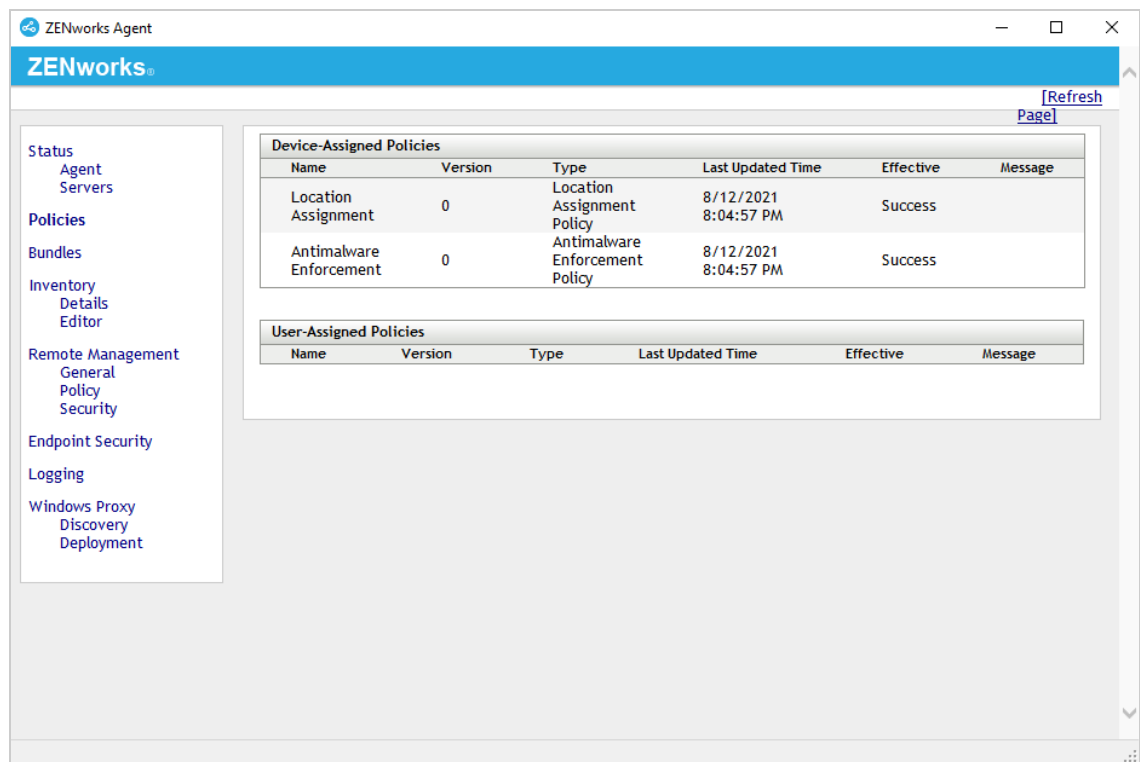
<< Back Next >> Cancel

- 2 Complete the wizard:
 - ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.

- ◆ **Step 2: Policies to be Assigned:** Select the Antimalware Enforcement policy, then click **OK** to add it to the list.
- ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
- ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

Verify the Policy

- 1 On your Windows 10 device, right-click the ZENworks icon , then click **Refresh** to enforce the Antimalware Enforcement policy.
- 2 Once the ZENworks icon stops spinning, right-click the icon, then click **Technician Application** to display the ZENworks Agent window.
- 3 Click **Policies** in the left-navigation pane and verify that the Antimalware Enforcement policy is assigned and effective.



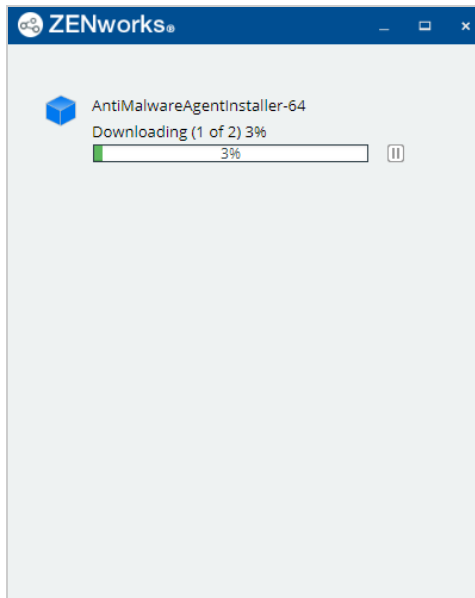
The screenshot shows the ZENworks Agent interface. The left navigation pane is open to the 'Policies' section. The main area displays two tables of assigned policies. The 'Device-Assigned Policies' table shows two entries: 'Location Assignment' and 'Antimalware Enforcement', both with version 0 and a 'Success' status. The 'User-Assigned Policies' table is currently empty.

Device-Assigned Policies					
Name	Version	Type	Last Updated Time	Effective	Message
Location Assignment	0	Location Assignment Policy	8/12/2021 8:04:57 PM	Success	
Antimalware Enforcement	0	Antimalware Enforcement Policy	8/12/2021 8:04:57 PM	Success	


User-Assigned Policies					
Name	Version	Type	Last Updated Time	Effective	Message

- 4 Right-click the ZENworks Agent icon again, then click **View Progress**.

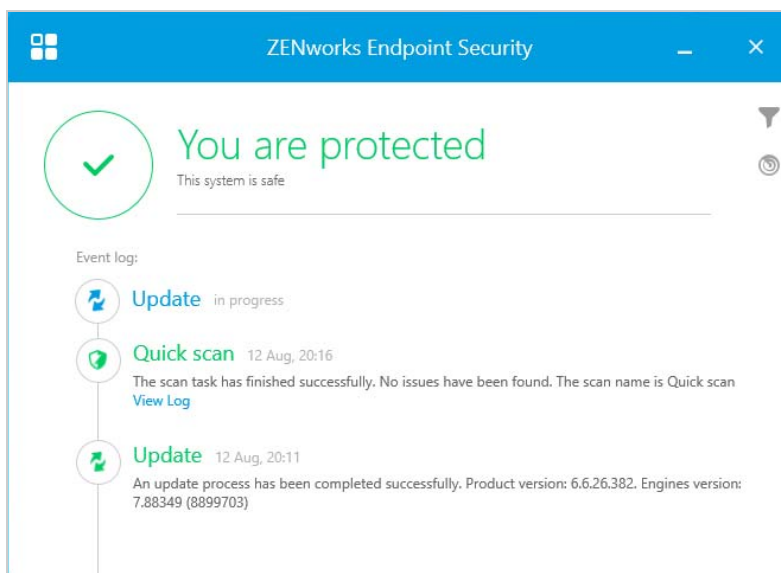
The View Progress dialog displays the progress of the Antimalware Agent file download and installation. If the process hasn't started already, it should start within a few minutes.



By default the Antimalware Agent is installed when the policy is enforced on the device. This is okay in an evaluation environment, but in a production environment you would want to modify the Antimalware Agent installation schedule so that not all assigned devices try to download the agent from the ZENworks Primary Server at the same time. You can access the installation schedule through the **Customize Agent Installation Schedule** link in the Antimalware Enforcement Policy section of the Getting Started Protecting Against Malware page.

- 5 When the Antimalware Agent installation is complete, double-click the new ZENworks Endpoint Security icon  that is added to the notification area to display the Antimalware Agent console.

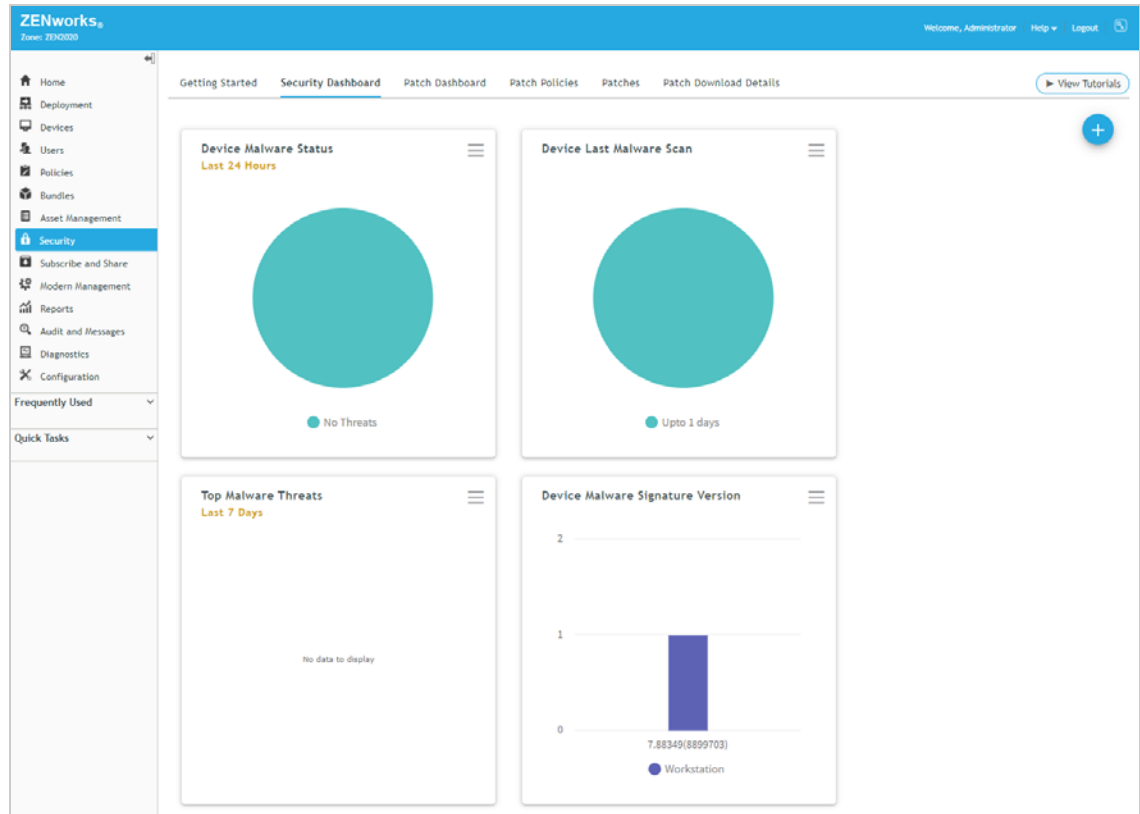
The Antimalware Agent automatically initiates a Quick scan. When the scan is finished, the event log displays the results of the scan.



- 6 Approximately five minutes after the scan completes, log in to ZENworks Control Center and go to the Security Dashboard (**Security > Security Dashboard**).

Whenever a device finishes a scan (or the device is refreshed), the device's malware status and threat details are uploaded to the ZENworks server. You can monitor the results through the four Antimalware dashlets on the Security Dashboard.

In the example screenshot shown below, three of the four dashlets contain data. The Top Malware Threats dashlet does not because no threats were found on the Windows 10 device we used. Clicking a dashlet expands it to show additional detail.



Explore More

Now that ZENworks Endpoint Security Antimalware is set up and the Antimalware Agent is installed on a Windows 10 device, here are some scenarios to help you explore the Antimalware capabilities:

- ♦ [“Antimalware Test Files”](#) on page 44
- ♦ [“Antimalware Enforcement Policy”](#) on page 44
- ♦ [“Malware Scans -- Initiated from the Antimalware Agent”](#) on page 45
- ♦ [“Malware Scans -- Initiated from the ZENworks Agent Command Line Utility \(zac\)”](#) on page 45
- ♦ [“Malware Scans -- Initiated from ZENworks Control Center”](#) on page 46
- ♦ [“Custom and Network Scan Policies”](#) on page 46
- ♦ [“Scan Exclusions”](#) on page 47
- ♦ [“Full and Quick Scan Schedules”](#) on page 47

- ♦ [“User Interaction” on page 48](#)
- ♦ [“Device Malware Status and Threat Monitoring” on page 48](#)

Antimalware Test Files

Obviously, evaluating the ZENworks Endpoint Security Antimalware capabilities is a lot more interesting when you have malware threats to detect. However, introducing real malware threats into our environment is not really what most of us want to do.

The European Institute for Computer Antivirus Research (EICAR) provides a set of four Antimalware Test Files that are non-viral but which the Antimalware Agent will detect as viruses. If you want to use the test files, visit eicar.org and click the “Download Antimalware Testfile” image in the upper-right corner of the Home page. The subsequent page will provide you with complete details and download options for the test files.

Antimalware Enforcement Policy

Review the Antimalware Enforcement policy settings to learn how you can customize the individual scan types and quarantine configuration. To access the policy in ZENworks Control Center, click **Policies** (in the left-navigation pane) to display the Policies list, click the Antimalware Enforcement policy to open it, then click the Details tab to display the policy settings. If you change any settings, you will need to click the Publish button that appears at the top of the policy to republish the policy to your devices.

- ♦ **On-Access Scan:** Scans files as they are opened, copied, moved, and executed. Can be disabled completely if you don’t want on-access scanning (not recommended). The **Scan Locations** settings let you scan local files and network files that are accessed and determine if you want to scan all accessed files, only accessed applications, or only files with a specific extension. The **Scan Behavior** settings let you determine areas you want to scan. The **Remediate Actions** settings let you determine the action to take when infected or suspicious files are detected.
- ♦ **Full Scan:** Intended to be your most thorough scan of the device. Can be disabled completely. The Full scan is run according to the schedule defined in the Antimalware Agent Schedules setting (**Configuration > Management Zone Settings > Security > Antimalware Agent Schedules**). The zone settings can be overridden on device folders and individual devices to provide more granular control.




The **User Rights** settings let you control whether or not users can initiate a Full scan and what actions they can take on a Full scan started by a policy, a Quick Task, or a zac command (i.e. Administrator-initiated scans). The **Files to Scan** settings let you determine if all files are scanned, applications only, or only files with specific extensions. The Scan Targets settings let you determine the locations that will be scanned; this can be all local drives, all removable drives, and/or specific folders on either local or removable drives. The **Scan Behavior** settings let you determine areas you want to scan. The **Remediate Actions** settings let you determine the action to take when infected or suspicious files are detected

- ♦ **Quick Scan:** Intended to be a quicker, more frequent scan of the most common areas attacked by malware. Can be disabled completely. The Quick scan is run according to the schedule defined in the Antimalware Agent Schedules setting (**Configuration > Management Zone Settings > Security > Antimalware Agent Schedules**). The zone settings can be overridden on device folders and individual devices to provide more granular control.

The Quick scan options are identical to the Full scan options.

- ♦ **External Device Scan:** Scans external storage devices upon connection. Can be disabled completely. The External Device scan options are identical to the Full and Quick scan options.
- ♦ **Contextual Scan:** Allows users to right-click a file or folder in Windows Explorer and scan the file or folder. Can only be disabled by hiding the ZENworks Endpoint Security icon ((**Configuration** > **Management Zone Settings** > **Security** > **Antimalware Agent Notification**)). The Scan Behavior and Remediate Action options are identical to the other scans.
- ♦ **Quarantine:** Controls settings for the device's local quarantine.
- ♦ **Exclusions:** Determines which scans the built-in exclusions apply to. Also lets you define custom exclusions in the policy or include the exclusions defined in any Antimalware Scan Exclusion policies assigned to the device.

