MICRO FOCUS

ZENworks 2020 Update 3

What's New Reference

November 2022

Legal Notice

Contents

About This Guide

This *ZENworks What's New Reference* describes the new features in the ZENworks 2020 Update 3 release. The guide includes the following sections:

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 3

The following sections describe the new features and enhancements in ZENworks 2020 Update 3:

1.1 Platform Support

For information on the supported platforms, see the ZENworks System Requirements document.

1.1.1 .NET Framework Version

If you have updated your zone to ZENworks 2020 Update 3, then ensure that you go through the following points before upgrading the Windows devices:

- If you are deploying the agent for the first time, then the agent package includes .NET 4.8 Framework, which will be installed on the device, if not available.
- The system update checks for .NET Framework version 4.8 or above on the device. If the required version is not available, then the update might not complete successfully. Ensure that you have .NET Framework version 4.8 or above on all Windows Managed Devices before deploying the system update. To download, click the Microsoft .NET download link (https://dotnet.microsoft.com/en-us/download/dotnet-framework).

  If you are facing any issues while deploying, see ZENworks 2020 Update 3 Readme.

NOTE: You must reboot the device after the installation of .NET 4.8.

1.2 ZENworks Configuration Management

1.2.1 Ondemand Distribution of Content

Up to this release, any content (bundles, policies, system updates, patches) that you wanted on a managed device had to first be replicated to a Content Server (Primary Server or Satellite) accessed by the device. In ZENworks 2020 Update 3, Content Servers can now retrieve content ondemand when a device requests it, meaning that the content no longer needs to be replicated as before. Instead, if a Content Server does not have the content cached locally, it requests the content from an upstream server, and that server streams it back to the requesting Content Server where it is cached for use. Both distribution methods - replication and ondemand - can be used.

This ensures that app installations do not fail with awaiting content, and installations can be triggered without waiting for content to be replicated across the zone.

1.2.2 ZENworks Control Center

Pin Favorites: In the Frequently Used tab in ZCC, you can pin and unpin frequently used objects as favorites.

Monitor Active Sessions: In the Diagnostics page, administrators can monitor the active sessions. The ZENworks Control Center Active Sessions lists the currently logged-on administrators (super administrators and non-super administrators). Administrators can search for active users by entering the name of the user in the Search field.

For more information, see ZENworks Control Center Active Sessions.

Rearranging Dashlets Arranging dashlets with the same height dashlet would cause a blank space. Now, this has been fixed and dashlets can be asymmetrically arranged for optimum utilization of the dashboard.

Session Timeout: Introduced a setting to control ZCC Session timeout. Using this setting administrators can choose a timeout value through UI instead of going through configuration files. Additionally, administrators can configure the setting to display a session timeout prompt and the ability to increase the timeout.

For more information, see Changing the Timeout Value for ZENworks Control Center.

Remove MDM Enrolled Devices: This setting applies only for Win MDM enrolled devices, you can also set the 'remove device' value on the device. If the device does not contact the ZENworks server, the device automatically gets un-enrolled from MDM, without any ZENworks intervention.

For more information, see Windows MDM Reference.

Auditing Logins: The information about the users logged into devices is audited. You can view the current and historical users to find out who is using the devices and also view which user was using which device.

Device Data Collection: ZENworks collects the Last Boot Time, Network Location and Reboot Pending data from the devices and displays it on the Device Summary page. Devices can also be searched using these fields.

Deployment Packages: From ZENworks 2020 Update 3 onwards, the Network (.NET required) and Standalone (.NET required) packages for Windows and Network (JRE required) for Linux are no longer supported. The Network, Standalone, and Web deployment packages for Windows and Linux are supported.

An administrator user can download the packages from the **Download ZENworks Tools** page in ZENworks Control Center (**Home** > **Download ZENworks Tools** > **ZENworks Agent** > **Agent Packages**). The three versions of each package are available in version x86, x86_64, and All architectures.

For more information, see Package Types and Architectures.

1.2.3 ZENworks Remote Management

Recording a Remote Management Session: A new session recording icon is added in the viewer toolbar to start the recording of the remove management session. You can view the remote session recordings and download the recording in FBS or MP4 format.

For more information, see Recording a Remote Management Session.

ZENworks Chat: TThe ZENworks Chat feature provides chat capability during a remote session. It allows administrators to communicate with the manage device user on the Remote Management session. It is enabled only when either a Remote Control or a Remote View session is initiated.

For more information, see Managing a Remote View Session.

Reboot Reconnect: If the managed device is shut-down during a remote management session, the viewer will wait for 10 minutes (customizable) for the device to reboot. On successful reboot within the specified time, the viewer session gets reconnected.

For more information, see Reconnecting a session after Reboot.

