ZENworks 2020 Update 1

What’s New Reference

June 2020

Legal Notice

Contents

About This Guide

This *ZENworks What's New Reference* describes the new features in the ZENworks 2020 Update 1 release. The guide includes the following sections:

- Chapter 1, "What's New in ZENworks 2020 Update 1," 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 1

The following sections describe the new features and enhancements in ZENworks 2020 Update 1:

1.1 Important Security Updates

The ZENworks 2020 Update 1 release includes some important security updates. Hence, it is strongly recommended that you upgrade to ZENworks 2020 Update 1.

1.2 Platform Support

The updated platform support for ZENworks 2020 Update 1 includes the following:

- Windows 10, 2004
- RHEL 7.7, 8, 8.1
- macOS 10.15 (Catalina)
- iPadOS 13

NOTE

- The Inventory Only Agent and the Portable Collector are not supported on macOS (Catalina) 10.15.
- ZENworks now supports macOS 10.11 and 10.12 only in the backward compatibility mode.

1.3 ZENworks Configuration Management

1.3.1 Ability to configure the Certificate Validity for MDM and Non-MDM servers

While performing a change CA (Certificate Authority) or a Remint CA operation, you can now provide the certificate validity for MDM and non-MDM servers, separately. This feature is helpful in ensuring a 2 year validity for MDM servers, which is a requirement for iOS devices. For more information, see Configuring the Certificate Authority in the *ZENworks SSL Management Reference*.

1.3.2 New Remote Management Viewer

From ZENworks 2020 Update 1 onwards, by default, the new Remote Management viewer will be used while remote controlling devices. You also have the option to use the legacy Remote Management Viewer, if required. The new viewer includes a lot of performance improvements and bug fixes. For more information, see ZENworks Remote Management Reference.

1.3.3 Enhanced security in Remote Control sessions

Remote Control sessions are now even more secure using TLS 1.3. This enhanced security is available only when both the Remote Viewer and Managed Device are running 2020 Update 1 components on Windows devices.

1.3.4 Migration from Oracle and Microsoft SQL to PostgreSQL

Using the latest database migration tool, you can migrate the database from Microsoft SQL and Oracle to PostgreSQL. For more information, see:

- Oracle to PostgreSQL Migration
- Microsoft SQL to PostgreSQL Migration

1.3.5 Mobile Management

Mobile Management includes the following new features and enhancements:

- Support for iPadOS platform: ZENworks now supports the iPadOS platform that are iPad devices with iOS version 13 or later installed. All policies and bundles that are applicable for iOS devices are now extended to include iPadOS devices as well. This feature is by default in a disabled state and needs to be enabled after migrating to the ZENworks 2020 Update 1 release version. For more information, see Support for the iPadOS platform in the *ZENworks Mobile Management Reference*.

Also, new settings have been introduced for iOS and iPadOS devices in the Mobile Device Control Policy and the Apple Device Enrollment Program (general and skip item settings). For more information, see Securing a Device in the *ZENworks Mobile Management Reference*.

- Distribute Provisioning Profile for iOS/iPadOS: You can now renew a provisioning profile that is required to run enterprise and developer apps. As a provisioning profile expires within a year, you can use the existing iOS/iPadOS Profile bundle to renew the profile without the user having to re-install the associated app manually on the device. For more information, see Distributing an iOS Profile in the *ZENworks Mobile Management Reference*.
- Deploy Web App shortcuts: Using the existing bundles feature, ZENworks now lets you deploy a web app shortcut to iOS, iPadOS, and Android devices. These shortcuts will allow users to have quick access to web pages that they use frequently. For more information, see Distributing Web App Shortcuts in the *ZENworks Mobile Management Reference*
- Auto-update bundles when updates are available for VPP apps: In previous ZENworks releases, when there was an update for a VPP app, it was not automatically deployed on the assigned devices and the end user had to manually update the app. From this release onwards, when an update for a VPP app is available, you can instruct ZENworks to automatically create a Sandbox version or a Published version of the associated bundle and deploy it on devices. This can be set at the Subscription level or for specific apps in the Apps Catalog page. For more information, see Distributing VPP Apps in the *ZENworks Mobile Management Reference*

