MICRO FOCUS

ZENworks 2020 Update 2

What's New Reference

August 2021

Legal Notice

Contents

About This Guide 5

1 What's New in ZENworks 2020 Update 2 7

1.1 Platform Support . . . 7
1.2 Installation and Upgrade . . . 7
1.2.1 Installing Docker and Docker Compose . . . 8
1.2.2 Migrating Server Data to New File Path . . . 8
1.2.3 Renaming of ZENworks Server services . . . 8
1.2.4 Introduction of a New Environment Variable . . . 8
1.2.5 TLS Version . . . 8
1.3 Replacing Primary Servers . . . 9
1.4 Moving a Primary Server to an Appliance . . . 9
1.5 ZENworks Configuration Management . . . 9
1.5.1 Windows 10 Device Management . . . 9
1.5.2 ZENworks Imaging . . . 11
1.5.3 ZENworks Remote Management . . . 11
1.5.4 Mobile Management . . . 11
1.5.5 Bundle Management . . . 12
1.5.6 Miscellaneous . . . 12
1.6 Security Enhancements in ZENworks . . . 12
1.6.1 Device Registration . . . 13
1.6.2 Device Communication . . . 13
1.6.3 Microsoft Data Encryption Policy Drive Exclusions . . . 14
1.7 Antimalware . . . 14
1.7.1 Protecting Against Malware - Getting Started page . . . 14
1.7.2 Antimalware Update Entitlement . . . 14
1.7.3 Windows Endpoint Security Policies . . . 14
1.7.4 Antimalware Security Dashlets . . . 15
1.7.5 Device Antimalware Page . . . 15
1.7.6 Malware Threat Details Page . . . 15
1.7.7 Antimalware Quick Tasks . . . 16
1.7.8 Antimalware zac Commands . . . 16
1.7.9 Antimalware Zone Configuration pages . . . 16
1.7.10 Ondemand Content Configuration Page . . . 16
1.7.11 Antimalware Service Status . . . 16
1.7.12 . . . Antimalware Database . . . 17

About This Guide

This *ZENworks What's New Reference* describes the new features in the ZENworks 2020 Update 2 release. The guide includes the following sections:

- Chapter 1, "What's New in ZENworks 2020 Update 2," on page 7

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 **comment on this topic** feature at the bottom of each page of the online documentation.

Additional Documentation

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

1 What's New in ZENworks 2020 Update 2

The following sections describe the new features and enhancements in ZENworks 2020 Update 2:

- Section 1.1, "Platform Support," on page 7
- Section 1.2, "Installation and Upgrade," on page 7
- Section 1.3, "Replacing Primary Servers," on page 9
- Section 1.4, "Moving a Primary Server to an Appliance," on page 9
- Section 1.5, "ZENworks Configuration Management," on page 9
- Section 1.6, "Security Enhancements in ZENworks," on page 12
- Section 1.7, "Antimalware," on page 14

1.1 Platform Support

The following new platforms are supported in this release:

- CentOS as a Managed Device
- macOS 11 (Big Sur) as a Managed Device
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 (Primary Server)
  - SLES 15 SP2 (Managed Device - Including SLES for SAP)
  - SLED 15 SP2 (Managed Device)
- New RHEL and Scientific Linux Platforms
  - Scientific Linux 7.7 and 7.8
  - RHEL 7.8 and 8.2

1.2 Installation and Upgrade

As ZENworks aims to adopt a more robust and flexible architecture, and to align itself with the Micro Focus standards, some enhancements have been introduced to the Install and Upgrade process in the ZENworks 2020 Update 2 release. The changes introduced in this release are as follows:

1.2.1 Installing Docker and Docker Compose

Before upgrading or installing ZENworks 2020 Update 2 on a Linux Primary Server, you are required to install Docker and Docker Compose on the server. For more information on Dockers, see https://docs.docker.com/. For more information, see Installing Docker and Installing Docker Compose.

For more information, see Changes in the Primary Server Upgrade or Migration Process and Prerequisites in the ZENworks Upgrade Guide.

1.2.2 Migrating Server Data to New File Path

After upgrading to ZENworks 2020 Update 2 on a Windows, Appliance or a Linux Primary Server, the ZENworks Server data such as MSIs, RPMs, logs, and configuration files that were earlier in the Novell file path will be moved to the new Micro Focus file path.