Malware Scans -- Initiated from the Antimalware Agent

- ♦ **Contextual Scan:** On the device, open Windows Explorer, right-click a folder, then select **Scan with ZENworks Endpoint Security**. Open the Antimalware Agent console. The Event Log will contain an entry for the scan and you can view the scan details. The scan uses the Contextual Scan settings defined in the device's assigned Antimalware Enforcement policy.
- ♦ **External Device Scan:** Insert a USB thumb drive. You will be prompted whether or not to scan the device. Click **Yes**. Open the Antimalware Agent console. The Event Log will contain an entry for the scan and you can view the scan details. The scan uses the External Device Scan settings defined in the device's assigned Antimalware Enforcement policy.
- ♦ **Quick Scan:** Open the Antimalware Agent console. Click the Scan Tasks icon  located towards the upper right of the console. Click **Quick Scan** to initiate the scan. The scan uses the Quick Scan settings defined in the device's assigned Antimalware Enforcement policy.
- ♦ **Full Scan:** Open the Antimalware Agent console. Click the Scan Tasks icon . Click **Full Scan** to initiate the scan. The scan uses the Full Scan settings defined in the device's assigned Antimalware Enforcement policy.
- ♦ **Custom Scan:** Open the Antimalware Agent console. Click the Scan Tasks icon . Click **New custom scan**, then select the scan targets and the scan options. When selecting the scan options, you can select predefined options (Aggressive, Normal, Permissive) or define your own Custom options.

Malware Scans -- Initiated from the ZENworks Agent Command Line Utility (zac)

- ♦ **Quick Scan:** Open a command prompt. Enter `zac malware-scan --quick` or `zac ms --quick`. The scan uses the Quick Scan settings defined in the device's assigned Antimalware Enforcement policy. Open the Antimalware Agent console to see the scan details.
- ♦ **Full Scan:** Open a command prompt. Enter `zac malware-scan --full` or `zac ms --full`. The scan uses the Full Scan settings defined in the device's assigned Antimalware Enforcement policy. Open the Antimalware Agent console to see the scan details.
- ♦ **Custom Scan:** Open a command prompt. Enter `zac malware-scan --custom <custom policy name>` or `zac ms --custom <custom policy name>`. This command can only be used to run a Custom scan using the settings from a Custom Scan policy or Network Scan policy already assigned to the device. You can use `zac malware-policy-list` or `zac mpl` to list all

policies assigned to the device. Open the Antimalware Agent console to see the scan details. NOTE: Custom Scan and Network Scan policy names are case sensitive. You must specify the name using the same lower-case and upper-case letters used when creating the policy. The `zacs mp1` command shows the correct case.

Malware Scans -- Initiated from ZENworks Control Center

- ♦ **Quick Scan:** In ZENworks Control Center, select the device in the Devices list, then click **Quick Tasks > Initiate Malware Scan**. Select **Quick** as the scan type, click **OK**, then click **Start** to send the Quick Task to the device. The scan uses the Quick Scan settings defined in the device's assigned Antimalware Enforcement policy. Open the Antimalware Agent console on the device to see the scan details.
- ♦ **Full Scan:** In ZENworks Control Center, select the device in the Devices list, then click **Quick Tasks > Initiate Malware Scan**. Select **Full** as the scan type, click **OK**, then click **Start** to send the Quick Task to the device. The scan uses the Full Scan settings defined in the device's assigned Antimalware Enforcement policy. Open the Antimalware Agent console on the device to see the scan details.
- ♦ **Custom Scan:** In ZENworks Control Center, select the device in the Devices list, then click **Quick Tasks > Initiate Malware Scan**. Select **Custom** as the scan type, browse for and select a Custom Scan policy that is assigned to the device, click **OK**, then click **Start** to send the Quick Task to the device. This Quick Task can only be used to run a Custom scan using the settings from a Custom Scan policy already assigned to the device. If you select a Custom Scan policy that is not assigned to the device, the scan will not be run. Open the Antimalware Agent console to see the scan details.
- ♦ **Network Scan:** In ZENworks Control Center, select the device in the Devices list, then click **Quick Tasks > Initiate Malware Scan**. Select **Network** as the scan type, browse for and select a Network Scan policy that is assigned to the device, click **OK**, then click **Start** to send the Quick Task to the device. This Quick Task can only be used to run a Network scan using the settings from a Network Scan policy already assigned to the device. If you select a Network Scan policy that is not assigned to the device, the scan will not be run. Open the Antimalware Agent console to see the scan details.

Custom and Network Scan Policies

- ♦ **Custom Scan Policy:** The Custom Scan policy allows you to define a targeted scan that you want run on a different schedule than the Full or Quick scan. For example, you could use a Custom scan to scan for an emerging malware threat or a target location not covered by a device's Quick scan.

To create a Custom Scan policy, click **Policies** to display the Policies list, click **New > Policy** to launch the wizard, select **Windows** as the platform, select **Windows Endpoint Security Policies** as the policy category, select **Antimalware Custom Scan Policy**, then follow the remaining prompts to define the policy. As part of the policy definition, you define the schedule for running the

Custom scan. After defining the policy, assign it to the desired devices. NOTE: Only assign the policy to devices on which the Antimalware Agent has been installed by an Antimalware Enforcement policy. Otherwise, the Custom Scan policy will not be enforced.

- ◆ **Network Scan Policy:** The Network Scan policy allows you to have a device scan network drives. This requires the policy to include credentials that provide Read/Write permissions on the target drives. You define the credentials (using `domain\user` format) in the Credential Vault (**ZCC > Configuration > Credential Vault**).

To create a Network Scan policy, click **Policies** to display the Policies list, click **New > Policy** to launch the wizard, select **Windows** as the platform, select **Windows Endpoint Security Policies** as the policy category, select **Antimalware Network Scan Policy**, then follow the remaining prompts to define the policy. When defining the policy:

- ◆ Add the network directories you want scanned using the following format:
`\\hostName\shareName\directory` or `\\IPAddress\shareName\directory`.
- ◆ Select the `domain\user` formatted credentials from the Credential Vault that provide Read/Write access to the network directories.
- ◆ Define the schedule for running the Network scan.
- ◆ After defining the policy, assign it to the device that you want to perform the scan. NOTE: Only assign the policy to a device on which the Antimalware Agent has been installed by an Antimalware Enforcement policy. Otherwise, the Network Scan policy will not be enforced.

Scan Exclusions

- ◆ **Policy-specific exclusions:** Files, folders, file types, and processes can be excluded from malware scans. Scan exclusions you define within a policy (Enforcement policy, Custom Scan policy, or Network Scan policy) apply only to scans initiated by that policy. Because there are multiple scan types (On-Access, Full, Quick, External Device, Contextual) in the Enforcement policy, you can specify which types the exclusion applies to. To add an exclusion, open the policy details in ZENworks Control Center, click the **Exclusions** tab, enable the **Use the custom exclusions** option, then click **New** to define the exclusion.
- ◆ **Global exclusions:** If you want scan exclusions to apply to multiple policies, you can define the exclusions in the Scan Exclusions policy. For example, you might want your Enforcement policy and all Custom policies to use the same set of exclusions. Or, you might have multiple Enforcement policies that you will use for different devices but want them to all use the same exclusions. To create a Scan Exclusions policy in ZENworks Control Center, click **Policies** to display the Policies list, click **New > Policy** to launch the wizard, select **Windows** as the platform, select **Windows Endpoint Security Policies** as the policy category, select **Antimalware Scan Exclusions Policy**, then follow the remaining prompts to define the policy. Assign the policy to the devices that you want to be able to use the exclusions, then edit the Enforcement, Custom, and Network policies to enable the **Use Antimalware Scan Exclusion policies assigned to device** option.

Full and Quick Scan Schedules

- ◆ **Full Scan Schedule:** By default, Full scans are scheduled to run once a week at 11:00 am on Wednesday. To change the schedule for all devices, modify the schedule at the zone level (**Configuration > Management Zone Settings > Security > Antimalware Agent Schedules > Full Scan**

Schedule). You can override the zone setting on device folders and individual devices (folder|device > Settings > Security > Antimalware Agent Schedules > Full Scan Schedule). After you change the schedule, you need to refresh the device before the new schedule will be used.

- ◆ **Quick Scan Schedule:** By default, Quick scans are scheduled to run daily at 11:00 am except for Wednesday. To change the schedule for all devices, modify the schedule at the zone level (Configuration > Management Zone Settings > Security > Antimalware Agent Schedules > Quick Scan Schedule). You can override the zone setting on device folders and individual devices (folder|device > Settings > Security > Antimalware Agent Schedules > Quick Scan Schedule). After you change the schedule, you need to refresh the device before the new schedule will be used.

User Interaction

- ◆ **User-Initiated Scan Rights:** By default, users can start Full, Quick, Custom, and Network scans. To disable this ability, edit the policy (Enforcement, Custom, or Network) and turn off the **Start scans and pause, postpone, or cancel those scans** option. Re-publish the policy, refresh the device, open the Antimalware Agent console, then attempt to start one of the scans. It will be disabled.
- ◆ **Administrator-Initiated Scan Rights:** By default, users can pause or postpone Full, Quick, Custom, and Network scans started by policies, a ZCC Quick Task, or the `zac malware-scan` command. They are not allowed to cancel the scans. To change these rights, edit the policy (Enforcement, Custom, or Network) and modify the **Pause scans...** option, the **Postpone scans...** option, and the **Cancel scans...** option. Re-publish the policy and refresh the device. Initiate a scan on the device via a Quick Task (see “[Malware Scans -- Initiated from ZENworks Control Center](#)” on page 46), open the Antimalware Agent console on the device, then confirm that only the enabled actions are displayed for the scan.
- ◆ **Agent Notifications:** By default, the Antimalware Agent icon is displayed in the notification area and the user receives notifications of security actions being performed by the agent (such as scans being started and completed) and alerts for security actions that require user intervention (such as prompts to scan an inserted USB device). You can control the level of notifications and alerts provided, even going as far as to turn off all notifications and remove the agent icon from the notification area. You can modify the settings at the zone level (**Configuration > Management Zone Settings > Security > Antimalware Agent Notifications**) for all devices. To provide more granular control, you can override the zone settings on device folders and individual devices (folder|device > Settings > Security > Antimalware Agent Notifications). After you change the settings, you need to refresh the device before the new settings will be used.

Device Malware Status and Threat Monitoring

- ◆ **Device Malware Status Dashlet:** This dashlet is located on the Security Dashboard (**Security > Security Dashboard**). It categorizes devices in four malware statuses based on the last 24 hours (the default), last 7 days, or last 30 days:
 - ◆ **No Threats:** No malware threats have been detected on the device during the selected time period.
 - ◆ **Resolved Threats:** Malware threats were detected on the device during the selected time period but all infected files have been disinfected, quarantined, or deleted.

- ◆ **Unresolved Threats:** Malware threats were detected on the device during the selected time period and at least one file was ignored or file access has been denied. This is an unresolved state because the file could still be a threat to the system.
- ◆ **Unknown:** The device has not reported its status within the last three days.

You can expand the dashlet to view details for each device and drill down into each device for additional details.

- ◆ **Device Last Malware Scan Dashlet:** This dashlet is located on the Security Dashboard (**Security > Security Dashboard**). It shows you the last time a scan was performed on the device. You can expand the dashlet to view details for each device and to customize the dashlet.
- ◆ **Top Malware Threats:** This dashlet is located on the Security Dashboard (**Security > Security Dashboard**). It shows the top 10 detected malware threats either by most recently detected (default), most infected devices, or most unresolved devices. You can expand the dashlet to view details for each detected malware threat and drill down into a threat for additional details.
- ◆ **Device Malware Signature Version:** This dashlet is located on the Security Dashboard (**Security > Security Dashboard**). It shows the malware signature version in use by each device. You can expand the dashlet to view details for each device and, if needed, initiate a signature update for a device. You can also customize the dashlet to show the Antimalware Agent version in use by each device.

3 Protect Data

The amount of sensitive data stored on endpoints today makes endpoint security more critical than ever. Encryption is an important security measure, and ZENworks Endpoint Security Management lets you encrypt data on both fixed disks and removable drives. And, if you don't want data being copied to USB drives or other types of removable drives, you can restrict or remove access to those drives.

- ♦ [“Encrypt Removable Drives” on page 51](#)
- ♦ [“Encrypt Folders on Fixed Disks” on page 56](#)
- ♦ [“Control Access to Removable Drives” on page 60](#)

Encrypt Removable Drives

ZENworks Endpoint Security Management uses Microsoft BitLocker to encrypt removable data drives.

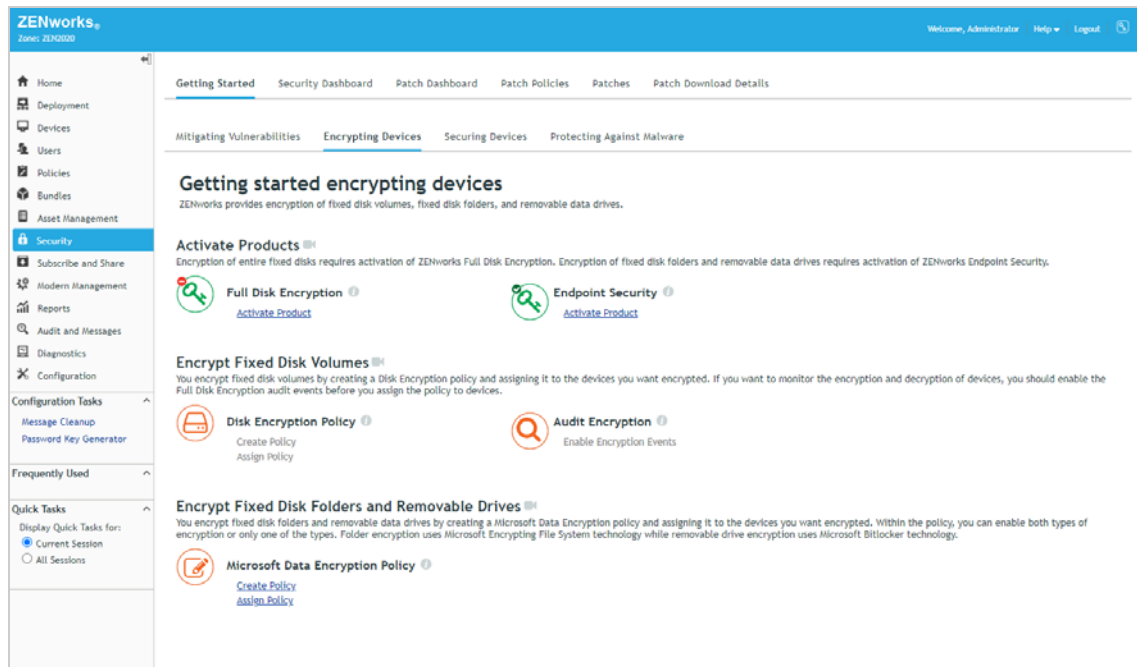
In addition to the standard BitLocker settings, ZENworks provides enhancements such as user hints for forgotten passwords, a “no password” option that unlocks encrypted drives only on ZENworks-managed devices, and encryption exclusion of designated removable drives.

Removable drive encryption is enforced through the Microsoft Data Encryption policy. We'll have you create a policy and encrypt a drive.

- ♦ [“Create a Microsoft Data Encryption Policy” on page 51](#)
- ♦ [“Assign the Policy” on page 52](#)
- ♦ [“Verify the Policy” on page 53](#)

Create a Microsoft Data Encryption Policy

- 1 In ZENworks Control Center, go to the Getting Started Encrypting Devices page.



- 2 In the Microsoft Data Encryption Policy section, click **Create Policy** to launch the Create New Policy wizard.
- 3 Complete the wizard:
 - ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
 - ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
 - ◆ **Step 3: Select Policy Type:** Keep the **Microsoft Data Encryption Policy** selection.
 - ◆ **Step 4: Define Details:** Name the policy **Data Encryption**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as Data Encryption throughout the rest of the evaluation.)
 - ◆ **Step 5: Configure BitLocker Encryption for Removable Data Drives:** Review the settings to see what each one does, but keep the default selections for now.
 - ◆ **Step 6: Configure Folder Encryption for Fixed Disks:** The policy also lets you enable folder encryption on fixed drives. For now, deselect **Enable folder encryption** to turn this feature off. We'll have you turn it on in "[Encrypt Folders on Fixed Disks](#)" on page 56.
 - ◆ **Step 7: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policy

- 1 In the Microsoft Data Encryption Policy section of the Getting Started Encrypting Devices page, click **Assign Policy to Devices** to launch the Assign Policy wizard.