1.3.6 Bundle Management

- Change in bundle status in the Device Relationship page: In the Device Relationship page, the bundle status is now displayed at a granular level based on the action sets that are Distribution, Install and Launch. This will enable you to identify the exact stage at which the bundle failed to apply on the device.
- Display block status for user assigned bundles: The deployment dashlets now reflects the correct status of a user assigned bundle when it is blocked. For more information, see Accessing the Bundle Dashboard in the . *ZENworks Software Distribution Reference*
- Addition of new value type and string type in Registry Key Value in System Requirements: A new value type “version” has been added in the Registry Key Value filter condition as a part of the Bundle and Policy system requirements. The ‘contains’ operator has also been added in the same filter condition. For more information, see Managing System Requirements in the *ZENworks Software Distribution Reference*
- Display exact reason of assignment failure for a bundle: If an assignment is not effective on the device, then the bundle assignment status dashlet will display the exact reason for the failure. To view these details, you need to click the hyperlink displayed in the Not Effective Reason column in the dashlet. For more information, see Accessing the Bundle Dashboard in the *ZENworks Software Distribution Reference*.

- Display device assignments for a disabled bundle: The Relationships tab of a bundle, now displays all the effective and non-effective device assignments of a bundle. This is particularly useful if you want to identify all the device assignments made for a disabled bundle. For more information, see Bundle Tasks in the *ZENworks Software Distribution Reference*.
- ZENworks has always supported execution of PowerShell scripts on Windows devices. While creating a bundle, and choosing a script to run, now it is possible to select PowerShell from the drop-down and ZENworks will automatically populate the execution parameters, thus making it easier to execute PowerShell scripts on Windows devices. For more information, see Action - Run Script in the *ZENworks Software Distribution Reference*

1.3.7 Vertica Database Enhancements

- Display pending records within Data Sync Status panel in the Diagnostics page: The Data Sync Status section in the Diagnostics page that displays the status of the data sync process between the RDBMS and Vertica, also displays the number of pending records that are yet to be migrated from each Kafka connector to Vertica. For more information, see Data Sync Status in the *Vertica Reference Guide*.
- Re-create Kafka connectors: When you migrate from one RDBMS to another, and if you have Vertica installed in your zone, then you need to re-create the Kafka connectors to enable syncing of data from the new RDBMS to Vertica. A new zman command has been introduced to re-create Kafka connectors after database migration. For more information, see Maintaining the Kafka Cluster in the *Vertica Reference Guide*
- Removal of the maximum cluster size parameter from the ZooKeeper update command: The requirement to update the maximum cluster size, if more than 3 ZooKeeper nodes are to be installed, is now removed.

1.3.8 Content Transfer Through a Secure Connection

By default, content is now transfered from Primary Servers, in an encrypted form, to other Primary Servers, Satellite Servers and managed devices through a secure connection (HTTPS port 443). However, content between Satellite Servers and Managed Devices will continue to be transfered over port 80.

1.3.9 Relationships page for Workstations has been split into Membership and Assignments pages

Since the Relationships page for Devices was earlier taking a lot of time to load as it included information related to device groups along with bundle and policy assignment details, this information has now been split into the following pages to improve readability and performance:

- Memberships: Includes information about groups and dynamic groups.
- Assignments: Includes information about Bundle and Policy assignments.

1.4 Inventory

- Section 1.4.1, "Administrator Defined Fields," on page 11

1.4.1 Administrator Defined Fields

From ZENworks 2020 Update 1 onwards, you can define 100 Workstation Administrator Defined Fields (ADFs). The existing ZENworks Control Center and ZENworks Reporting reports include these additional ADFs. For more information, see Using Administrator-Defined Fields in the *ZENworks Asset Inventory Reference*.

1.5 ZENworks Agent

- Section 1.5.1, "Mac Agent Installation," on page 11
- Section 1.5.2, "Ability to hide the folder list in the ZENworks Agent," on page 11

1.5.1 Mac Agent Installation

From this release onwards, you can install the ZENworks Agent on Mac (10.13 or later) devices using the new installer. For more information, see Manually Deploying the Agent on a Macintosh Device in the *ZENworks Discovery, Deployment, and Retirement Reference*.

