ZENworks 2017 Update 3
What's New Reference

August 2018

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.novell.com/company/legal/.

Contents

About This Guide

This *ZENworks What's New Reference* describes the new features in the ZENworks 2017 release. The guide includes the following sections:

- Chapter 1, "What's New in ZENworks 2017 Update 3," 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 2017 Update 3

The following sections describe the new features and enhancements in ZENworks 2017 Update 3:

-
-
-
-
-

1.1 Platform Support

ZENworks 2017 Update 3 supports the following new platforms:

- Windows 10 April 2018 Update, version 1803
- openSUSE Leap 42.3 and 15
- SUSE Linux Enterprise Server 15 (SLES 15)
- SUSE Linux Enterprise Desktop 15 (SLED 15)
- iOS 11.4

For more information on the system requirements, refer to the ZENworks 2017 Update 3 System Requirements

1.2 ZENworks Configuration Management

-
-
-
-
-
-
-
-

1.2.1 Dashboard

Actionable Dashboards For Patch and Device Management: Actionable Dashboards provide you with a visual representation of the data in your zone, helping you to identify problems faster. With this release, administrators can monitor vital system statuses, such as the patch compliance status of devices, the security compliance status of Android Enterprise mobile devices, and the last time devices scanned for vulnerabilities or made contact with a ZENworks server. After identifying the various statuses, the required actions can be taken to resolve any concerns. Custom dashlets can be created based on requirements and then saved and pinned to a dashboard.

This release includes the following dashlets:

- Device Management Dashlets: Android Enterprise Compliance Status, Device Last Contact Time, and Device Distribution
- Patch Management Dashlets: Patch Subscription Status, Recently Released Patches, Device Patch Compliance, and Device Last Patch Scan

For more information, see the ZENworks 2017 Update 3 Dashboard Reference.

1.2.2 Mobile Management

- "Work Managed Mode for Android Devices" on page 8
- "Support for Intune App Protection" on page 8
- "Locate Lost Mobile Devices" on page 9
- "Lost Mode Support for iOS Devices" on page 9
- "Support for new iOS 11 Restrictions and DEP Settings" on page 9
- "Restart and Shutdown Quick Tasks for iOS Mobile Devices" on page 9
- "User Interface for Mobile Inventory Configuration" on page 9

Work Managed Mode for Android Devices

ZENworks has now extended its Android Enterprise support to include the Work-Managed Device mode. This feature enables administrators to manage the entire device, without the creation of containers to separate corporate and personal data, thereby restricting it to corporate use only. Only administrator-approved apps can be installed from Google Play Store. The administrator can also remotely wipe corporate data from a work-managed device. All the Android Enterprise related features will continue to be available in this mode.

For more information, see Enrolling devices in the work-managed device mode in the ZENworks 2017 Mobile Management Reference.

Support for Intune App Protection

ZENworks enables you to secure apps built using the Intune SDK (for example, Microsoft Office 365 apps), without users having to enroll the devices in ZENworks. By configuring Microsoft Graph API, you can create policies from within ZENworks, to secure Intune apps on iOS devices. These policies help you to enforce the manner in which end users access data (Example: Enforce the use of a PIN), restrict the devices on which they access data (Example: Restrict access on jail-broken devices), and restrict the cut, copy and paste of data. If required, you can wipe the app data off a device, from within ZENworks itself.

For more information, see Managing Intune Apps in the ZENworks 2017 Mobile Management Reference.

Locate Lost Mobile Devices

With this release, administrators can now use ZENworks to identify the current location of lost iOS and Android devices. As and when the lost supervised devices are located, end users are notified through notifications and emails. The built-in privacy settings ensure that only the last known location of the device is stored in ZENworks, in an encrypted format, and access to location details is controlled by rights. Apart from this, every attempt to access a location, is audited.

For more information, see Locating a Device in the ZENworks 2017 Mobile Management Reference.

Lost Mode Support for iOS Devices

This feature enables you to lock an iOS supervised device, when it is lost, with the option to display a recovery message and call-back phone number.

For more information, see Enabling Lost Mode in the ZENworks 2017 Mobile Management Reference.