Assign Policy

Step 1: Devices to be Assigned
Select one or more objects to assign policies to.

Add Remove


<input type="checkbox"/>	Name	In Folder
No items selected, click add to select items		

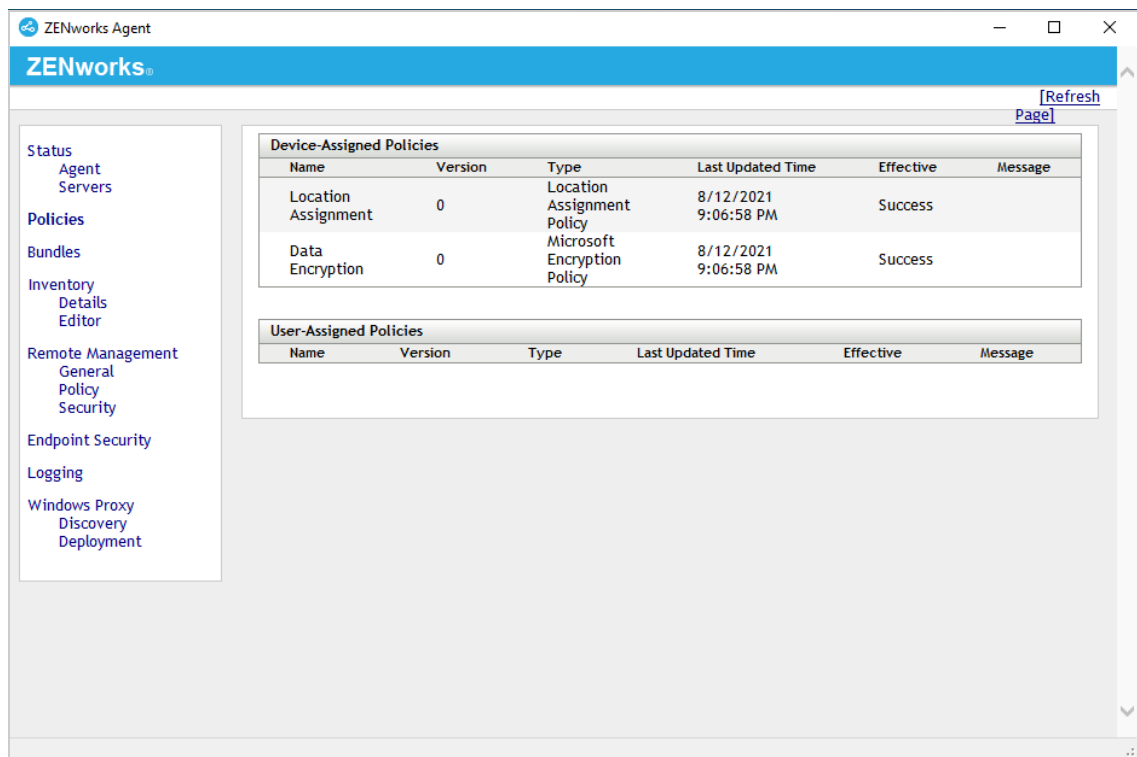
<< Back Next >> Cancel

2 Complete the wizard:

- ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
- ◆ **Step 2: Policies to be Assigned:** Select the Data Encryption policy, then click **OK** to add it to the list.
- ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
- ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

Verify the Policy

- 1 On your Windows 10 device, right-click the ZENworks icon , then click **Refresh** to enforce the Data Encryption policy.
- 2 Once the ZENworks icon stops spinning, right-click the icon, then click **Technician Application** to display the ZENworks Agent window.
- 3 Click **Policies** in the left-navigation pane and verify that the Data Encryption policy is assigned and effective.



ZENworks Agent

ZENworks

[Refresh Page]

Device-Assigned Policies

Name	Version	Type	Last Updated Time	Effective	Message
Location Assignment	0	Location Assignment Policy	8/12/2021 9:06:58 PM	Success	
Data Encryption	0	Microsoft Encryption Policy	8/12/2021 9:06:58 PM	Success	

User-Assigned Policies

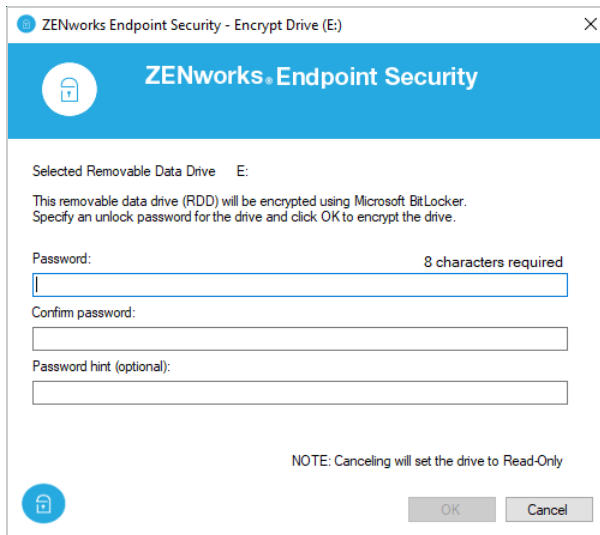
Name	Version	Type	Last Updated Time	Effective	Message
------	---------	------	-------------------	-----------	---------

Left navigation pane:

- Status
 - Agent
 - Servers
- Policies
- Bundles
- Inventory
 - Details
 - Editor
- Remote Management
 - General
 - Policy
 - Security
- Endpoint Security
- Logging
- Windows Proxy
 - Discovery
 - Deployment


4 Insert a USB drive.

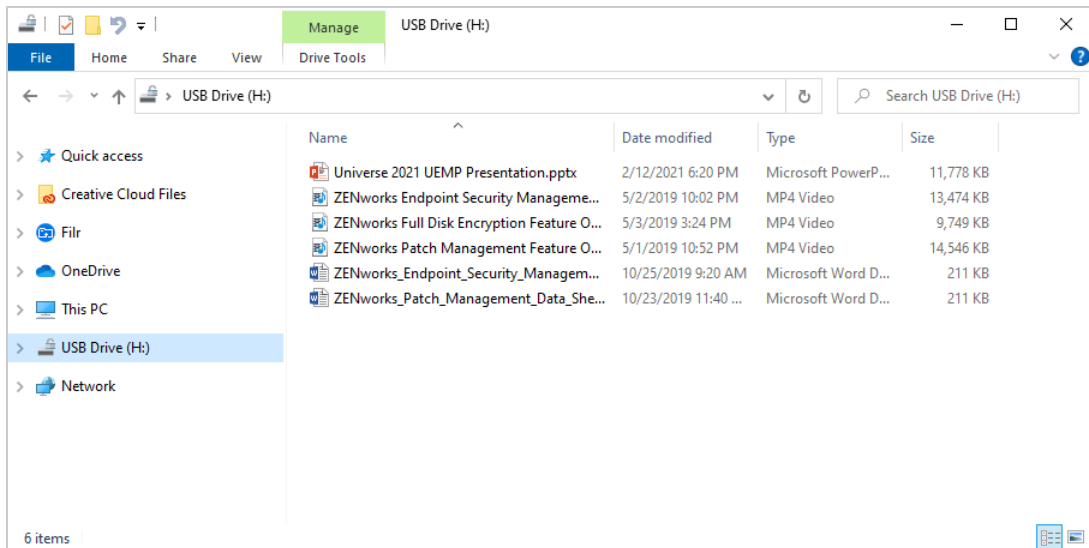
You are prompted to define an unlock password for the removable drive.



5 Enter a password and confirm it, provide a forgotten-password hint, then click **OK** to encrypt the drive.

6 When encryption is complete, open Windows Explorer.

The removable drive has the standard icon  for an unlocked BitLocker-protected drive. Open a file to verify that the drive's files are accessible.

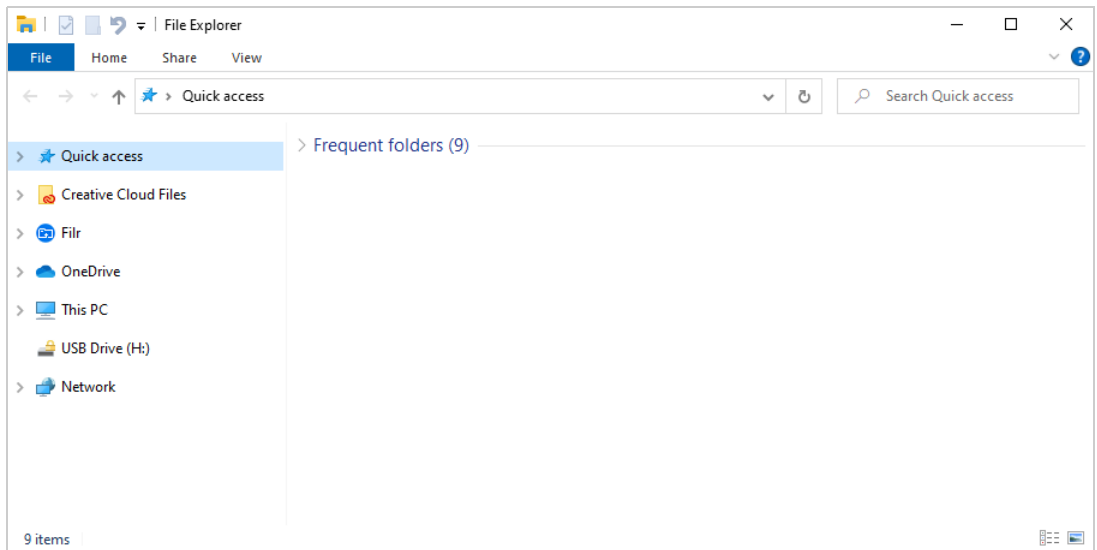


7 Eject the drive and reinsert it.

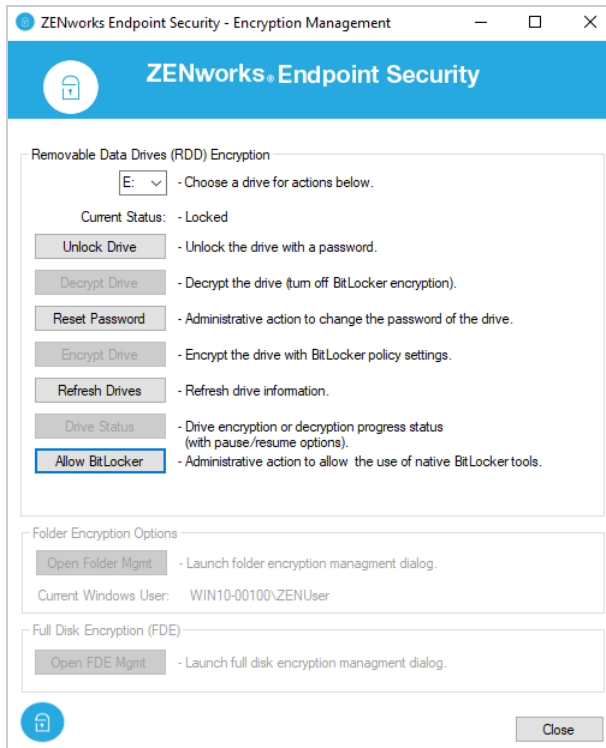
8 When prompted to unlock the drive, click **Cancel**.

9 Open Windows Explorer.

The removable drive has the standard icon  for a locked BitLocker-protected drive and the drive's files are not accessible.



- 10 Click the drive to display the ZENworks Encryption Management dialog that you can use to unlock the drive and perform other management tasks.



Encrypt Folders on Fixed Disks

ZENworks Endpoint Security Management uses Microsoft Windows Encrypting File System (EFS) technology to encrypt folders on a device’s fixed disks. Folders can be encrypted by policy or by user.

By default, a user can access an encrypted folder immediately after logging in to Windows. To enhance security, you can enforce a secondary authentication password that the user must enter after Windows login to gain access to the encrypted folders.

In some cases, such as a user forgetting his secondary authentication password or leaving the organization, it might be necessary to recover encrypted files from a device. To accomplish this, you can log in to the device through a Windows administrator account and use the policy-defined Administrator Recovery Password to gain access to the folders. Or, if the device is no longer ZENworks-managed, you can use the standalone folder decryption tool and the centrally-stored encryption certificate to decrypt the folders.

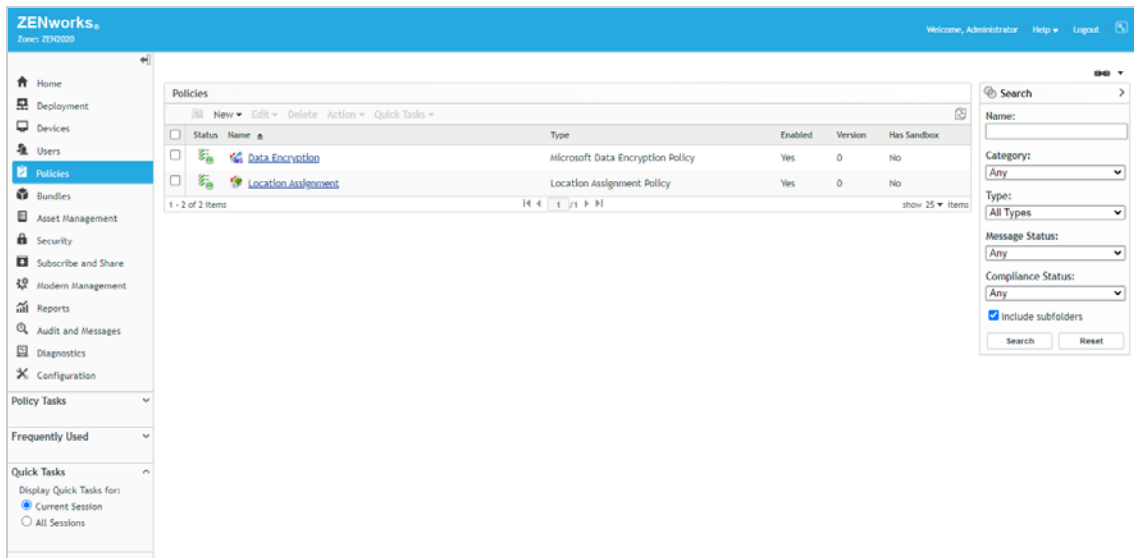
Folder encryption is configured through the Microsoft Data Encryption policy. We’ll have you modify the policy you created in [“Encrypt Removable Drives” on page 51](#) to enable and configure folder encryption, republish the policy, and enforce the new policy on your Windows 10 device.

- ♦ [“Modify the Microsoft Data Encryption Policy” on page 56](#)
- ♦ [“Verify the Policy” on page 58](#)

NOTE: The ZENworks Full Disk Encryption product also provides encryption of entire fixed disk volumes. If you want to evaluate full disk encryption, use the Getting Started Encrypting Devices page to activate ZENworks Full Disk Encryption and create a Disk Encryption policy. The videos on the page provide helpful guidance as well.

Modify the Microsoft Data Encryption Policy

- 1 In ZENworks Control Center, click **Policies** (in the left-navigation pane) to display the Policies list.



- 2 Click the Data Encryption policy to open the policy, then click the **Details** tab to display the policy settings.