1.5.2 Ability to hide the folder list in the ZENworks Agent

A setting to hide the folder structure for a bundle in the ZENworks Agent and ZENworks Explorer window has been introduced in the ZENworks Explorer Configuration Policy. For more information, see ZENworks Explorer Configuration Policy in the *ZENworks Configuration Policies Reference*

1.6 Patch Management

- Section 1.6.1, "Security Dashboard Enhancements," on page 11
- Section 1.6.2, "Custom Patch Enhancement," on page 12
- Section 1.6.3, "User interface displayed while applying patches during shutdown," on page 12

1.6.1 Security Dashboard Enhancements

- Added a Vulnerability Status filter in the Top CVEs dashlet and CVE Severity Distribution dashlet. In previous releases, the dashlets displayed a CVE that applied to devices regardless of whether or not any of the devices remained vulnerable (not patched) to the CVE. In Update 1, the Vulnerability Status filter lets you display only the CVEs with currently vulnerable (not patched) devices. After the system update, the two default dashlets have the filter automatically applied; however, custom dashlets must be edited to turn on the filter. For more information, see CVE Reference.

- Added the ability to easily create CVE Tracker dashlets from the Top CVEs dashlet and CVE Severity Distribution dashlet by selecting the desired CVEs from the dashlet's CVE list and using the Create CVE Tracker option.
- Added the ability to easily create Patch Tracker dashlets from the Recently Released Patches dashlet and the zone Patches list by selecting the desired Patches from the Patch list and using the Create Patch Tracker option. For more information, see CVE Reference and ZENworks Patch Management Reference.
- Added the ability to pin Patch dashlets to the Security dashboard.

1.6.2 Custom Patch Enhancement

Using the Custom Patch feature, you can now monitor patches that are downloaded manually, from external sources (not through the Patch subscription), using ZENworks Patch Management. For example, the Windows 7 ESU patches. The Custom Patch feature has been enhanced to enable you to define the criteria that makes the custom patch applicable to a device and also define the criteria that indicates a device is patched. For more information, see Create a Custom Patch in the *ZENworks Patch Management Reference*.

1.6.3 User interface displayed while applying patches during shutdown

From this release onwards, instead of the PowerShell window, a user interface is displayed while applying patches at shutdown.

1.7 Full Disk Encryption

Full Disk Encryption includes the following updates:

- The Full Disk Encryption Agent now includes a “Graphical PBA” boot method for pre-boot authentication that you can configure for upgraded hardware compatibility on UEFI enabled devices. This option, when added to the DMI file and when used in tandem with custom PBA resolution, is particularly useful on tablet devices during pre-boot authentication. To use this feature, add the following string to the DMI file hardware compatibility settings:

  ```
  KERNEL=[SDP_KERNEL_SIMPLE_PBA_GUI]
  ```

  For more information about this setting or hardware compatibility in general, see “Configure Pre-Boot Authentication - Hardware Compatibility” in the *ZENworks Full Disk Encryption Policy Reference*.
- Full Disk Encryption now requires UEFI enabled devices to boot from Secure Boot Manager in the boot order. This configuration gets reverted to Windows Boot Manager in the boot order if the Disk Encryption policy is deployed to a device after the device is upgraded to a ZENworks 2020 Update 1 or later version from a ZENworks 2020 or earlier version. If the Disk Encryption policy is already deployed to a device before the upgrade, in this version scenario, the device continues to boot to Secure Boot Manager.

- At least 50 MB of free disk space is required for the EFI system partition (ESP) when the system’s firmware is configured to run UEFI BIOS.

  For more information about managed device requirements with Full Disk Encryption, see “System Requirements” in the *ZENworks Full Disk Encryption Agent Reference*.

1.8 ZENworks Reporting

As part of the Inventory feature, ZENworks now enables you to define 100 Workstation Administrator Defined Fields (ADFs). To include these 100 ADFs in the ZENworks Reporting reports, you need to re-configure the ZENworks Reporting Appliance.