ZENworks 2017 Update 4 Readme

January 2019

The information in this Readme pertains to the ZENworks 2017 Update 4 release.

- Section 1, “What’s New in ZENworks 2017 Update 4,” on page 1
- Section 2, “Planning to Deploy ZENworks 2017 Update 4,” on page 1
- Section 3, “Downloading and Deploying ZENworks 2017 Update 4,” on page 3
- Section 4, “Issues Resolved in ZENworks 2017 Update 4,” on page 3
- Section 5, “Continuing Issues in ZENworks 2017 Update 4,” on page 3
- Section 6, “Known Issues,” on page 4
- Section 7, “Additional Documentation,” on page 7
- Section 8, “Legal Notice,” on page 7

1 What’s New in ZENworks 2017 Update 4

For information on the new features included in this release, see the ZENworks What’s New Reference.

2 Planning to Deploy ZENworks 2017 Update 4

Use the following guidelines to plan for the deployment of ZENworks 2017 Update 4 in your Management Zone:

- If you are using Disk Encryption and you want to update the Full Disk Encryption Agent from a version earlier than ZENworks 2017 Update 1, you MUST remove the Disk Encryption policy from those managed devices before you update them to ZENworks 2017 Update 4.

  If you are updating the Full Disk Encryption Agent from ZENworks 2017 Update 1 or 2017 Update 2 to ZENworks 2017 Update 4, leave the Disk Encryption policy in place, no change is required prior to the system update.

  For more information about updating Full Disk Encryption in ZENworks 2017 Update 4 from a version earlier than ZENworks 2017 Update 1, see the ZENworks 2017 Update 4 - Full Disk Encryption Update Reference.
- You must first upgrade the Primary Servers, then update the Satellite Servers, and finally the managed devices to ZENworks 2017 Update 4. Do not upgrade the managed devices and Satellite Servers (or add new 2017 Update 4 Agents in the zone) until all Primary Servers in the zone have been upgraded to ZENworks 2017 Update 4.

  NOTE: Agents might receive inconsistent data from the zone until all Primary Servers are upgraded. Therefore, this part of the process should take place in as short a time as possible - ideally, immediately after the first Primary Server is upgraded.
- You can directly deploy version 2017 Update 4 to the following devices:

Device Type	Operating System	Minimum ZENworks Version
Primary Servers	Windows and Linux	ZENworks 2017 and subsequent versions
Satellite Servers	Windows, Linux and Mac	ZENworks 11.x and subsequent versions
Managed Devices	Windows	ZENworks 11.x and subsequent versions
	Linux	ZENworks 11.x and subsequent versions
	Mac	ZENworks 11.2 and subsequent versions

- The system reboots once after you upgrade to ZENworks 2017 Update 4. However, a double reboot will be required in the following scenarios:
  - If you update from 11.x to ZENworks 2017 or a subsequent version (2017 Update 1, Update 2, Update 3 or Update 4) with Endpoint Security enabled, you will need a second reboot to load the ZESNETAccess driver.
  - If a managed device uses Windows 10 with Client Self Defense enabled and you are upgrading from 11.4.x to ZENworks 2017 or a subsequent version (2017 Update1, Update 2, Update 3 or Update 4), you need to disable Client Self Defense in ZENworks Control Center, reboot the managed device, and then run the update, requiring a second reboot on the device.
  - If you have a Disk Encryption policy enforced on a managed device, and you want to update the Full Disk Encryption Agent from a version earlier than ZENworks 2017 Update 1 to ZENworks 2017 Update 4, you must first remove the policy and decrypt the device, which requires a device reboot. You then update the device to 2017 Update 4, requiring a second reboot.

  IMPORTANT: Managed Devices running versions prior to 11.x must first be upgraded to 11.x. The system reboots after the upgrade to 11.x and then reboots again when the ZENworks 2017 Update 4 system update is deployed.

- Prior to installing the System Update, ensure that you have adequate free disk space in the following locations:

Location	Description	Disk Space
Windows: `%zenworks_home%\install\downloads` **Linux:** `opt/novell/zenworks/install/downloads`	To maintain agent packages.	5.7 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	To import the zip file to the content system.	5.7 GB
Agent Cache	To download the applicable System Update contents that are required to update the ZENworks server.	1.5 GB
Location where the System Update file is copied. This is only applicable for the ZENworks Server that is used to import the System Update zip file	To store the downloaded System Update zip file.	5.7 GB

3 Downloading and Deploying ZENworks 2017 Update 4

For instructions on downloading and deploying ZENworks 2017 Update 4, see the *ZENworks System Updates Reference*.