The screenshot shows the 'Data Encryption' policy configuration page. The 'Details' tab is selected. Under the 'Removable Data Drives' subtab, the following settings are visible:

- Enable Removable Data Drive encryption
- Encryption Algorithms**
 - Compatible mode (AES-CBC)
 - New encryption mode (XTS-AES)
 - XTS-AES if supported; otherwise AES-CBC
- Initial Encryption**
 - Encrypt used drive space only
 - Encrypt entire drive
- Unlock Method**
 - Always prompt for the unlock password
 - Prompt for the password on first use; auto-unlock on subsequent uses on same device
 - No unlock password: auto-unlock on ZENworks managed devices only; no access on non-managed devices
 - Require a strong unlock password
- Encrypted Drives**
 - Apply these policy settings to BitLocker drives that were not encrypted via ZENworks
 - Apply these policy settings to BitLocker drives (encrypted via ZENworks) if the drive's encryption settings are different
- Excluded Drives**
 - Drives to Exclude from Encryption
 - Buttons: Add, Export, Delete
 - Table with columns: Name, Device Summary, Comment
 - Message: No items available.

Buttons for 'Apply' and 'Reset' are located at the bottom of the page.

- 3 Click the **Fixed Disk Folders** subtab.

The screenshot shows the 'Data Encryption' policy configuration page with the 'Fixed Disk Folders' subtab selected. The following settings are visible:

- Enable folder encryption
- Administrator Recovery**
 - Administrator Decryption Password: [Text Field] [Set...](#)
- Encrypted Folders**
 - Default Encrypted Folders
 - Buttons: Add, Remove
 - Table with column: Folder Location
 - Message: No items available.
 - Show encrypted folders/files in color
- Secondary Authentication**
 - After Windows login, require user to enter a secondary password to decrypt folders
 - Require a strong secondary password

Buttons for 'Apply' and 'Reset' are located at the bottom of the page.

- 4 Select **Enable folder encryption**.
- 5 In the Administrator Recovery section, click **Set** to define an Administrator Decryption Password.

The password enables an administrator to access encrypted folders on any device to which the policy is applied.

- 6 In the Default Encrypted Folders list, click **Add**, enter `C:\%USERPROFILE%\Documents\Encrypted`, then click **OK** to add the folder to the list.

This creates a folder named Encrypted in the Documents folder of the logged-in user. If the Encrypted folder were to already exist, the existing folder and its contents would be encrypted. You could encrypt other folders and even encrypt the Documents folder itself, but we'll just do the Encrypted folder for now and let you explore more later on your own.


- 7 Leave the **Show encrypted folders/files in color** option enabled.
- 8 Under Secondary Authentication, enable the **After Windows login, require user to...** option.

When the policy is applied, the user will be prompted to define the password. After subsequent Windows logins the user will be prompted for the password in order to access the encrypted folders.

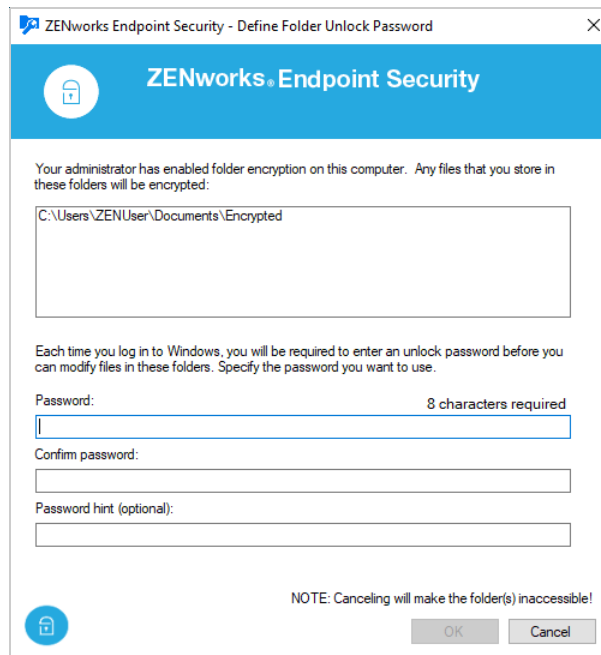
- 9 Click **Apply** to save the policy changes.
- 10 Click **Publish** > **Finish** to make the policy available to assigned devices.

Notice the published policy has a new version number.

Verify the Policy

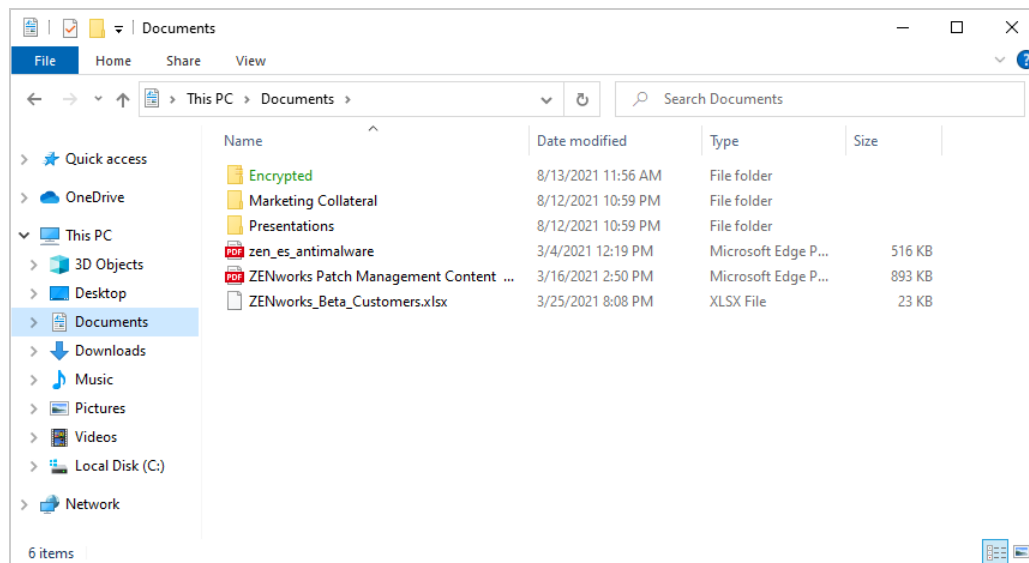
- 1 On your Windows 10 device, right-click the ZENworks icon , then click **Refresh** to enforce the Data Encryption policy.

After a moment, the Define Folder Unlock Password dialog is displayed.



The screenshot shows a dialog box titled "ZENworks Endpoint Security - Define Folder Unlock Password". The dialog has a blue header with the ZENworks logo and the text "ZENworks® Endpoint Security". Below the header, there is a message: "Your administrator has enabled folder encryption on this computer. Any files that you store in these folders will be encrypted:". A text box contains the path "C:\Users\ZENUser\Documents\Encrypted". Below this, another message reads: "Each time you log in to Windows, you will be required to enter an unlock password before you can modify files in these folders. Specify the password you want to use." There are three input fields: "Password:" with a note "8 characters required", "Confirm password:", and "Password hint (optional):". At the bottom, there is a note: "NOTE: Canceling will make the folder(s) inaccessible!" and two buttons: "OK" and "Cancel".

- 2 Enter a password and confirm it, provide a forgotten-password hint, then click **OK**.
- 3 Open Windows Explorer and go to the Documents folder.
The newly-created Encrypted folder displays in green to indicate it is encrypted.



4 Try the following:

- ◆ Move a document into the Encrypted folder and open the folder. You'll see that the document has a lock overlay indicating that it is encrypted.
- ◆ Open the document in the Encrypted folder. It should open with no problem.
- ◆ Select a folder you want to encrypt, right-click the folder, click **ZENworks folder encryption > Encrypt folder**. Click **Yes** to confirm the encryption. As soon as encryption finishes on the folder, the folder name turns green.
- ◆ Move a document from the Encrypted folder to a non-encrypted folder. Notice that the document remains encrypted.
- ◆ Right-click the encrypted document that is not in an encrypted folder. Notice that you can't decrypt an individual file; decryption and encryption are initiated at the folder level only. Move the encrypted file into the folder you encrypted (not the Encrypted folder that was encrypted by policy). If you want to decrypt the folder and its files, right-click the folder, click **ZENworks folder encryption > Decrypt folder**. Click **Yes** to confirm the decryption.
- ◆ Right-click the folder you encrypted, click **ZENworks folder encryption > Manage folder encryption settings** to display the Folder Encryption Management dialog. This dialog shows both the policy-encrypted and user-encrypted folders, lets you clear the secondary authentication password and define a new one, lets you unlock folders if you canceled the unlock during login, and lets you add and remove encryption on user folders.
- ◆ In ZENworks Control Center, click **Devices**, locate and open your Windows 10 device, then click the Encryption tab. Notice that the Folder Encryption Certificates list contains the EFS certificate used to encrypt the folders. This certificate can be used with the standalone decryption utility to move and decrypt files in encrypted folders. We won't go into that in the evaluation.
- ◆ Restart your device and log in. When prompted for your folder unlock password, click **Cancel** and confirm the cancellation. Open Windows Explorer and try to open one of the encrypted folders. Access is denied. Right-click one of the folders, click **ZENworks folder encryption > Manage folder encryption settings**. When prompted, enter the unlock password. The encrypted folders will now be accessible.

Control Access to Removable Drives

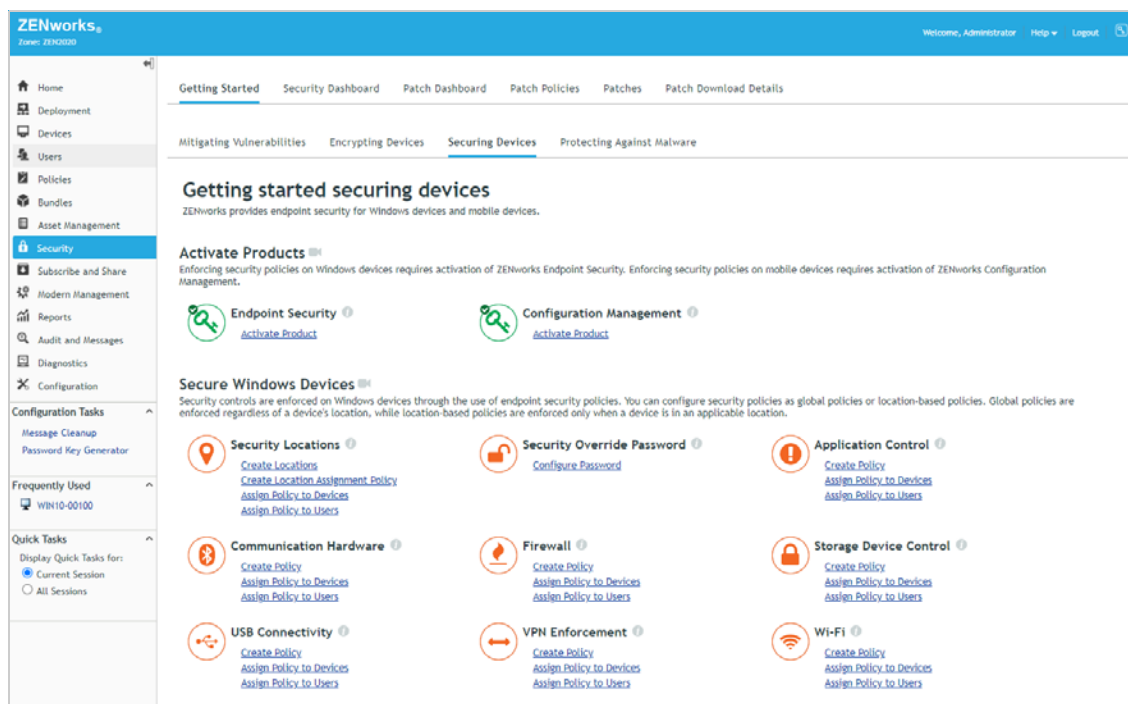
Removable drives are one of the easiest ways to transfer data from devices. In some cases, you might want users to be able to read data from removable drives such as USBs but not write data to those drives. Or maybe you don't want users to be able to access removable storage on Windows Portable Devices such as mobile phones and tablets.

The Storage Device Control policy lets you control access to removable storage devices such as USBs, WPDs, DVDs/CDs, and storage cards. We'll have you create a policy to set all USB drive access to Read Only so that data can be read from USB drives but not written to them.

- ◆ “Create a Storage Device Control Policy” on page 60
- ◆ “Assign the Policy” on page 61
- ◆ “Verify the Policy” on page 61

Create a Storage Device Control Policy

- 1 In ZENworks Control Center, go to the Getting Started Securing Devices page.



- 2 In the Storage Device Control section, click **Create Policy** to launch the Create New Policy wizard.
- 3 Complete the wizard:
 - ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
 - ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
 - ◆ **Step 3: Select Policy Type:** Keep the **Storage Device Control Policy** selection.

- ◆ **Step 4: Define Details:** Name the policy **USB Read-Only Access**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as USB Read-Only Access throughout the rest of the evaluation.)
- ◆ **Step 5: Configure Inheritance and Location Assignments:** You can enforce the policy globally (in all locations) or in specific locations only. For this evaluation, we'll enforce it globally, so keep the **Global Policy - available in all locations** selection.
- ◆ **Step 6: Configure Storage Device Control Settings:** Read/Write is the default access for all removable storage devices. To override the default access for USB devices, select the **USB Device Access** check box, then change the access to **Read Only**. The Exception List lets you define USB devices and assign different access to them. You can explore that capability later.
- ◆ **Step 7: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policy

- 1 In the Storage Device Control section on the Getting Started Securing Devices page, click **Assign Policy to Devices** to launch the Assign Policy wizard.

Assign Policy

Step 1: Devices to be Assigned
Select one or more objects to assign policies to.