Support for new iOS 11 Restrictions and DEP Settings

This release includes support for additional iOS 11 restrictions related to AirPrint, system app removal and additional settings to enable features such as voice dictation, Wi-Fi whitelisting and VPN configuration.

The DEP settings are also enhanced to support features such as Aerial screensavers, Touch-To-Setup, Home Screen Sync and TV Provider Sign-in for Apple TVs. Apart from this, Update 3 also provides support for features such as Keyboard Setup, Onboarding, and Watch Migration.

For more information, see the ZENworks 2017 Mobile Management Reference.

Restart and Shutdown Quick Tasks for iOS Mobile Devices

The Restart and Shutdown quick task is now extended to include iOS supervised devices as well.

For more information, see Reboot or Shutdown iOS Devices in the ZENworks 2017 Mobile Management Reference

User Interface for Mobile Inventory Configuration

Using ZENworks Control Center you can now schedule an inventory scan of mobile devices at the Management Zone, Device Folder and Device level. You can either configure the inventory scan to run during specific intervals, or you can run a quick task to manually initiate the inventory scan to collect inventory details instantaneously.

For more information, see Managing a Device in the ZENworks 2017 Mobile Management Reference

1.2.3 Audit Management

Integration with SIEM Tools: ZENworks can now send audit and system events or messages in CEF format to Syslog servers. These events can be correlated in Security Information and Event Management (SIEM) tools, such as ArcSight and Sentinel, to alert administrators when specific events occur on the system.

1.2.4 System Update

More Accurate Device Count During System Update The enhanced representation of the System Update Deployment status now provides you with a more accurate count of devices to which the update is assigned, regardless of whether they are part of a direct assignment, a group or a dynamic group. This ensures that at any point in time you get an accurate view of the status of the update.

Automatic Download of PRUs You can now automate the monthly Product Recognition Update (PRUs) deployments. Using ZENworks Control Center you can configure monthly schedules to check for PRU availability, download and deployment. You can also configure email notifications to inform administrators about the PRU deployment status.

For more information, see PRU Schedule in the ZENworks System Updates Reference.

1.2.5 Imaging

MDT Deployment using INI files: Based on requirements, MDT deployment can now be automated using the `CustomSettings.ini` or the `Bootstrap.ini` files. Using these INI files, you can achieve Lite Touch to Zero Touch deployment.

Rule Variables for Preboot bundles: Users can now define rule variables for Preboot bundles.

Conversion from MBR to GPT using WinPE distro: Using the WinPE distro users can now convert MBR disks to GPT disks.

Bundle Name Change: The names of the following imaging bundles have been changed:

- Imaging Script to Linux Imaging Script
- Third-Party Script to WinPE Imaging Script

Firmware Type Filter to assign bundles based on firmware: The new Firmware Type filter in the Rule Logic filter enables users to assign bundles based on the firmware type.

For more information, see the ZENworks Preboot Services and Imaging Reference.

1.2.6 Support for Windows 10 Version Details

ZENworks now displays Windows 10 version details (build numbers) in the Device Properties, Inventory and System Requirements pages.

1.2.7 ZENworks App

Updated ZENworks Branding Policy: Using the ZENworks Branding Policy you can now specify the size of the icons displayed in ZENworks Application (ZAPP).

1.2.8 Database Migration Support from Oracle to MSSQL

ZENworks now supports the migrations of data from Oracle to a Microsoft SQL database that is installed on a device on which ZENworks is not installed.

For more information, see Migrating the Data from an Oracle Database to an MS SQL Database in the ZENworks Database Management Reference.

1.3 ZENworks Reporting

1.3.1 Updated ZENworks Reporting Inventory Domain

With the enhanced ZENworks Reporting Inventory domain, reports are now generated much faster than before.

IMPORTANT: In ZENworks Reporting 6.4.3 release, use port 443 instead of 8443 to access the ZENworks Reporting console.

1.3.2 Inclusion of Mobile Inventory data in ZENworks Reporting

You can now generate Mobile App Inventory data reports for devices enrolled with ZENworks.

For more information, see the ZENworks Reporting Universe Objects and Predefined Reports Reference.