For example, on a Linux server, the configuration files that were earlier in: `/etc/opt/novell/zenworks` will now be available in `/etc/opt/microfocus/zenworks`. Similarly, on a Windows server, the configuration files that were earlier in: `C:\Program Files(x86)\Novell\ZENworks\conf` will now be available in `C:\Program Files (x86)\Micro Focus\ZENworks\conf`

The ZENworks agent related files and data will be retained in the old Novell location.

1.2.3 Renaming of ZENworks Server services

After upgrading to ZENworks 2020 Update 2 on a Windows, Appliance or a Linux Primary Server, certain ZENworks server services such as ZENServer service, ZENLoader service and ZENJoinProxy service, will be renamed from Novell to Micro Focus. For example, on a Linux server, `novell-zenserver.service` will be renamed to `microfocus-zenserver.service`.

1.2.4 Introduction of a New Environment Variable

For a Windows server, a new environment variable %ZENSERVER_HOME% has been introduced that it points to the Server installation location for non default path as well(`C:\Program Files(x86)\Micro Focus\ZENworks`.)

1.2.5 TLS Version

If you have freshly installed ZENworks 2020 Update 2, then by default, TLS1.2 will be enabled in the zone and when you try to register devices with Microsoft .NET version older than 4.7, then the device registration fails. However, the agent will be installed on the device.

If you are upgrading an existing zone to ZENworks 2020 Update 2, TLS1.2 will not be enabled by default. If you are enabling TLS 1.2 in the zone, then some of the features might not work as expected and ensure that you install Microsoft .NET 4.7 on all the devices in the zone.

If you have enabled TLS1.2 in the zone, then to register the device, the device should be installed with Microsoft .NET 4.7.

1.3 Replacing Primary Servers

For more details on replacing the first Primary Server with the second Primary Server, or replacing an existing Primary Server with a new Primary Server, see the *Replacing Primary Servers* in the *ZENworks Disaster Recovery Reference*.

1.4 Moving a Primary Server to an Appliance

For more details on the procedure to move an existing Primary Server (Windows or Linux) to an Appliance server, see *Moving from a Windows or Linux Primary Server to Appliance* in the *ZENworks Primary Server and Satellite Reference*.

1.5 ZENworks Configuration Management

- Section 1.5.1, “Windows 10 Device Management,” on page 9
- Section 1.5.2, “ZENworks Imaging,” on page 11
- Section 1.5.3, “ZENworks Remote Management,” on page 11
- Section 1.5.4, “Mobile Management,” on page 11
- Section 1.5.5, “Bundle Management,” on page 12
- Section 1.5.6, “Miscellaneous,” on page 12

1.5.1 Windows 10 Device Management

In the ZENworks 2020 Update 2 release, new capabilities have been added that will enable you to manage the entire life cycle of Windows 10 devices using the built-in MDM agent on these devices. To address the use cases beyond the capabilities of Windows 10 devices, you can also deploy the ZENworks agent on devices that use the Windows 10 MDM agents.

For more information on each of the capabilities listed in this section, see Windows MDM Reference.

The new capabilities are as follows:

Configuration Capabilities

You can now configure Windows Notification Service (WNS) to send push notifications to Windows devices that are managed through Windows Modern Management.

Enrollment Capabilities

The following enrollment capabilities have been introduced. For more information, see

Enrolling Methods: Windows 10 devices can be enrolled to ZENworks using the following methods.

- Provisioning package (PPKG) enrollment
- Azure Active Directory (Azure AD) Join
- AutoPilot Enrollment

Deploying the ZENworks Agent: You can now deploy the ZENworks Agent on Windows 10 devices that are already enrolled using the MDM mode of enrollment.

Configuring Terms of Use: You can assign the Terms of Use policy to devices to add the Terms of Use content to be displayed on the agent while enrolling Windows 10 devices using either the Azure AD Join or Auto Pilot enrollment.

Management Capabilities

The following management capabilities have been introduced:

Deploying Windows 10 MDM Bundles: You can now deploy the following bundles to Windows 10 MDM devices:

NOTE: Support for these bundles is on an experimental basis and should be used for evaluation purposes only.