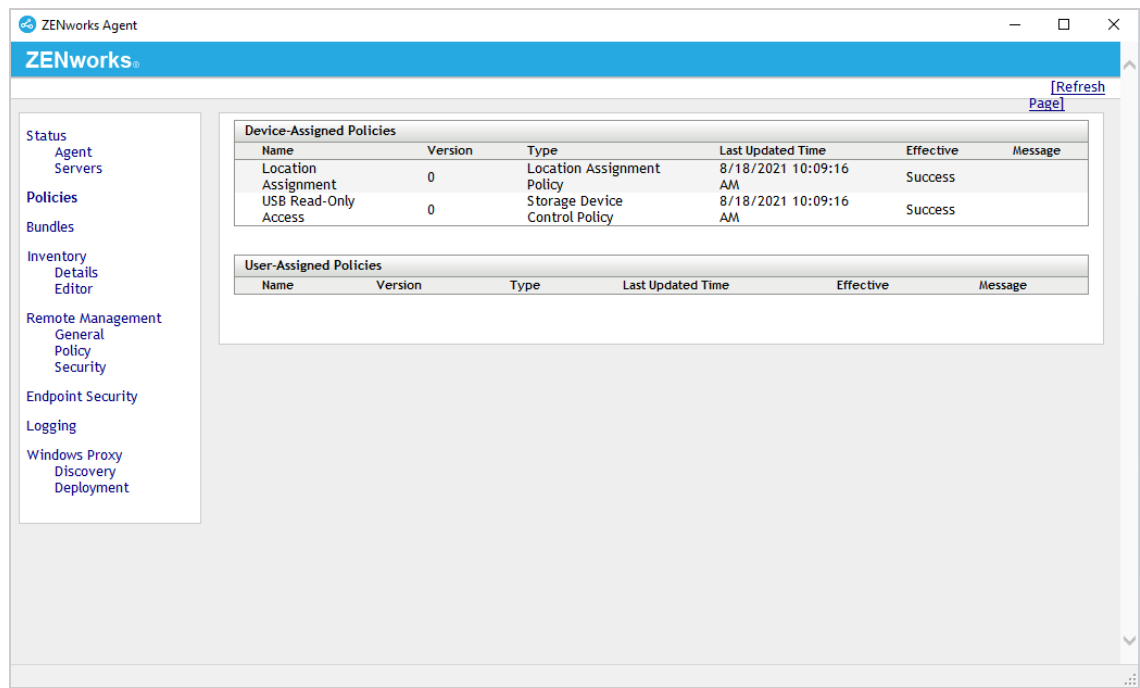
Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

<< Back Next >> Cancel

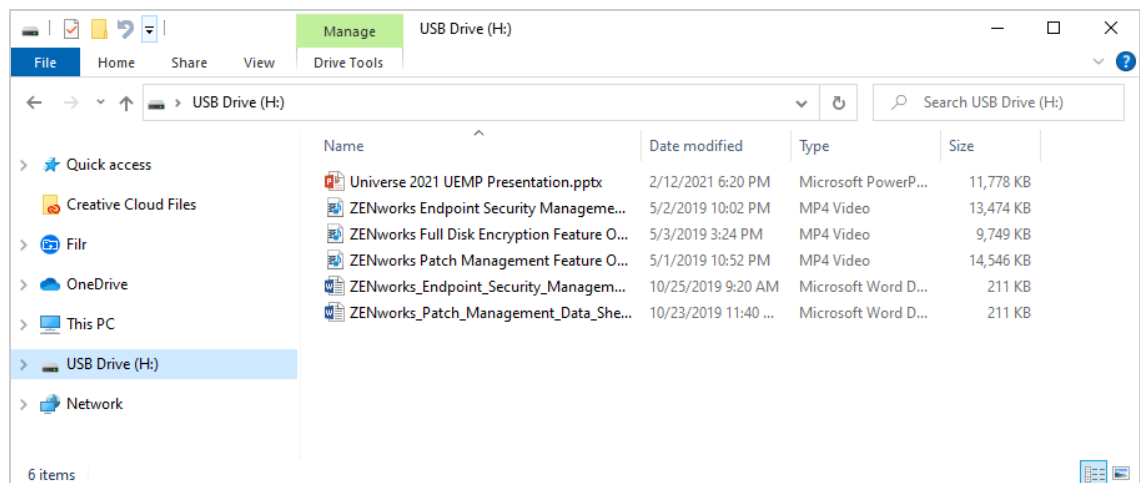
- 2 Complete the wizard:
 - ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
 - ◆ **Step 2: Policies to be Assigned:** Select the USB Read-Only Access policy, then click **OK** to add it to the list.
 - ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
 - ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

Verify the Policy

- 1 On your Windows 10 device, right-click the ZENworks icon , then click **Refresh** to enforce the USB Read-Only Access policy.
- 2 Once the ZENworks icon stops spinning, right-click the icon, then click **Technician Application** to display the ZENworks Agent window.
- 3 Click **Policies** in the left-navigation pane and verify that the USB Read-Only Access policy is assigned and effective.



- 4 Insert a USB drive.
- 5 Open Windows Explorer and click the USB drive to display its contents.



- 6 Open one of the files on the USB drive. The file is successfully read and opened.
- 7 Copy a file to the USB drive. The file copy fails because the drive access is Read Only.

4 Secure Wireless Communication

When it comes to wireless networks, users are oftentimes their own worst enemies. With ZENworks, you can secure wireless communication by restricting access to approved wireless networks only or to wireless networks that support a minimum security level. For times when users need to connect to public networks, you can enforce secure communication through your VPN service.

- ◆ [“Control Wireless Network Access” on page 63](#)
- ◆ [“Enforce a VPN Connection” on page 67](#)

Control Wireless Network Access

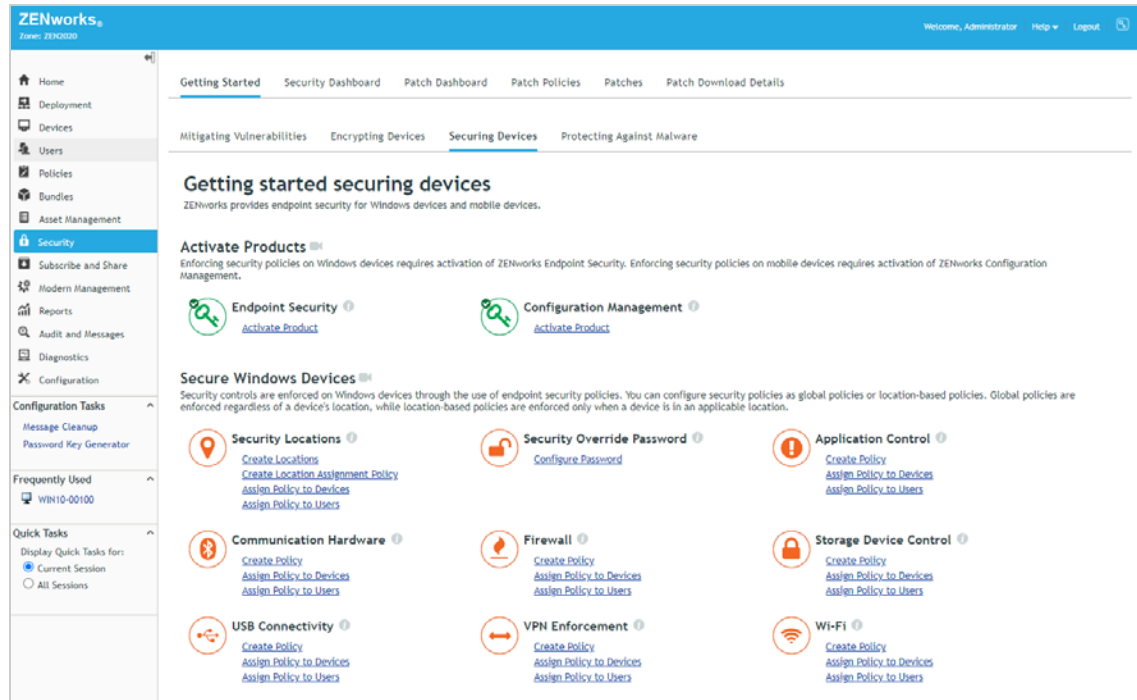
ZENworks Endpoint Security Management lets you blacklist/whitelist specific network access points or establish minimum security requirements for connecting to any wireless network.

We'll have you create a Wi-Fi policy that allows your Windows 10 device to connect only to your organization's private wireless network and hides other detected wireless networks. A policy like this allows you to ensure that users are not connecting to any unauthorized wireless networks while in your work place.

- ◆ [“Create a Wi-Fi Policy” on page 64](#)
- ◆ [“Assign the Policy” on page 65](#)
- ◆ [“Verify the Policy” on page 65](#)

Create a Wi-Fi Policy

- 1 In ZENworks Control Center, go to the Getting Started Securing Devices page.



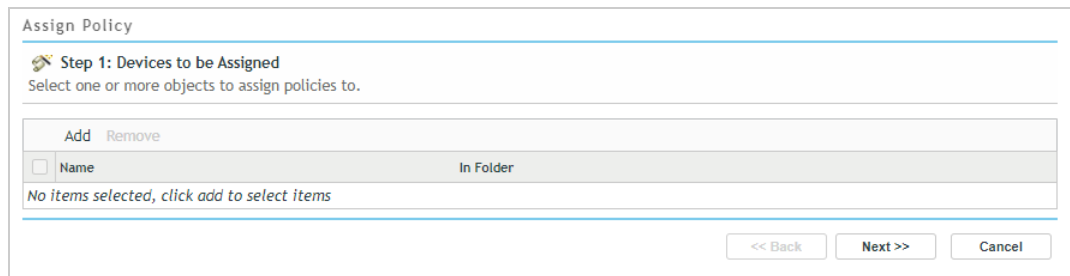
- 2 Under Wi-Fi, click **Create Policy** to launch the Create New Policy wizard.

- 3 Complete the wizard:

- ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
- ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
- ◆ **Step 3: Select Policy Type:** Keep the **Location Assignment Policy** selection.
- ◆ **Step 4: Define Details:** Name the policy **Work-Approved Wireless Networks**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as Work-Approved Wireless Networks throughout the rest of the evaluation.)
- ◆ **Step 5: Configure Inheritance and Location Assignments:** You can enforce the policy globally (in all locations) or in specific locations only. If you've set up security locations, select **Location Based Policy**, click **Add**, then add the Work location. If you haven't set up locations, keep the **Global Policy - available in all locations** selection.
- ◆ **Step 6: Configure Wi-Fi Settings:** In the Minimum Security list, select **WPA2**. In the Access Points list, click **Add > Create New**. Enter **Work Access Points** for the name, enter your organization's wireless network SSID, then click **OK** to add it as an approved wireless network. Ignore the rest of the settings.
- ◆ **Step 7: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policy

- 1 On the Getting Started Securing Devices page in the Wi-Fi section, click **Assign Policy to Devices** to launch the Assign Policy wizard.




The screenshot shows the 'Assign Policy' wizard interface. At the top, it says 'Assign Policy' and 'Step 1: Devices to be Assigned'. Below this, it instructs the user to 'Select one or more objects to assign policies to.' There is a table with columns for 'Name' and 'In Folder'. The table is currently empty, with a message below it stating 'No items selected, click add to select items'. At the bottom right, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

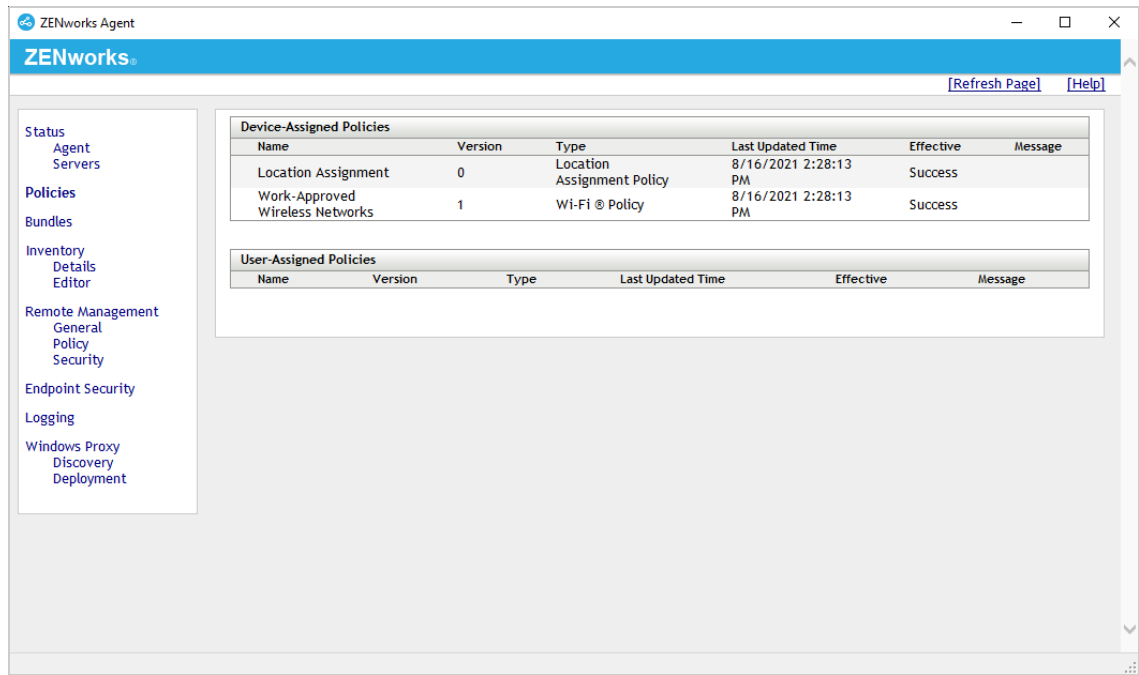
- 2 Complete the wizard:
 - ♦ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
 - ♦ **Step 2: Policies to be Assigned:** Select the Work-Approved Wireless Networks policy, then click **OK** to add it to the list.
 - ♦ **Step 3: Policy Conflict Resolution:** Keep the default selection.
 - ♦ **Step 4: Finish:** Click **Finish** to assign the policy to the device.


Verify the Policy

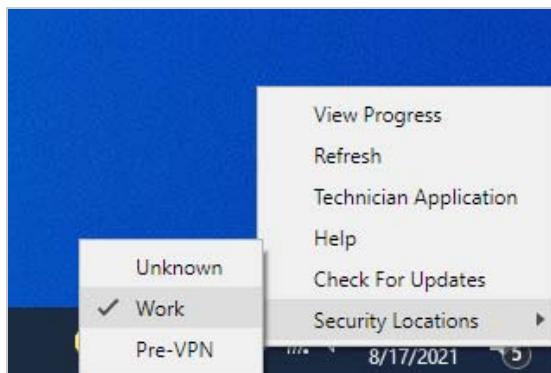
- 1 On your Windows 10 device, click the Wireless Networks icon in the Notification area to view the available wireless networks.



- 2 Right-click the ZENworks icon , then click **Refresh** to enforce the Work-Approved Wireless Network policy.
- 3 After the ZENworks icon stops spinning, right-click the icon, then click Technician Application to display the ZENworks Agent window.
- 4 Click Policies in the left-navigation pane and verify that the Work-Approved Wireless Network policy is assigned and effective.

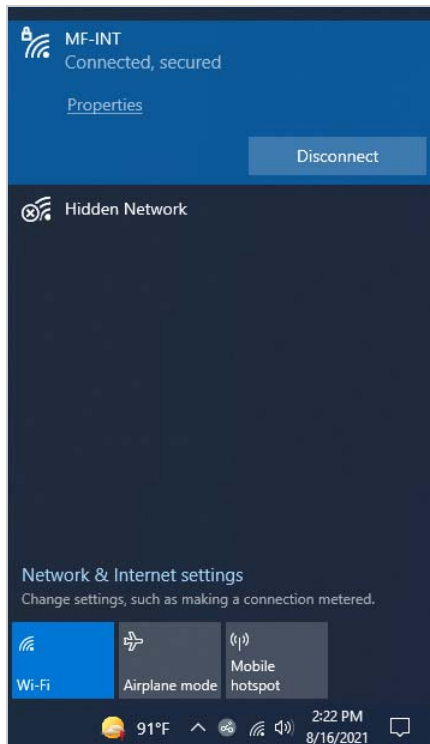


- 5 If you configured the policy to be enforced in the Work location, right-click the ZENworks icon , click **Security Locations**, then click **Work** to manually change the device's location to the Work location if it is not already in that location.



- 6 Click the Wireless Network icon and verify that only your approved wireless network is available.

If you notice a Hidden Network as shown below, the device is finding an access point that is not broadcasting its SSID. You would have to know the SSID to be able to connect to the access point. If you don't want hidden networks displayed, you can use MAC addresses in addition to SSIDs to block them.



Enforce a VPN Connection

Remote users present additional security challenges compared to users who reside on your private network. One of those challenges is ensuring that they have a secure network connection for accessing your private network resources. Equally as important is ensuring that they can work safely while on public networks.

To help with these and similar challenges, ZENworks Endpoint Security Management lets you manage VPN connections for devices based upon their location. For example, when a remote user's device moves into an Unknown location, you could launch a VPN client and require the user to log in before gaining access to the Internet or other network services, which is what we'll have you do in this part of the evaluation.

Before you can enforce a VPN connection, you need to:

- ◆ Make sure you created the Work and Pre-VPN locations covered in [“Set Up Security Locations” on page 26](#). We'll use those two locations and the Unknown location.
- ◆ Make sure your Windows 10 device has a VPN client that can connect through your VPN service to access your private network. This can be a full tunnel or a split tunnel connection.

