

opentext™

ZENworks 23.3 Security

August 2023

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/en-us/legal>).

© Copyright 2008 - 2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Reference	5
1 Getting Started	7
2 Mitigating Vulnerabilities	9
Getting Started Mitigating Vulnerabilities	9
More Information	9
3 Encrypting Devices	11
Getting Started Encrypting Devices	11
More Information	11
4 Securing Devices	13
Getting Started Securing Devices	13
More Information	13
5 Protecting Against Malware	15
Getting Started Protecting Against Malware	15
More Information	15

About This Reference

This *ZENworks Security* reference provides an overview of how to get started with enabling and employing all the security capabilities of the ZENworks Suite, which includes security features from ZENworks Patch Management, Full Disk Encryption, Endpoint Security, Mobile Management, and Configuration Management.

Audience

This guide is intended for ZENworks administrators.

Feedback

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

Additional Documentation

ZENworks Security is supported by other documentation for the ZENworks products mentioned above (in both PDF and HTML formats) that you can use to learn about and implement security features. For additional documentation, see the [ZENworks Documentation website](#).

1 Getting Started

ZENworks Security provides a four-tiered approach to protect the managed devices in your enterprise by mitigating software vulnerabilities, encrypting device drives, securing device features, and protecting devices against malware. By accessing Security in ZENworks Control Center, you have first level navigation access to take action on a variety of security related functions directly from the Getting Started pages. For more information about the capabilities launched from these pages, continue reading:

- ♦ **Mitigating Vulnerabilities.** ZENworks helps you stay in front of emerging threats by tracking software vulnerabilities for devices through the use of Common Vulnerabilities and Exposures (CVE) data and then responding to those vulnerabilities by applying the appropriate patches. This enables you to establish regularly scheduled maintenance patching to ensure that your devices have the most recent security and quality updates.

For information on how to get started with mitigating vulnerabilities using ZENworks, see [Mitigating Vulnerabilities](#).

- ♦ **Encrypting Devices.** Manage encryption of fixed disk volumes, fixed disk folders, and removable drives on devices in your environment by activating Full Disk Encryption and Endpoint Security and creating, configuring, and applying encryption-based policies.

For information on how to get started with encrypting your manage devices, see [Encrypting Devices](#).

- ♦ **Securing Devices.** Secure Windows and mobile devices by creating, configuring, and applying policies to manage application, storage, communication hardware, and mobile device security in your environment.

For information on how to get started with securing your manage devices, see [Securing Devices](#).

- ♦ **Protecting Against Malware.** Protect your managed devices and servers from malware threats by configuring the ZENworks Endpoint Security Antimalware capability, and then by creating, customizing, and deploying Antimalware policies to these devices.

For information on how to get started with ZENworks Antimalware, see [Protecting Against Malware](#).

2 Mitigating Vulnerabilities

In today's rapidly increasing reliance on software upgrades and security for managed devices, ZENworks can ensure that Windows and Linux devices in your enterprise stay protected with the latest security patches, software updates, and service packs that are critical to mitigate vulnerabilities and maintain a secure environment.

This is done with an automated patch policy process that draws on the world's largest repository of automated patches, including patches for all major operating systems and various third-party applications to detect patch vulnerabilities and deploy them to managed devices. You can also customize patch deployment and rapidly remediate vulnerabilities manually to pro-actively manage threats.

A key ZENworks feature for maintaining security and awareness of patch vulnerabilities is a robust monitoring system of dashlets and reports to maintain security compliance on all of your managed devices. This includes interactive features in the dashlets that enable you to go directly to devices or patches or to take action to deploy patch remediations, assign devices to a patch policy or group, or generate an immediate vulnerability scan on devices.

Getting Started Mitigating Vulnerabilities

When you access Security in the ZENworks navigation menu, Mitigating Vulnerabilities is one of three Getting Started pages for Security. This page is designed to be a single point of entry to activate, configure, and begin protecting your devices using the capabilities of the ZENworks Patch Management security features. You can create a CVE subscription to import CVE data from the NVD repository and configure the Patch Service to import the patch data from the Patch content repository. After ZENworks maps the CVE and patch data, you can identify the vulnerable devices through a patch scan and then remediate these devices by deploying remediation bundles or assigning patch policies. You can also directly access and create security dashlets from this page to monitor the vulnerability status of your zone and to take actions to further mitigate vulnerabilities.