- Using the Windows 10 MDM - Install MSI bundle deploy a Microsoft Installer (MSI) package on Windows 10 MDM devices.
- Using the Windows 10 MDM CSP bundle distribute Configuration Service Providers (CSPs) to deploy various configurations available through CSPs on Windows 10 MDM devices.

Initiating Quick Tasks: The following quick tasks are supported on Windows 10 MDM Devices:

- Delete Device
- Unregister Device
- Retire Device
- Un-retire Device
- Lost Device
- Unenroll Device

Other Capabilities

Some of the other capabilities introduced for the Windows 10 MDM feature are as follows:

- Windows 10 Devices support automatic reconciliation.
- The CA Remint process now issues certificates to Windows 10 MDM devices.
- The MS Graph API setting has been renamed to Azure MDM Application and needs to be re-configured to benefit from the new enhancements introduced in this release.

Getting Started with Modern Management

The Mobile Management Getting Started page is refurbished to include enrollment and management of Windows 10 MDM devices as well. For more information, see Modern Management Reference.

1.5.2 ZENworks Imaging

Restore Image using bundle name on WinPE: On ZENworks 2020 Update 1 and earlier versions, the WinPE distro supported restoring of the image by providing the image name using the IMG command, and the command did not recognize if the bundle was passed through the command. From ZENworks 2020 Update 2 onwards, the IMG bundle commands are supported on the WinPE distro. For more information, see Preboot Services and Imaging guide.

New tool to read ZENworks Image Information: The zmginfo tool helps to gather information about an image. This is particularly useful when you have multiple images in the content repository or the shared path, and you need to collect information about each image to save time. Using the zmginfo tool, you can gather either the basic or full information about the image. Using zmginfo, admin can create the bundle xml which can be imported as bundle and used to convert all the linux base images in to winpe base images.

For more information, see the Preboot Services and Imaging guide

1.5.3 ZENworks Remote Management

Remote Control of a device having active RDP Session: You will now be able to launch a remote session on a device with an active RDP session just like a normal Remote Management session. For more information, see the Remote Management Reference guide.

Recording a Remote Management Session (Experimental Support): Enables the users on the managed device to record the remote management session. For more information, see the Remote Management Reference guide.

1.5.4 Mobile Management

Enabling device assignments for Android bundles: Android bundles created for approved play store apps that were earlier restricted to user assignments, can now be assigned to devices as well. For more information, see Mobile Management Reference.

Provisioning System Apps: Using the Bundles feature, you can enable or disable System Apps on Android devices. System apps are in-built apps that are already pre-installed on the device. or more information, see Mobile Management Reference.

Getting started with Modern Management: The Mobile Management Getting Started page is refurbished to include the enrollment and management of Windows 10 MDM devices as well. Also, certain additional features associated with enrolling and managing of Apple and Android devices, have been included on this page. For more information, see Modern Management Reference.

Modifying the Android Device Log Location The location of the ZENworks App logs on Android devices have been modified to `Android/data/com.novell.zapp/files/Documents/zapp.log`. To share these logs, you need to deploy the Files app on Android devices.

1.5.5 Bundle Management

A new **Continue on Failure** option has been introduced in the Copy Relationships workflow. While copying relationships from one device to another set of objects, if there is an error encountered, the operation will continue for the rest of objects. The details of the errors will be displayed at the end of operation, along with an option to export the details of the operation for further reference and action. For more information, see Software Distribution Reference.

1.5.6 Miscellaneous

Enabling customers to use the latest version of the puppet-agent package: Previously, ZENworks provided the puppet-agent package as part of the build, which enabled users to use the Puppet policy. However, with the continuous updates to the puppet-agent version, post the ZENworks release, users were not able to use most recent version of the puppet-agent package. From this release onwards, for the Puppet policy to be effective on ZENworks 2020 Update 2 and later, Linux managed devices, you need to ensure that the puppet-agent package is installed on the devices. For more information, see Configuration Policies Reference.

1.6 Security Enhancements in ZENworks

The security enhancements introduced in this release enable you to securely register and communicate with devices even in a DMZ environment.

- If you have newly installed ZENworks 2020 Update 2, then, by default, the Security settings will be enabled on all the Primary Servers.
- If you are upgrading the Primary Servers, then the Security settings will be disabled by default.
- If you have added a new Primary Server to the zone, after upgrading to ZENworks 2020 Update 2, then, by default, the Security Settings will be enabled. Ensure that you disable the Security Settings temporarily until all the agents in the zone are updated to ZENworks 2020 Update 2, else the agents stop communicating or the device registration might not work.