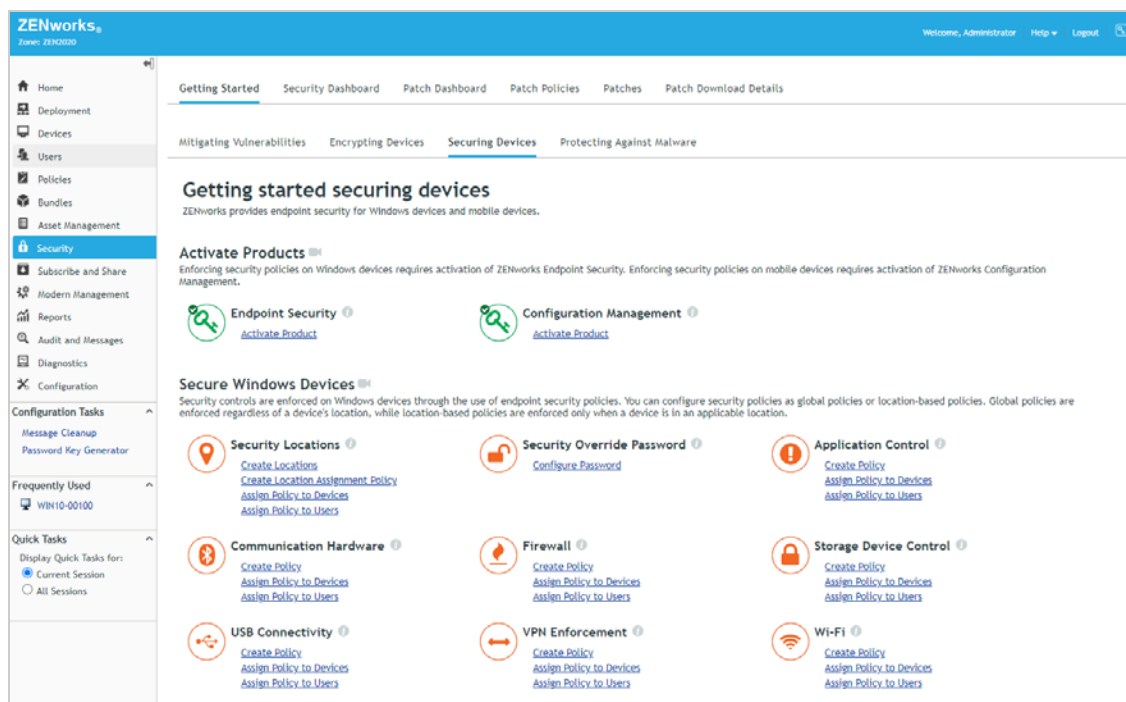
Once you have met the prerequisites above, complete the tasks in the following sections:

- ◆ “Create a VPN Enforcement Policy” on page 68
- ◆ “Create a Firewall Policy” on page 71
- ◆ “Assign the Policies” on page 73
- ◆ “Verify the Policy” on page 74
- ◆ “Unassign the Policies” on page 75

Create a VPN Enforcement Policy

The VPN Enforcement policy lets you identify the Unknown location as the “trigger” location in which you want to enforce a VPN. When the device enters the Unknown location, we’ll launch a VPN client, change the device’s location to the Pre-VPN location, and apply a firewall (which we’ll create next in “Create a Firewall Policy” on page 71) that blocks Internet access until the user logs into the VPN service. Once the user logs into the VPN service, we’ll move the device to the Work location so that the restrictive firewall is removed and the user can access the Internet. It sounds complicated, but it will become clearer as we walk through the policy creation.

- 1 In ZENworks Control Center, go to the Getting Started Securing Devices page.



- 2 Under VPN Enforcement, click **Create Policy** to launch the Create New Policy wizard.

- 3 Complete the wizard:

- ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
- ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
- ◆ **Step 3: Select Policy Type:** Keep the **VPN Enforcement Policy** selection.

- ◆ **Step 4: Define Details:** Name the policy **VPN Enforcement**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as VPN Enforcement throughout the rest of the evaluation.)
- ◆ **Step 5: Select the Policy Level:** Select **Advanced Version**.
- ◆ **Step 6: Select the Trigger Locations:** Configure the settings as follows:
 - ◆ Trigger Locations: Keep **Unknown** as the trigger location.

Trigger Locations	
Add Remove	
Name	
<input type="checkbox"/> Unknown	

1 - 1 of 1 items show 5 items

- ◆ **Internet Detection Method:** Keep the default settings. The VPN Enforcement policy is only applied in the trigger location (Unknown) if the Internet is detected; otherwise, it is not needed. The default settings try to access a set of predefined web pages to determine if Internet is available.

Internet Detection Method

Retrieve web pages

Use the default web pages

Use the web pages included in the list

Web Pages	
New Edit Delete	
URL	Validate

No items available.

- ◆ **Connect Settings:** We'll display a message prompt with a link to the VPN client. Select **Use VPN Message**. Enter **VPN Required** for the message window title and body text such as **You are in a location that requires a VPN connection in order for you to access the Internet. Please launch the VPN client and log in.** Select **Include message hyperlink**, then enter the executable path for the VPN client in the **Link** field and add any required parameters to the **Parameter** field.

Connect Settings

Use Connect Command

Link:

Parameters:

Use VPN Message

Title of Message Window: *

VPN Required

Body: *

You are in a location that requires a VPN connection in order for you to access the Internet. Please launch the VPN client and log in.

Message Hyperlink

Include message hyperlink

Display Text:

Link: *

Parameters:

Fields marked with an asterisk are required.

- ◆ **Step 7: Configure VPN Detection:** These settings let you configure how ZENworks determines that a VPN connection has been successfully established. Select **Enable VPN traffic detection**. In the Network Traffic Address list, add a network address from your private network that the device can detect only when the VPN connection is active. For example, you could use the IP address or DNS hostname of the ZENworks Primary Server if it on your private network.

Network Traffic

Add the network addresses to monitor for VPN activity. Activity is determined by detecting ping replies or packet streams from the addresses.

Network Traffic Addresses	
Type	Value
<input type="checkbox"/> DNS	zendoc2a.provo.novell.com

1 - 1 of 1 items

- ◆ **Step 8: Select a Pre-VPN Location:** Once the device detects it is in the trigger location (Unknown), it can switch to a pre-VPN location to apply policies, such as a restrictive firewall, until the VPN connection is established. Select **Use a Pre-VPN location**, then select the Pre-VPN location you created in [“Create a Pre-VPN Location” on page 29](#).

The Exit Criteria determines when the device changes from the pre-VPN location to the VPN location, which is the location the device will use while the VPN connection is active. Select **Switch from the Pre-VPN location to the VPN location when VPN traffic is detected**.

Use a Pre-VPN location

Pre-VPN Location:

Exit Criteria

Switch from the Pre-VPN location to the VPN location when VPN traffic is detected

Switch from the Pre-VPN location after minutes

Switch to the VPN location

Switch to the Timeout location:

- ◆ **Step 9: Select the VPN Location:** Once the device detects an active VPN connection, it switches to the VPN location to apply the policies you’ve assigned to that location. In our case, we’ll re-use the Work location for the VPN location to make it so that you don’t have to create another location. Select **Work** for the VPN location, the select **Exit the VPN location if no VPN traffic has been detected for 2 minutes**.

VPN Location: *

Exit the VPN location if no VPN traffic has been detected for minutes

Use Disconnect Command

Link: *

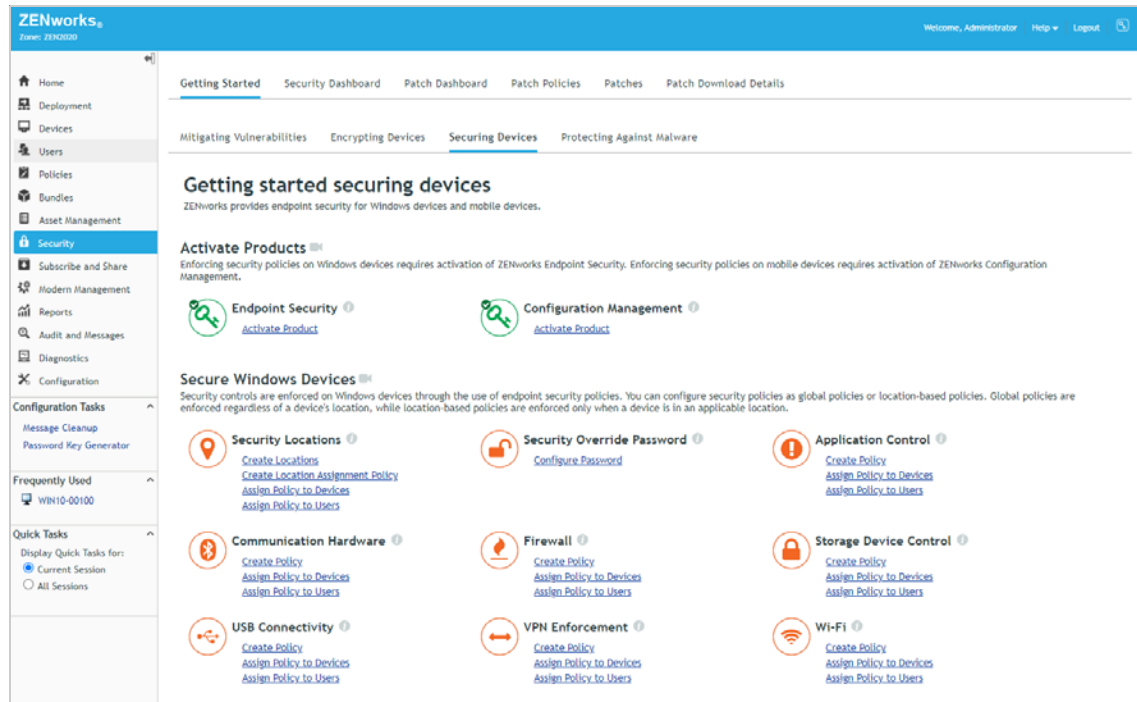
Parameters:

- ◆ **Step 10: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Create a Firewall Policy

We'll create a Firewall policy that restricts network access and assign it to the pre-VPN location. With the restrictive firewall, users will be forced to log in to VPN in order to access the Internet.

- 1 In ZENworks Control Center, go to the Getting Started Securing Devices page.



- 2 Under Firewall, click **Create Policy** to launch the Create New Policy wizard.

- 3 Complete the wizard:

- ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
- ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
- ◆ **Step 3: Select Policy Type:** Keep the **Firewall Policy** selection.
- ◆ **Step 4: Define Details:** Name the policy **VPN Firewall**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as VPN Firewall throughout the rest of the evaluation.)
- ◆ **Step 5: Configure Inheritance and Location Assignments:** You want this firewall enforced when the device enters the Pre-VPN location. Select **Location Based Policy**, click **Add**, then add the Pre-VPN location.
- ◆ **Step 6: Configure Firewall Settings:** Configure the settings as follows:
 - ◆ Default Behavior: Set to **Closed**.
 - ◆ Port/Protocols Rules: Add a DNS rule with Default Behavior set to **Open** for TCP/UDP port 53.

Edit Port/Protocol Rule [X]

Name: *

Description:

Default Behavior:

Port Types			
New Delete			
<input type="checkbox"/>	Port/Protocol Type	Start	End
<input type="checkbox"/>	TCP/UDP	53	53

1 - 1 of 1 items | 1 / 1 | show 10 items

OK Cancel

Fields marked with an asterisk are required.

- ◆ Port/Protocols Rules: Add a DHCP rule with Default Behavior set to **Open** for TCP/UDP ports 67 and 68.

Edit Port/Protocol Rule [X]

Name: *

Description:

Default Behavior:

Port Types			
New Delete			
<input type="checkbox"/>	Port/Protocol Type	Start	End
<input type="checkbox"/>	TCP/UDP	67	68

1 - 1 of 1 items | 1 / 1 | show 10 items

OK Cancel

Fields marked with an asterisk are required.

- ◆ Standard Access Control Lists: Set Ethernet Multicast, ICMP, IP Multicast, and IP Subnet Broadcast to **Inherit**. Leave 802.1x, ARP, Logical Link Layer Control, SNAP, and ZENworks Server set to **Allow**.

Standard Access Control Lists

802.1x:	<input type="text" value="Allow"/>	IP Subnet Broadcast:	<input type="text" value="Inherit"/>
ARP:	<input type="text" value="Allow"/>	Logical Link Layer Control (LLC):	<input type="text" value="Allow"/>
Ethernet Multicast:	<input type="text" value="Inherit"/>	SNAP:	<input type="text" value="Allow"/>
ICMP:	<input type="text" value="Inherit"/>	ZENworks Server:	<input type="text" value="Allow"/>
IP Multicast:	<input type="text" value="Inherit"/>		

- ◆ Access Control Lists: Add your VPN server as a trusted ACL. This allows a device's VPN client to establish a connection to the VPN server.

Edit Access Control List

Name: *

Description:

ACL Behavior:

Configure optional ports

Port Rule: *

Address Types	
New Edit Delete	
<input type="checkbox"/> Type	Value
<input type="checkbox"/> IP Address or DNS Name	ams-remoteaccess.microfocus.net

1 - 1 of 1 items show 10 items

Fields marked with an asterisk are required.

- ◆ **Step 7: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policies

- 1 In the VPN Enforcement Policy section of the Getting Started Securing Devices page, click **Assign Policy to Devices** to launch the Assign Policy wizard.

Assign Policy

Step 1: Devices to be Assigned
Select one or more objects to assign policies to.


Add Remove

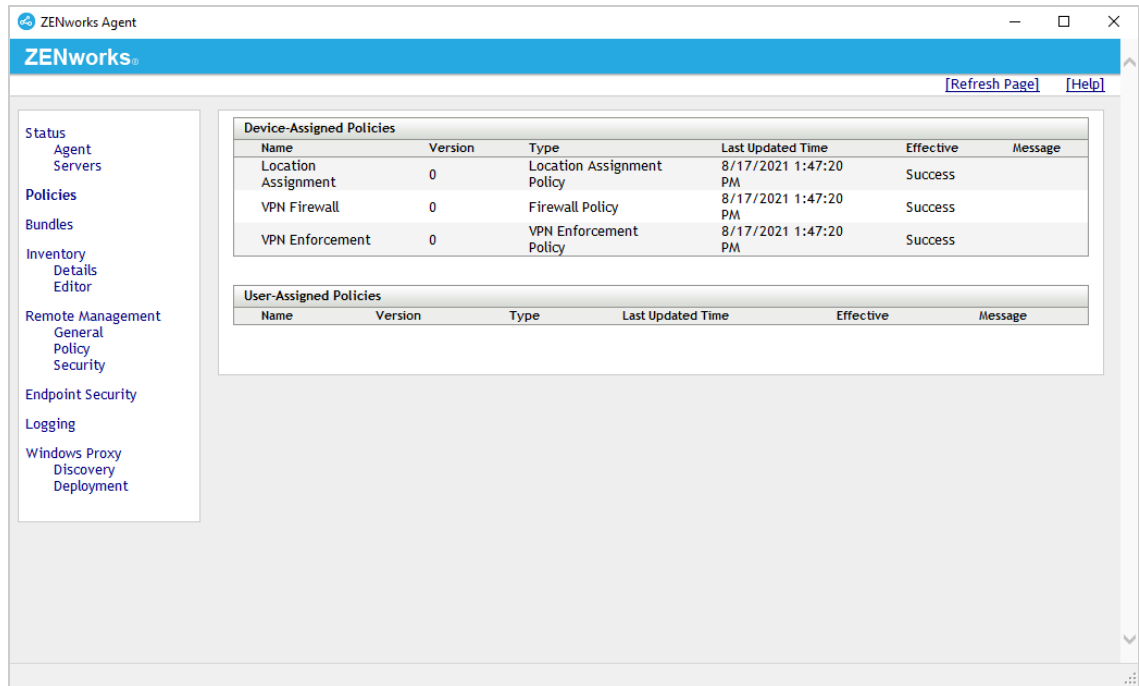
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

- 2 Complete the wizard:

- ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
- ◆ **Step 2: Policies to be Assigned:** Select the VPN Enforcement policy and the VPN Firewall Policy, then click **OK** to add them to the list.
- ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
- ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

Verify the Policy

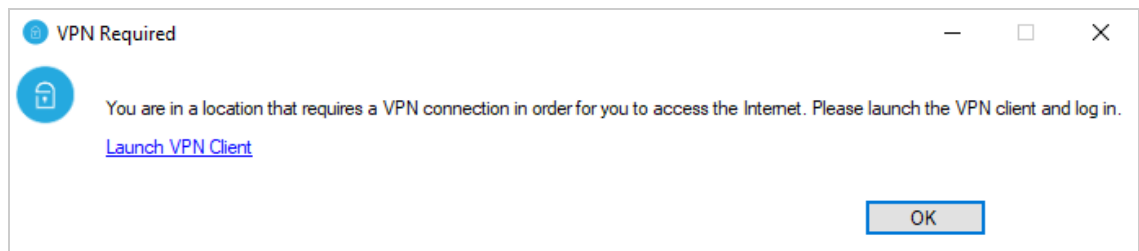
- 1 On your Windows 10 device while connected to your private network, right-click the ZENworks icon , then click **Refresh** to enforce the VPN Enforcement and VPN Firewall policies.
- 2 After the ZENworks icon stops spinning, right-click the icon, then click Technician Application to display the ZENworks Agent window.
- 3 Click Policies in the left-navigation pane and verify that the two policies are assigned and effective.