1.3.3 ZENworks Reporting 6.4.3

Changes in ZENworks Reporting 6.4.3 include the following:

Dashboards

Dashboards now support:

- Hyperlinks for dashlets that can replace the current dashboard with a web page, report, dashboard, or Ad Hoc view.
- New formatting options for text dashlets.
- New Undo, Redo, and Undo All buttons on the dashboard toolbar that allow you to undo and redo recent changes made to the dashboard, including changes to input control values.
- New Time-Date wildcards for dashlets.

Dashboard enhancements include:

- Dashboard and dashlet exporting.
- Text and image dashlets now support hyperlinks.
- More formatting options for dashboards and dashlets.
- New time and date wildcards for dashlets.

- Auto-complete for parameters and time and date wildcards.
- Image dashlets have a Browse button for selecting images from the repository.

Scheduler

New enhancements include:

- Support for scheduling dashboard exports.
- Support for SFTP with SSH key authentication as a transfer protocol.
- Automatic validation of the path to the repository output folder when clicking Save
- Support for changing the default output folder; it's specified by editing a configuration file.

Performance Improvements

JasperReports Server is faster and uses less memory when working with high-cardinality data in Ad Hoc views or reports based on Ad Hoc views.

Security Improvements

JasperReports Server implements a new Cross-Site Request Forgery (CSRF) protection mechanism that is more effective and less intrusive.

1.3.4 Jaspersoft Studio 6.4

Advanced report designer now supports:

- Updated interface for HTML5 charts. An updated chart dialog for HTML5 charts lets you configure your data and preview your chart when it is created.
- Improved customizers for JFreeCharts in JasperReports Library,including:
  - New chart customizers classes for working with specific chart types.
  - Support for configurable chart customizers, which let the user enter values at report runtime.
  - Support for multiple chart customizers applied to a single chart.
  - User interface support for chart customizers in Jaspersoft Studio using a JSON file that can be uploaded.

1.4 Full Disk Encryption

Full Disk Encryption added support for Windows Secure Boot, which enables the deployment of Full Disk Encryption policies on Windows devices configured with UEFI firmware settings.

1.5 Patch Management

Patch Management includes the following changes and enhancements:

1.5.1 Redesigned Dashboard

Patch Management is part of the new ZENworks Dashboard, which significantly enhances the utility of the Patch Dashboard, both for assessing the health of your patch environment and for taking action when weaknesses are found. The new Patch Management Dashboard includes four default dashlets and the capability to create custom dashlets from the default dashlets. See descriptions for each of the Patch Management dashlets below:

- **Patch Subscription Status:** Displays the number of known patches in the zone, their status, and the last start and end times of subscription activities for licenses, patch discovery, and patch download.
- **Recently Released Patches:** Displays the number of recently released patches by patch impact type.
- **Device Patch Compliance:** Displays compliance status for devices in the zone.
- **Device Last Patch Scan:** Displays the number of devices scanned for patches by time range.

1.5.2 Redesigned Patch Compliance Criteria

In conjunction with the redesigned Patch Management Dashboard, patch compliance is now based on a configurable percentage of Critical and Recommended patches installed on each device. This change is configured in the Patch Management > Dashboard and Trending configuration, and displays data in the new Device Patch Compliance dashlet.

For more information, see Configuring Patch Dashboard and Trending in the ZENworks 2017 Patch Management Reference.

1.5.3 New Patch Scan Behavior

In previous releases, scheduled scans would only execute if the scan engine detected that a new DAU (Discover Applicable Updates) bundle had been delivered to the device since the last scan. While this behavior minimized potential performance impacts due to patch scanning, it also introduced the following concerns:

- A patch scan detects whether a patch has been installed regardless of the installation source. If a patch is installed by a non-ZENworks tool (such as the application's native updater), skipping the scan because the DAU bundle has not changed would cause the device's patch status to be incorrect.
- The Last Patch Scan date in the Device Last Patch Scan dashboard (enhanced in this release) could be misleading because the scan engine reports that it performed the scan even if it skipped the scan because the DAU bundle had not changed.

To resolve this issue, the scan behavior was modified to ensure that a scheduled scan is performed every time regardless of whether or not the DAU bundle has changed. If users encounter a noticeable performance impact on their devices, you can revert to the previous scan behavior by adding PATCH_SCAN_ALWAYS=FALSE to the System Variables.

For more information, see Patch Management System Variables in the ZENworks 2017 Patch Management Reference.