More Information

For detailed information about the Security capabilities related to mitigating vulnerabilities in your zone, reference the following document:

- ♦ [ZENworks CVE Reference](#)
- ♦ [ZENworks Patch Management Reference](#)

3 Encrypting Devices


ZENworks has three distinct encryption capabilities: (1) encrypting fixed disk volumes, (2) encrypting removable data drives, and (3) encrypting fixed disk folders.

- ◆ Encrypting fixed disk volumes is enabled by configuring and deploying the **Disk Encryption Policy** to devices after activating Full Disk Encryption.
- ◆ Encrypting removable data drives and fixed disk folders is enabled by configuring and deploying the **Microsoft Data Encryption Policy** to devices after activating Endpoint Security.

The Microsoft Data Encryption Policy manages the encrypting capabilities of Microsoft BitLocker and Encrypting File System (EFS) to encrypt removable data drives and fixed disk folders, respectively. You can enable either feature independently in the policy or enable them both in the policy.

Getting Started Encrypting Devices

When you navigate in the ZENworks Control Center to **Security > Getting Started > Encrypting Devices**, you access a page that is designed to simplify the process of implementing the encryption features of ZENworks Security.

From this page you can access several quick links to activate Full Disk Encryption and Endpoint Security, create and assign the policies that manage encryption capabilities, and enable audit events for fixed disk encryption processes. You can also access how-to videos  that walk you through these actions.

More Information

For more detailed information about the capabilities and employment of the Disk Encryption and Microsoft Data Encryption policies, reference the following documents:

- ◆ [ZENworks Full Disk Encryption Policy Reference](#)
- ◆ [ZENworks Endpoint Security Policies Reference](#)


4 Securing Devices

ZENworks secures Windows and mobile devices by creating and assigning security policies to those devices via the ZENworks Control Center. These security policies include the following:

Security Policies for Windows Devices	Security Polices for Mobile Devices
Location Assignment	Mobile Security
Application Control	Mobile Device Control
Communication Hardware	Mobile Compliance
Firewall	
Storage Device Control	
USB Connectivity	
VPN Enforcement	
Wi-Fi	

Getting Started Securing Devices

When you navigate in the ZENworks Control Center to **Security > Getting Started > Securing Devices**, you access a page that is designed to simplify the process of creating and deploying security policies for Windows and mobile devices.

From this page you can access several quick links to activate Endpoint Security, update Endpoint Security and Configuration Management licenses, set the Security Override Password, create security locations, and create and assign security policies that protect Windows and mobile devices. You can also access how-to videos  that walk you through these actions.

More Information

For more detailed information about the capabilities and employment of Endpoint Security and Mobile Management policies, reference the following documents:

- ♦ [ZENworks Endpoint Security Policies Reference](#)
- ♦ [ZENworks Mobile Management Reference](#)


5 Protecting Against Malware

ZENworks protects Windows 10 devices and Windows 2012 and newer servers by creating and assigning Antimalware policies to those devices via the ZENworks Control Center. These Antimalware policies include the following:

- ♦ **Antimalware Enforcement Policy:** This policy is required for all devices that you want to protect from malware threats by implementing on-access and ondemand scans. It installs the Antimalware Agent on assigned devices. Once applied, you can also assign any combination of the other three optional policies to the same devices.
- ♦ **Antimalware Custom Scan Policy:** This policy is designed to customize ondemand scans of local files to target specific malware threats. You can define a schedule for scans or use a quick task to run a scan.
- ♦ **Antimalware Network Scan Policy:** This policy is designed to scan files on network drives only. One example for using this policy would be to scan a file storage disk in an array of disks. You can define a schedule for scans or use a quick task to run a scan.
- ♦ **Antimalware Scan Exclusions Policy:** This policy is designed to exclude specific files from malware scans implemented from the other three policies. You can define file exclusions by specific files or folders, file types (extensions), or specific processes.

Getting Started Protecting Against Malware

When you navigate in the ZENworks Control Center to **Security > Getting Started > Protecting Against Malware**, you access a page that is designed to simplify the process of configuring your zone for Antimalware capabilities, to include zone configuration, and creating and deploying Antimalware policies for Windows devices and servers.

From this page you can access several quick links to activate Endpoint Security and Antimalware, add an Antimalware entitlement key, configure scan schedules and notifications, create and assign Antimalware policies, and view dashlets that show the status of malware protection on devices. You can also access how-to videos  that walk you through these actions.

More Information

For more detailed information about the capabilities and employment of Antimalware policies and configuration, see the [ZENworks Endpoint Security Antimalware Reference](#).