- 4 Disconnect from your private network and connect to another network (for example, a public network, your home network, or a hotspotted mobile phone).

Unlike when testing the other policies during this evaluation, we can't just manually switch to the Unknown location to initiate the VPN Enforcement policy. Well, we could, but the policy wouldn't work correctly because we configured it to detect a VPN connection using one of your private network addresses. We don't want the address detected until you establish the VPN connection, so you need to connect to a network other than your private network.

When you connect to the other network, the device switches to the Unknown location which triggers the VPN Enforcement policy. This causes the device to display the VPN prompt.



At the same time, the device switches to the Pre-VPN location and enforces the VPN Firewall assigned to the Pre-VPN location.

5 Before launching the VPN client, open a Web browser and try to open a website. You can't because Internet access is blocked.

6 Click **Launch VPN Client** to open the VPN client and log in.

After the VPN connection is established, the device is able to reach the private network address you defined to determine an active VPN connection. This causes the device to switch to the Work location and removes the VPN Firewall policy.

7 After the device has switched to the Work location, access a web site. This time you can because the firewall is no longer restricting access.

8 Disconnect from the VPN. The device switches back to the Unknown location which triggers the VPN Enforcement policy again. This will continue to occur as long as the device is in an Unknown location.

We've shown you one way to configure the policy to enforce a VPN connection. However, because of the policy's flexible options, you can configure a VPN Enforcement policy that best suites your organization's environment and your users needs.

Unassign the Policies

Before moving on to other security policies, you might want to remove the VPN Enforcement and VPN Firewall policy assignments from the device. Otherwise, every time the device switches to the Unknown location you'll have to use the VPN connection to gain network access.

To remove the policy assignment:

- 1 In ZENworks Control Center, click **Devices** to display the Devices list, click **Workstations** to open the Workstations folder, then click the device to open it.
- 2 Click the **Assignments** tab.
- 3 In the Assigned Policies section, select the check boxes for the VPN Firewall and VPN Enforcement policies, then click **Remove**.

5 Block Applications

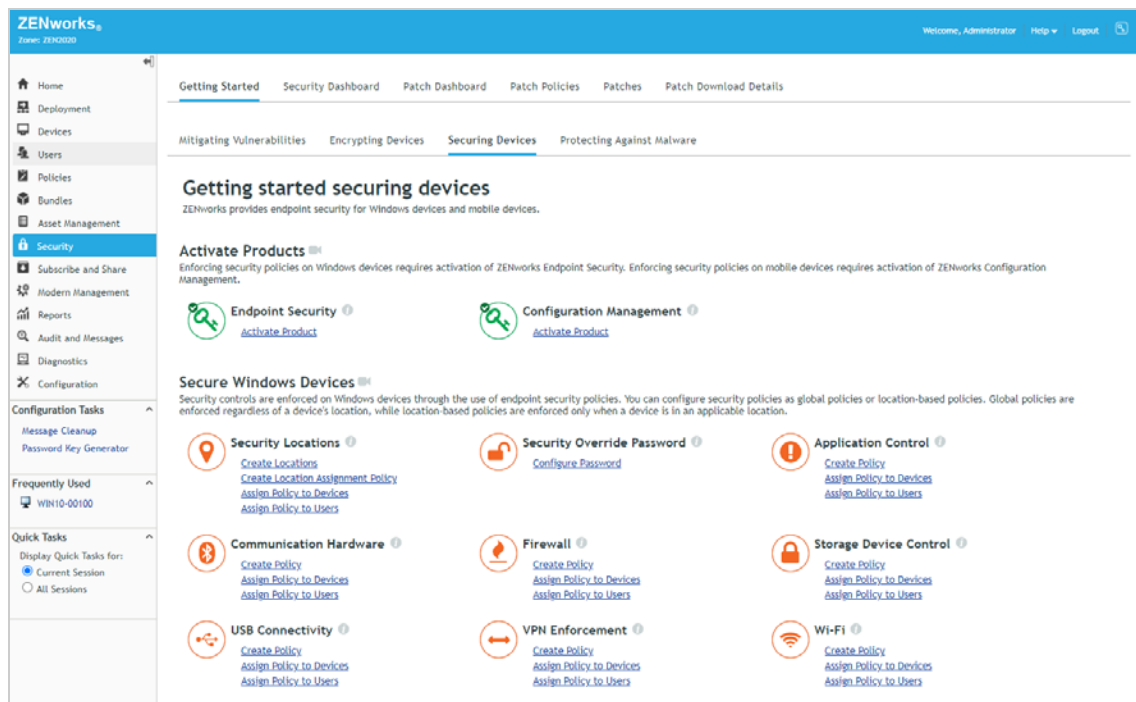
You can prevent specific unauthorized or undesirable applications from running on Windows devices. In this evaluation, we'll block Google Chrome and Mozilla Firefox and inform the user to run Microsoft Edge instead.

If you don't have Chrome or Firefox installed on your Windows 10 device and don't want to install one of them, you can substitute another application (such as Calculator) to block instead.

- ◆ “Create an Application Control Policy” on page 77
- ◆ “Assign the Policy” on page 78
- ◆ “Verify the Policy” on page 79

Create an Application Control Policy

- 1 In ZENworks Control Center, go to the Getting Started Securing Devices page.



- 2 Under Application Control, click **Create Policy** to launch the Create New Policy wizard.

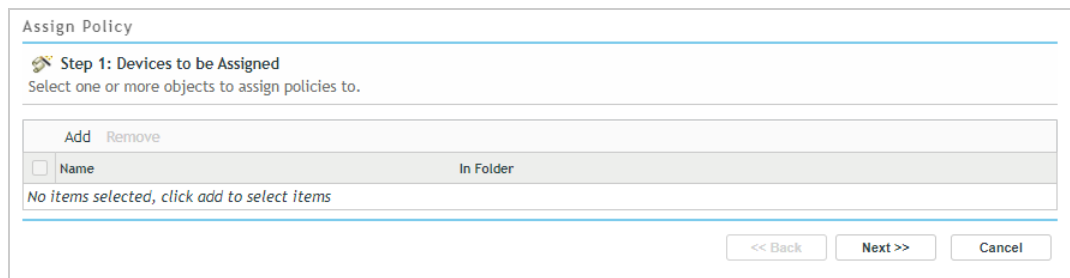
- 3 Complete the wizard:

- ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
- ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
- ◆ **Step 3: Select Policy Type:** Keep the **Application Control Policy** selection.

- ♦ **Step 4: Define Details:** Name the policy **Application Control**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as Application Control throughout the rest of the evaluation.)
- ♦ **Step 5: Configure Inheritance and Location Assignments:** You can enforce the policy globally (in all locations) or in specific locations only. For this evaluation, we'll enforce it globally, so keep the **Global Policy - available in all locations** selection.
- ♦ **Step 6: Configure Application Control Settings:** Define Chrome and Firefox and block their execution:
 1. In the Application Control List, click **Add > Create New**.
 2. In the Name field, enter `Block Unauthorized Browsers`.
 3. For the Default Behavior, select **No Execution**.
 4. In the Applications list, click **New**, enter `chrome.exe` in the Name field, then click **OK**. Do not specify a path; `chrome.exe` will be blocked regardless of its location on the device.
 5. Repeat step 4 to add Mozilla Firefox (`firefox.exe`) to the Applications list. If you don't have Chrome or Firefox on your managed Windows 10 device, substitute another application such as `calculator.exe`.
 6. Click **OK** to add the Application Control to the list.
 7. In the Enforcement Behavior on Running Processes section:
 - a. Select **Enforce after 5 minutes**.
 - b. Enable the **Display message when enforcing behavior** option.
 - c. In the Title of Message Windows field, enter `Unauthorized Web Browser`.
 - d. In the Body field, enter `The web browser you are using is not authorized for use on this computer. Please use Microsoft Edge for your Web browser.`
 - e. Enable the **Include message hyperlink** option.
 - f. In the Display Text field, enter `Launch Microsoft Edge`.
 - g. In the Link field, enter `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.
 - h. Click **Next**.
- ♦ **Step 7: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policy


- 1 In the Application Control section of the Getting Started Securing Devices page, click **Assign Policy to Devices** to launch the Assign Policy wizard.

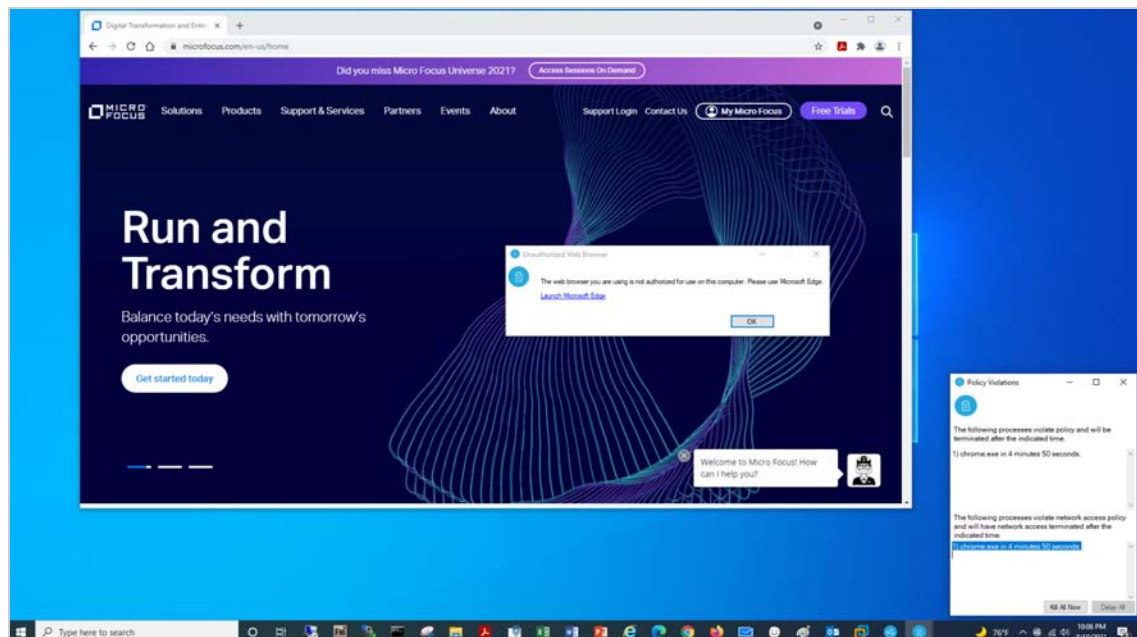


2 Complete the wizard:

- ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
- ◆ **Step 2: Policies to be Assigned:** Select the Application Control policy, then click **OK** to add it to the list.
- ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
- ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

Verify the Policy

- 1 On your Windows 10 device, open Chrome and/or Firefox. Or, if you substituted another application in the policy, open that application.
- 2 Right-click the ZENworks icon , then click **Refresh** to enforce the Application Control policy. The “Unauthorized Web Browser” message dialog is displayed and the countdown pops up in the Notification area.



- 3 Wait for 5 minutes to force close the application.

or

Click **Kill All Now** to immediately close the application.

- 4 Try launching the application again. It will not start.

6 Control Device Hardware

ZENworks Endpoint Security Management lets you control communication hardware and USB device connectivity. For example, you can enable/disable access to Bluetooth, serial/parallel ports, and wired and wireless network adapters. Likewise, you can determine the USB devices (mass storage devices, HID-compliant peripherals, scanners, printers) that can connect.

- ♦ [“Control Communication Hardware” on page 81](#)
- ♦ [“Control USB Device Connectivity” on page 85](#)

Control Communication Hardware

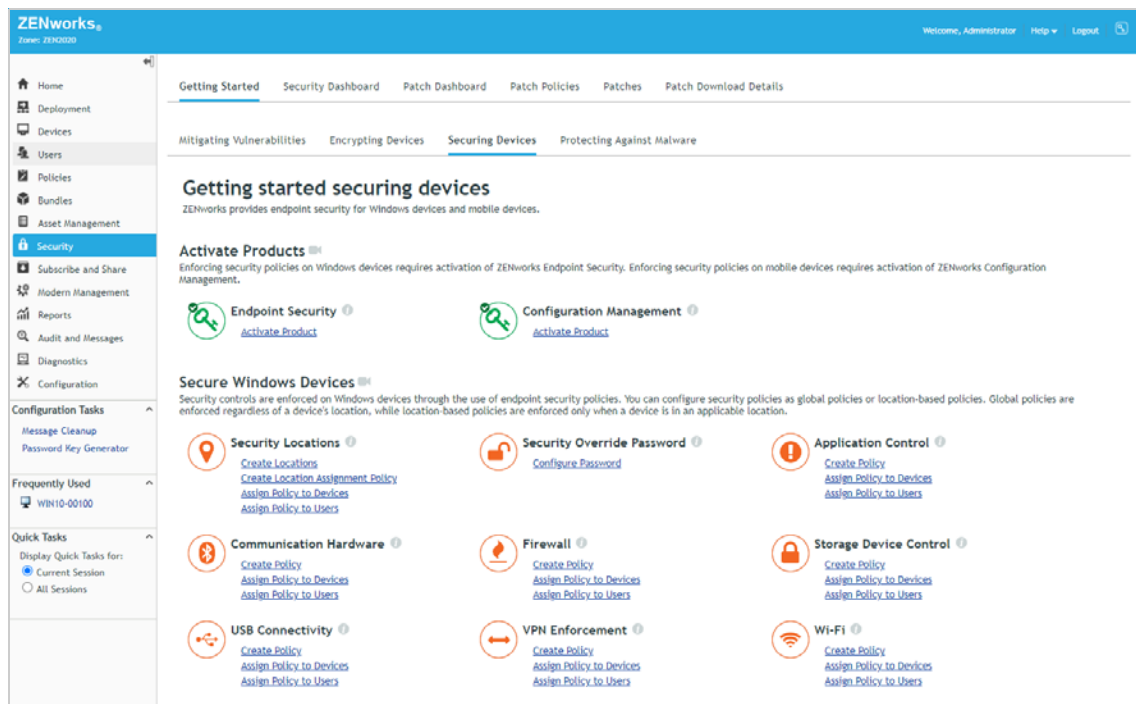
You can control the types of communication hardware available to users. For example, you might feel that Bluetooth connections in some environments pose risks that outweigh the benefits (remember BlueBorne?). Or, maybe you want to disable wireless connections when a wired connection is available. Or, maybe you don't want users using 1394 (FireWire) connections because of the security risks. The Communication Hardware policy lets you do each of these things and more.