You need to run the following zman command to enable the settings:

- `zman ssassc` (Security-Set-Agent-Server-Secure-Communication) is introduced to enable or disable authentication for communication between the ZENworks Agent and the ZENworks servers.

For more information, see Security Commands in the ZENworks Command Line Utilities Reference and Security Administrator in the ZENworks Best Practices Guide.

1.6.1 Device Registration

Pre-approving Device Registration

Pre-approved devices are those devices that are approved by the administrators to be part of the zone. This is particularly useful when you have to pre-approve devices while bulk enrolling a known set of devices. It can also be used to allow known devices to reconcile, if required.

For more information, see Adding Pre-approved Devices in the ZENworks Discovery, Deployment, and Retirement Reference

Using the Authorization Key

An Authorization key can be used by the ZENworks agent to authorize itself to register to the zone and for any communication with the server during installation.

For more information, see Creating Authorization Key in the ZENworks Discovery, Deployment, and Retirement Reference

Securing Managed Device and Inventory-Only Agent (IOA) Device Registration

To register newer Inventory-Only Agents (IOA) or Managed Device to the zone, you need to either specify an Authorization key during device registration or ensure that the device is a part of the pre-approved devices list.

For more information, see Secure Communication between Managed Devices and ZENworks Servers.

1.6.2 Device Communication

Using OSP for Device Communication Including ZCC Login

For most features, ZENworks has switched to using the O-Auth protocol for establishing user identity. Therefore, a new service called the OSP has been introduced and it is used for logging in to ZCC, inter-service communication and for communication between device and servers.

Securing Content and Collection between Devices, Primary Servers and Satellite Servers

With the introduction of this new security feature, the end to end collection and transfer of content between managed devices, Primary Servers and Satellite Servers is through SSL. This can be achieved by configuring the setting within ZCC or by using the newly introduced zman commands. For more information, see Adding and Configuring Satellite Devices in the ZENworks Primary Server and Satellite Reference.

Securing Webservice Communication Between Device and Primary or Satellite Server

To further secure webservice communication between the ZENworks Agent and the ZENworks Primary and Satellite servers, security enhancements have been introduced to the web service calls in this release.

1.6.3 Microsoft Data Encryption Policy Drive Exclusions

Removable data drives can now be excluded from encryption by drive type in the Microsoft Data Encryption Policy when the policy is enforced on managed devices.

1.7 Antimalware

ZENworks Antimalware is a new component of ZENworks Endpoint Security Management under the Security grouping in the ZENworks Control Center. Antimalware is a compressive solution that protects managed devices from all the latest malware threats. When deployed to devices in your zone, the Antimalware Agent continuously receives updates of malware signature files from the Antimalware Cloud Service to detect malware infections using both on-access and on-demand scans. Infected files are quarantined until they are disinfected.

For more information about the topics in this section, see the following:

- ZENworks Endpoint Security Antimalware Reference

1.7.1 Protecting Against Malware - Getting Started page

Security's Getting Started page includes an additional tabbed page titled, "Protecting Against Malware." You can use this page as a single point of access to configure, deploy, and customize all the features that ZENworks Antimalware has to offer.

1.7.2 Antimalware Update Entitlement

The Antimalware Update Entitlement is required to deploy Antimalware policies to devices. The entitlement is automatically enabled for the evaluation period when activating Endpoint Security Management in Evaluation mode.

1.7.3 Windows Endpoint Security Policies

Four new policies are used to manage Antimalware deployment, customization, and continuity:

Antimalware Enforcement Policy: This is the base policy that installs the Antimalware Agent on managed devices. This policy must be deployed to use any of the other Antimalware policies. It includes configurations for all types of malware scans, including on-access and full, quick, external device, and contextual ondemand scans. There are also settings for quarantine behavior and defining content to exclude from scans.

If the default settings for end user rights and notifications are maintained when the policy is deployed, end users will have access to the Agent Status Console on their endpoints, which enable them to initiate their own scans, view scan and agent update status, and receive notifications of agent activity controlled by the policy.