1.2.4 Mobile Management

Support for Android 13: The ZENworks Agent app version 20.2.1 now supports Android 13.

Android Enterprise App The Android Enterprise App bundle enables you to distribute an app that is available in the Google Play Store. After creating this bundle, assign the bundle to users or devices. On assigning the bundle to a mobile device, the assigned app will be distributed to a device based on the assignment schedule.

For more information, see Distributing Android Enterprise Apps.

1.2.5 Bundle or Policy Management

Show Summary: In the Requirement tab, the Show Summary button is introduced to view the summary of the added filters, which helps administrators to view the applied filter in an equation form.

For more information, see Software Distribution Reference.

Searchability To improve the searchability, in the bundle list page and new filters are introduced for disabled and sandbox bundles.

For more information, see Software Distribution Reference.

Search using GUID: Devices, Bundles, or Policies can be searched using GUID on the respective listing page.

For more information, see Software Distribution Reference.

Summary Page: Bundle and Policy Summary pages include the Original Created Date, the Version Created Date, and the Modified Date. These fields will be updated with month, date, year and time details.

For more information, see Software Distribution Reference.

MSIx The new feature is added to support installing MSIx files on the Windows Agent devices as a bundle action. An MSIx application installer can be created from existing installers such as .exe, .msi, etc., and a valid certificate from a Certificate Authority by using the Microsoft MSIX Packaging tool.

For more information, see Action - Install MSIX.

1.2.6 Advanced Authentication

Introduced multi-factor authentication using Micro Focus NetIQ Advanced Authentication. To enhance security, you can configure advanced authentication while logging into ZENworks Control Center. ZENworks provides a free limited entitlement to Advanced Authentication, which supports the following authentication methods:

- One-Time Password (OTP via Hard or Soft Token)
- SMS OTP
- Email OTP
- RADIUS Client
- Emergency Password
- LDAP Password

NOTE: If required, you can purchase the Full Advanced Authentication from Micro Focus and use all the supported methods.

For more information, see Getting Started with Advance Authentication.

1.2.7 Security Enhancements in ZENworks

Disabling of port 7628 on Primary Server: Port 7628 is disabled on Primary Servers for both Windows and Linux to reduce the attack surface on the primary server.

The following functionalities are achieved via port 7628:

- ZENworks Agent Status on the Device Summary page
- Quick task execution
- Discovery of devices with ZENworks Agent installed

We are now enabling all Quick task Execution and Agent status retrieving for primary servers via ZeUS push notification instead of via port 7628. This is done for both Windows and Linux Primary servers.

Port 80 is Disabled: ZENServer's non-secure port (80) is disabled by default to ensure that the ZENServer communication is over a secure port (443).

HTTP Strict-Transport-Security: HTTP Strict Transport Security (HSTS) is now enabled to protect web application users against some passive and active network attacks.

For more information, see Disabling HTTP Strict Transport Security (HSTS).

Tomcat Split: In ZENworks 2020 Update 3, Tomcat is split into separate instances, client, and administrative services for enhanced system security and management. The administrative service hosts the ZENworks Control Center and all administrative services which are accessed by zman commands. By default, this process runs on the 7443 port. The other Tomcat process hosts client web services, ZENworks End User Portal, and the ZENworks Setup page. By default, this process runs on the 443 port.

For more information, see Configuring an Update.

Satellite Server Support: From ZENworks 2020 Update 3, the Macintosh devices are no longer supported as Satellite Servers.

Dockerisation of Imaging: As part of ZENworks 2020 Update 3 dockerisation of imaging, all the imaging service, log and conf names have been changed from 'novell' to 'micro focus'.

For more information, see Dockerisation of Imaging.

1.3 Patch Management

ZENworks 2020 Update 3 introduces the next generation of patch management. The new ZENworks Patch Management provides:

- Faster patch scanning on endpoints
- A new patch feed with an actively growing patch catalog of operating system and third-party application patches
- Faster support for new platforms and patch content issues
- Use of the new Unified Content Management capabilities to stream patch content to Content Servers as patches are needed (ondemand) rather than pre-replicating the content
- Automated, periodic cleanup of unused patch content from Content Servers
- Improved formatting of patch-related email notifications
- Decreased amount of patch data stored in the ZENworks database
- Same administrative workflows (Patch policies, Remediation deployments, etc.) for managing your day-to-day patching activities

If You Have Never Used ZENworks Patch Management

If you have never activated ZENworks Patch Management in your system, the new patch management is available immediately after installing Update 3. All you need to do is follow the Getting Started instructions on the Security tab of ZENworks Control Center.

If You Have ZENworks Patch Management

If you have previously activated ZENworks Patch Management, you migrate to the new patch management capabilities after installing Update 3. The current patch capabilities remain in place after the system update, giving you time to ensure that the system update has completed successfully on your Primary Servers and Satellites before starting the patch migration.