We'll have you create a policy that disables Bluetooth on your Windows 10 device. If you've previously defined security locations (see [“Set Up Security Locations” on page 26](#)), we'll configure the policy to disable Bluetooth in the Unknown location only. If you haven't set up locations, we'll have you disable Bluetooth in all locations.

- ♦ [“Create a Communication Hardware Policy” on page 81](#)
- ♦ [“Assign the Policy” on page 82](#)
- ♦ [“Verify the Policy” on page 83](#)

Create a Communication Hardware Policy

- 1 In ZENworks Control Center, go to the Getting Started Securing Devices page.



2 Under Communication Hardware, click **Create Policy** to launch the Create New Policy wizard.

3 Complete the wizard:

- ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
- ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
- ◆ **Step 3: Select Policy Type:** Keep the **Communication Hardware Policy** selection.
- ◆ **Step 4: Define Details:** Name the policy **Disable Bluetooth**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as Disable Bluetooth throughout the rest of the evaluation.)
- ◆ **Step 5: Configure Inheritance and Location Assignments:** You can enforce the policy globally (in all locations) or in specific locations only. If you've set up security locations, select **Location Based Policy**, click **Add**, then add the Unknown location. If you haven't set up locations, keep the **Global Policy - available in all locations** selection.
- ◆ **Step 6: Configure Communication Hardware Settings:** In the Bluetooth list, select **Disable**.
- ◆ **Step 7: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policy

1 In the Communication Hardware section of the Getting Started Securing Devices page, click **Assign Policy to Devices** to launch the Assign Policy wizard.

Assign Policy

Step 1: Devices to be Assigned
Select one or more objects to assign policies to.

Add Remove	
<input type="checkbox"/>	In Folder
No items selected, click add to select items	

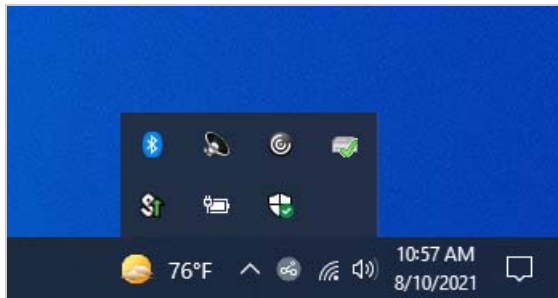
<< Back Next >> Cancel


2 Complete the wizard:

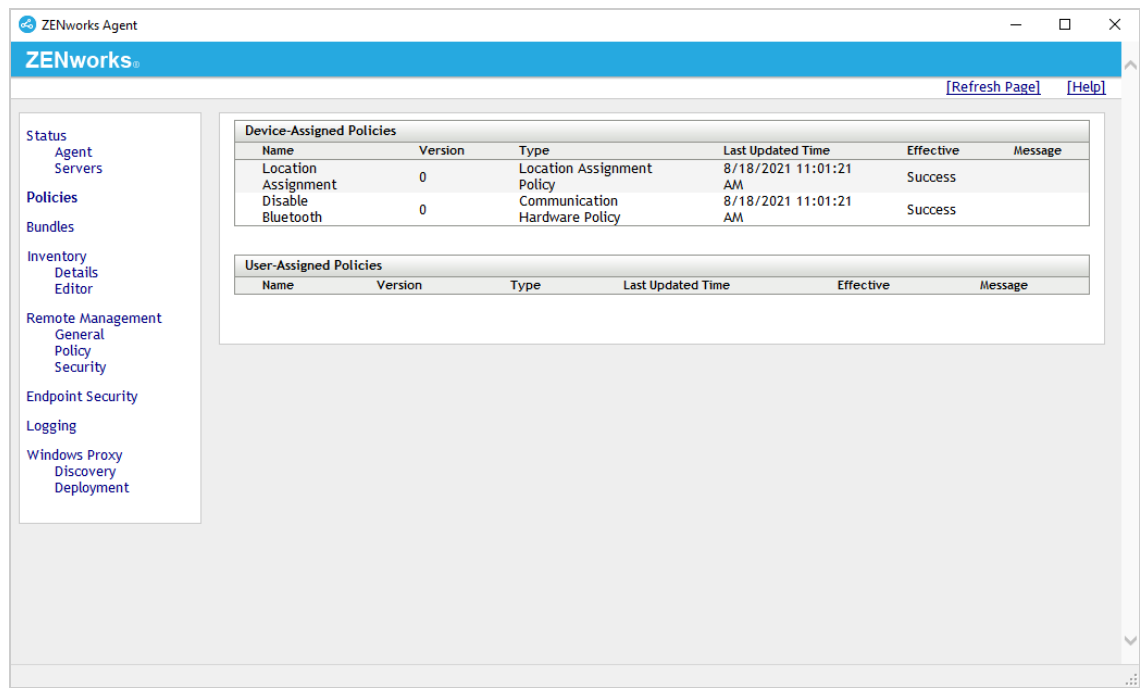
- ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
- ◆ **Step 2: Policies to be Assigned:** Select the Disable Bluetooth policy, then click **OK** to add it to the list.
- ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
- ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

Verify the Policy

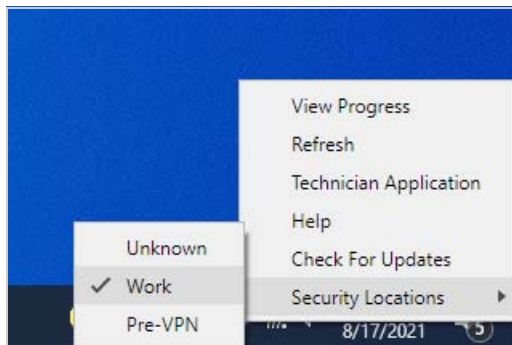
- 1 On your Windows 10 device, check the Notification area to verify that Bluetooth is enabled.



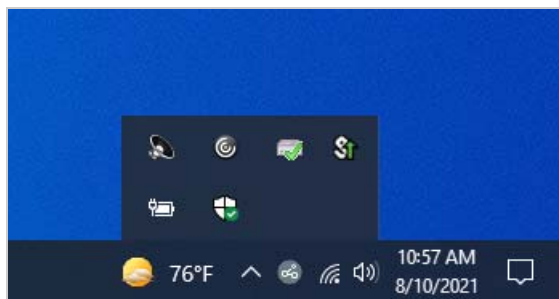
- 2 Right-click the ZENworks icon , then click **Refresh** to enforce the Disable Bluetooth policy.
- 3 Once the ZENworks icon stops spinning, right-click the icon, then click Technician Application to display the ZENworks Agent window.
- 4 Click Policies in the left-navigation pane and verify that the Disable Bluetooth policy is assigned and effective.



- If you configured the policy to be enforced in the Unknown location, right-click the ZENworks icon , click **Security Locations**, then click **Unknown** to manually change the device's location to the Unknown location.



- Verify that Bluetooth is disabled.
The Bluetooth icon is no longer displayed in the Notification area:



Control USB Device Connectivity

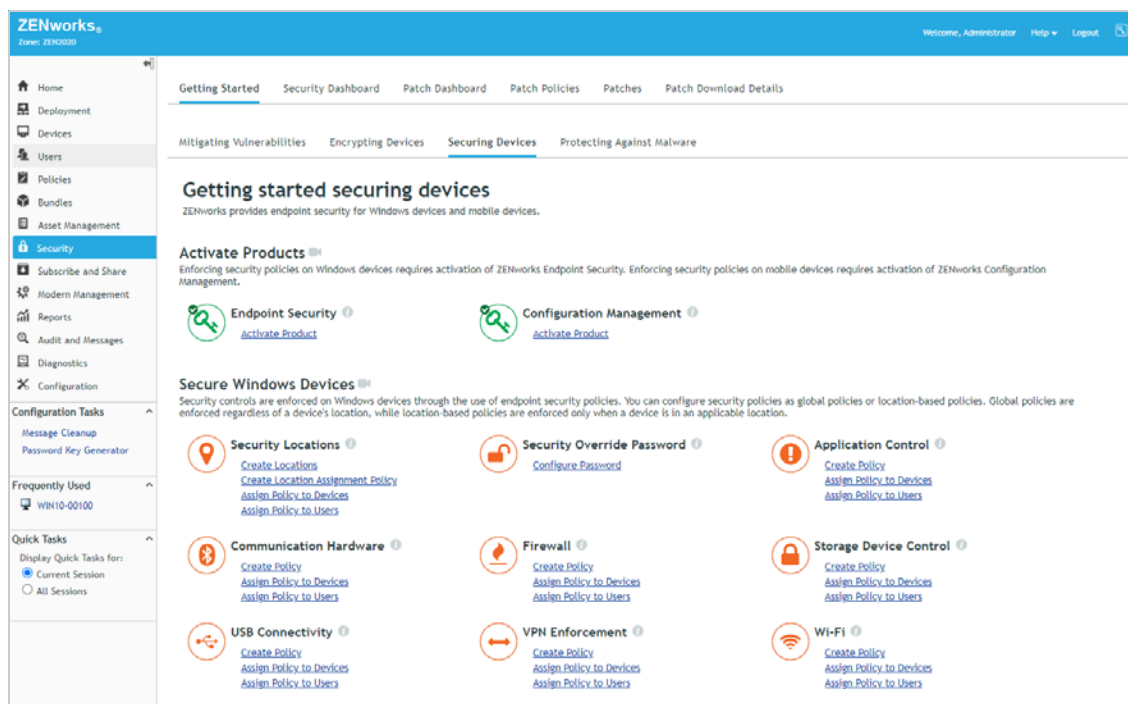
USB ports are one of the primary methods of connecting hardware devices such as removable data drives, scanners, printers, mice, and keyboards.

With the USB Connectivity policy, you can control which USB devices are connected, including disabling all USB device connectivity completely. Since we don't know exactly what USB devices you have available on your Windows 10 device, we'll stick with creating a policy to disable all USB storage drives (Mass Storage Class) and have you test it with a USB drive. This way we won't end up disabling your mouse, keyboard, or some other USB device needed to use the computer.

- ◆ “Create a USB Connectivity Policy” on page 85
- ◆ “Assign the Policy” on page 86
- ◆ “Verify the Policy” on page 86

Create a USB Connectivity Policy

- 1 In ZENworks Control Center, go to the Getting Started Securing Devices page.



- 2 In the USB Connectivity section, click **Create Policy** to launch the Create New Policy wizard.
- 3 Complete the wizard:
 - ◆ **Step 1: Select Platform:** Keep the **Windows** selection.
 - ◆ **Step 2: Select Policy Category:** Keep the **Windows Endpoint Security Policies** selection.
 - ◆ **Step 3: Select Policy Type:** Keep the **USB Connectivity Policy** selection.
 - ◆ **Step 4: Define Details:** Name the policy **Disable USB Storage Devices**. (Note: You can name the policy whatever you want, but for clarity we'll refer to this policy as Disable USB Storage Devices throughout the rest of the evaluation.)

- ◆ **Step 5: Configure Inheritance and Location Assignments:** You can enforce the policy globally (in all locations) or in specific locations only. For this evaluation, we'll enforce it globally, so keep the **Global Policy - available in all locations** selection.
- ◆ **Step 6: Configure SUSB Connectivity Settings:** By default, connectivity is enabled for all devices. To disable all USB storage devices, locate the Mass Storage Class list and select **Disable**. This disables all USB devices that enumerate to the operating system as Mass Storage including external hard drives, external optical drives, portable flash memory devices, digital cameras, mobile devices, and more. The USB Device Access Settings list lets you define USB devices and assign different access to them. For example, if you had specific USB storage devices you wanted to use, you could define them in the list and enable them; the individual device setting would then override the Device Group setting. We'll let you explore that capability on your own later.
- ◆ **Step 7: Summary:** Deselect **Create as Sandbox** so that the policy is published and available to use, then click **Finish** to create the policy.

Assign the Policy

- 1 In the USB Connectivity section of the Getting Started Securing Devices page, click **Assign Policy to Devices** to launch the Assign Policy wizard.

Assign Policy

🔍 Step 1: Devices to be Assigned
Select one or more objects to assign policies to.


Add Remove

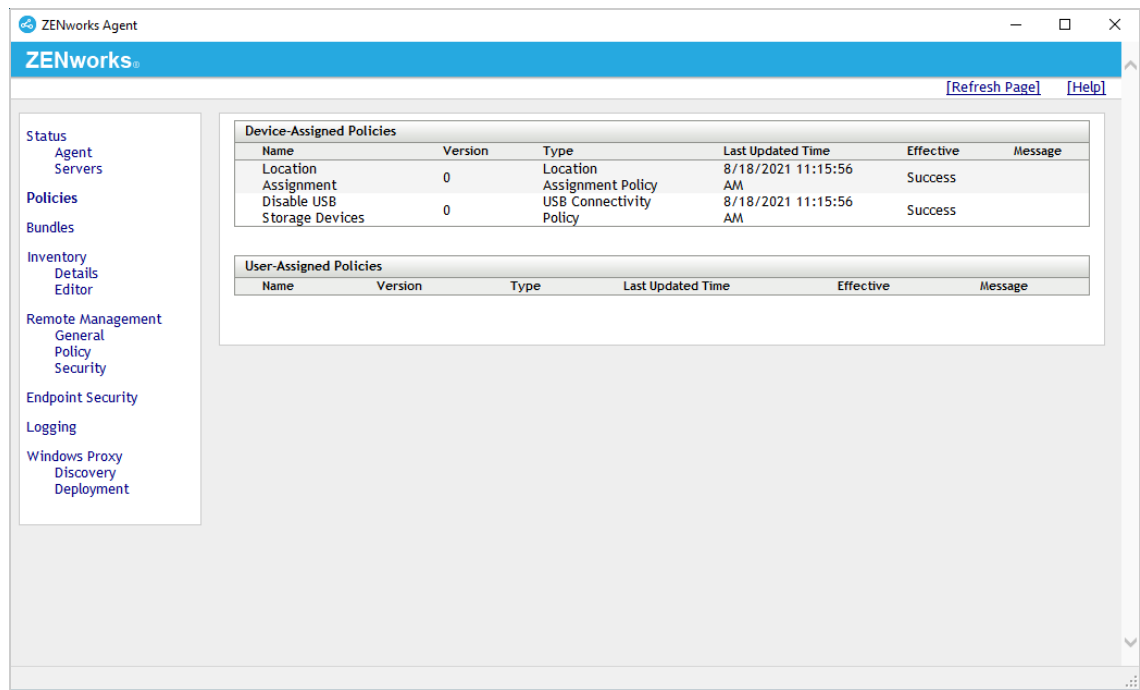
<input type="checkbox"/>	Name	In Folder
No items selected, click add to select items		

<< Back Next >> Cancel

- 2 Complete the wizard:
 - ◆ **Step 1: Devices to be Assigned:** Click **Add**, browse to the Workstations folder and select your Windows 10 device, then click **OK** to add it to the list.
 - ◆ **Step 2: Policies to be Assigned:** Select the Disable USB Storage Devices policy, then click **OK** to add it to the list.
 - ◆ **Step 3: Policy Conflict Resolution:** Keep the default selection.
 - ◆ **Step 4: Finish:** Click **Finish** to assign the policy to the device.

Verify the Policy

- 1 On your Windows 10 device, right-click the ZENworks icon , then click **Refresh** to enforce the Disable USB Storage Devices policy.
- 2 Once the ZENworks icon stops spinning, right-click the icon, then click **Technician Application** to display the ZENworks Agent window.
- 3 Click **Policies** in the left-navigation pane and verify that the Disable USB Storage Devices policy is assigned and effective.



- 4 Insert a USB drive.
- 5 Open Windows Explorer. You'll see that the USB drive is not listed because it has been blocked.