Antimalware Scan Exclusions Policy: Antimalware has scan exclusions that are both built-in and custom scan exclusions that you can add to any of the Antimalware policies. The Scan Exclusions policy is employed by device assignment when other Antimalware policies are also assigned to the same devices, which enables a more simplified way to propagate scan exclusions across the zone. Exclusions can by enabled or disabled for specific scan types

Antimalware Custom Scan Policy: The Custom Scan Policy is used for a more targeted approach to scan local drives on managed devices when a specific threat is suspected or to target scans to specific locations on those devices. It includes its own schedule as opposed to using the zone schedule that is configured for the Antimalware Enforcement Policy

Antimalware Network Scan Policy: The Network Scan Policy is also used for a more targeted approach, but is explicitly used for scanning folders and files on Network drives. It also has its own schedule, and includes an additional setting for authentication to network locations.

1.7.4 Antimalware Security Dashlets

Four new dashlets that default to the Security Dashboard are provided to monitor malware threats, malware scans, and malware signature updates.

Device Malware Status: This dashlet displays the malware status for individual devices in the zone, for a selected detection period.

Device Last Malware Scan: This dashlet displays the health of the devices in your zone against malware threats. By default, it displays information about any type of scan that was performed on devices for a specified time period.

Top Malware Threats: This dashlet displays the list of top malware threats in the zone. By default, the top malware threats are displayed based on the number of infected devices.

Device Malware Signature Version: This dashlet displays the list of Malware Signature versions and the Antimalware Agent versions that are installed on devices in the zone.

1.7.5 Device Antimalware Page

This page is a new tab that is accessed when a device is selected. It provides a snapshot status of malware threats, the scan schedule, and quarantined file information for the selected device. You can also take specific actions on files, kickoff scans, and update the Antimalware Agent and Malware Signature versions on the device.

1.7.6 Malware Threat Details Page

This page is accessed by clicking a malware threat link in the Malware Threats section of a device's Antimalware page. It provides detailed information about the selected threat and details of the devices that have been infected with the threat.

1.7.7 Antimalware Quick Tasks

When one or more devices that have the Antimalware Agent installed are selected in the Devices grouping of the ZENworks Control Center, five new quick tasks are available to run on the selected devices. These include the following quick tasks:

- Initiate a Malware Scan
- Update Malware Signature
- Update Antimalware Agent
- Restore File from Malware Quarantine
- Delete File from Malware Quarantine

1.7.8 Antimalware zac Commands

Antimalware comes with several new zac commands that are specific to this component. These includes commands to initiate malware scans on devices, check Antimalware Agent malware status, install, update, or remove the agent, and delete files from quarantine, among others.

1.7.9 Antimalware Zone Configuration pages

Three new zone configuration pages are now included in the Security grouping from the main ZENworks configuration page. Each of these pages include default settings that you can customize. The pages are as follows:

Antimalware Agent Schedules: Configures the schedules for malware scans and malware signature updates. You can override this schedule at the device folder and device level.

Antimalware Agent Notifications: Configures the alerts and notifications that are displayed by the Antimalware agent on managed devices. You can override these settings at the device folder and device level.

Antimalware Configuration: Defines the ZENworks Primary Server to use as the Antimalware server, which must be manually configured to deploy the Antimalware component. Also configures the maintenance schedule for the Antimalware Agent.

1.7.10 Ondemand Content Configuration Page

This new zone configuration page is now included in the Bundle, Policy, and Content grouping from the main ZENworks configuration page. It manages the content download rate and content cache size for content distribution in the zone, which currently includes Antimalware signature files and Antimalware Agent updates.

1.7.11 Antimalware Service Status

The Antimalware Service status can now be accessed in the ZCC Diagnostics page.

1.7.12 Antimalware Database

The Antimalware Database is new with ZENworks 2020 Update 2. Its purpose is to provide data for the monitoring capabilities of Antimalware via the Antimalware page and the Antimalware security dashlets. When configured, this database synchronizes with the ZENworks Database and therefore must be of the same database type. For example: PostgreSQL, Microsoft SQL Server, or Oracle.

The Antimalware Database is configured from the Protecting Against Malware - Getting Started page for Security in the ZENworks Control Center. If the Antimalware Database will be configured using an external database that does not yet exist, one can be created from a CLI command using the `setup.exe` file.