The patch migration is necessary because of changes in the patch feed and the Patch agent; improvements in the management of the patches in the ZENworks database and content system; and enhanced processing of patch-related data on Primary Servers through the use of a new Patch service. The migration does the following:

1. Cleans up all patch-related database entries.
2. Removes all patch content from Primary Servers and Satellites.
3. Gives you the option of retaining or removing your Patch policies and Patch configuration settings. Please note that the change in patch feeds has resulted in changes to patch names, patch naming conventions, and vendor names. For example, many patch names now include OS build numbers rather than “Windows 10”, “Windows 11”, “Windows Server 2019”, and so forth. If you retain your Patch policies, the policies are disabled during migration until you edit the policy rules to ensure that the criteria provide the results you are expecting.
4. After migration, displays the Getting Started page in ZENworks Control Center to help you configure the new patch system, including starting the new Patch service on all Primary Servers.

If You Are Using Older ZENworks Agents

The new Patch agent is backwards compatible with older ZENworks 2017 and 2020 Agents that meet the following requirements:

- For Windows managed device, .NET Framework 4.8 or newer is installed. Not all Windows operating systems support version 4.8. Please refer to Microsoft’s .NET Framework system requirements article.
- The managed device operating system is supported for patching by ZENworks Patch Management.

We recommend that you upgrade as many managed devices to the ZENworks 2020 Update 3 Agent as possible before migrating. If that is not possible, please consider the following when using older ZENworks Agents:

1. The reboot prompt for Remediation deployments and Patch policies does not display on devices.
2. In ZENworks Control Center on the device Patches page, the “Installed by” field will always show “Other” even when installed by ZENworks.
3. On Windows devices, the new Patch Agent requires Microsoft .NET Framework 4.8 or newer. ZENworks installs .NET 4.8 with the ZENworks 2020 Update 3 Agent if necessary. However, Update 2 and earlier ZENworks Agents only required .NET 4.5. You need to update them to .NET 4.8 for the Patch Agent to work.

If You Are Using the Airgap Solution

An Airgap solution for the new ZENworks Patch Management is not available in this Update 3 release. It will be provided in the next ZENworks release. You need to continue using the current solution until the next release is available.

If You Patch macOS Devices

Please be aware of the following for macOS patching with the new ZENworks Patch Management:

- Both patch detection and remediation for third-party applications works for macOS Intel and macOS Silicon.

- Patch detection for operating systems works for both macOS Intel and macOS Silicon.
- Patch remediation for operating systems DOES NOT work for either macOS Intel or macOS Silicon. This is due to recent changes by Apple that require admin or volume user credentials to be supplied when applying operating system patches. We are currently working on securely providing this capability and expect it to be available within a few months of the Update 3 release. If the current ZENworks Patch Management solution is working for your macOS patching needs, we recommend that you do not migrate to the new solution until we have released the fix.

1.4 ZENworks Endpoint Security Management

The Data Encryption security policy has been removed in this release due to outdated encryption driver technology that is not supported on Windows 10 or later. As previously announced, the Microsoft Data Encryption policy is the replacement for the Data Encryption policy and uses BitLocker encryption technology for removable drive encryption.

During system update, any Data Encryption policies you have created will be deleted from your system resulting in the policies being removed from any managed devices to which they were assigned. If you are still using the Data Encryption policy, **before applying Update 3**, you have the following options:

- Keep the Data Encryption policy assigned to devices and configure and apply the Microsoft Data Encryption policies to those same. The Microsoft Data Encryption policy will take affect over the Data Encryption policy; when a user inserts a removable drive encrypted by the Data Encryption policy, it will be automatically decrypted and re-encrypted with the Microsoft Data Encryption policy. Give users notice that they need to transition all drives before the date you plan on doing your system update.
- Remove the Data Encryption policy and distribute the ZESM Standalone Decryption Utility (**ZCC** > **Home** > **Download ZENworks Tools** > **Endpoint Security**) to users to allow them to decrypt removable drives. For information about using the tool, see File Decryption Utility.

For more information about the Microsoft Data Encryption policy, see Microsoft Data Encryption Policy.

1.5 ZENworks Full Disk Encryption

The Disk Encryption policy has been enhanced to allow you to select the pre-boot authentication method to use with UEFI and legacy BIOS devices. UEFI devices can use a native UEFI app (the default), Linux kernel, or text-based UI. Legacy BIOS devices can use a Linux kernel (default) or text-based UI. Configuration no longer needs to be done through the DMI file and defaults can be set for both firmware types.

Existing policies will continue to use their existing DMI settings but can be reconfigured to use the new settings if desired. New policies can be configured using the new settings during creation.