If your Management Zone consists of Primary Servers with a version prior to ZENworks 2017, you can deploy ZENworks 2017 Update 4 to these Primary Servers only after all of them have been upgraded to ZENworks 2017. For instructions, see the *ZENworks Upgrade Guide*.

For administrative tasks, see the ZENworks 2017 Update 4 documentation site.

IMPORTANT: Do not update the Remote Management (RM) viewer until all the Join Proxy Satellite Servers are updated in the zone. To perform Remote Management through Join Proxy, you need to ensure that the RM viewer version and the Join Proxy version are the same.

Ensure that you read Section 2, “Planning to Deploy ZENworks 2017 Update 4,” on page 1 before you download and deploy the ZENworks 2017 Update 4 update.

IMPORTANT: While deploying the ZENworks update, in the Preparing stage, the ZENworks Updater Service (ZeUS) on Primary Servers will be replaced with the new package that is included in the update.

Do not deploy ZENworks 2017 Update 4 until all Primary Servers in the zone have been upgraded to ZENworks 2017

This update requires schema changes to be made to the database. During the initial patch installation, the services will run only on the Master or dedicated Primary Server. This is to ensure that other Primary Servers do not try to access the tables being changed in the database.

After the Master or dedicated Primary Server has been updated, the services will resume on the remaining servers and the update will be applied simultaneously.

NOTE: You do not need to manually stop or start the services on the servers during the update. The services will be stopped and started automatically.

When you postpone a system update and log out of the managed device, the system update is applied on the device.

For the list of supported Managed Device and Satellite Server versions in a Management Zone with ZENworks 2017 Update 4, see Supported Managed Devices and Satellite Server Versions.

4 Issues Resolved in ZENworks 2017 Update 4

Some of the issues identified in previous releases have been addressed in this release. For a list of the resolved issues, see TID 7023612 in the Support Knowledgebase.

5 Continuing Issues in ZENworks 2017 Update 4

Some of the issues that were discovered in versions prior to ZENworks 2017 Update 4 and have not yet been resolved. Review the following Readme documents for more information:

- ZENworks 2017 Readme

- ZENworks 2017 Update 1 Readme
- ZENworks 2017 Update 2 Readme
- ZENworks 2017 Update 3 Readme

6 Known Issues

This section contains information about issues that might occur while you work with ZENworks 2017 Update 4:

- Section 6.1, “Brightness percentage set as a part of the Mobile Device Control policy cannot be applied on Android devices,” on page 4
- Section 6.2, “Direct Boot is not supported on Android P (9.0) devices,” on page 4
- Section 6.3, “Device Keyguard settings do not work on devices where the ZENworks Agent app is upgraded from an earlier version to the 17.4.0. version,” on page 5
- Section 6.4, “Device keyguard settings fails to apply on Android Lollipop and Marshmallow devices enrolled in the work profile mode,” on page 5
- Section 6.5, “Unlock device quick task fails to apply on Android Lollipop and Marshmallow devices enrolled in the work profile mode,” on page 5
- Section 6.6, “After updating ZENworks, the novell-zenworks-xplat-uninstall RPM displays an incorrect version in ZDC,” on page 5
- Section 6.7, “Unwanted Characters in the Intel AMT Devices Folder Name,” on page 5
- Section 6.8, “The Non-Trusted access control rule is not blocking network traffic on devices with the Endpoint Security Firewall Policy enforced,” on page 6
- Section 6.9, “ZENworks Passive Mode login does not work after upgrading to Windows v1709, v1803, or v1809,” on page 6
- Section 6.10, “Quick Tasks and System Updates are Not Executed on ZENworks Agents,” on page 6
- Section 6.11, “The novell-proxydhcp service might not work on RHEL 7.5 and 7.6 imaging satellite server,” on page 7

6.1 Brightness percentage set as a part of the Mobile Device Control policy cannot be applied on Android devices

A Mobile Device Control policy, with a specific brightness percentage value defined in the **Set Brightness Percentage** field, is assigned to an Android work-managed device, then the brightness value does not apply on the device and an error message “App not supported” is displayed in the Policy Status messages.

Workaround: None.

6.2 Direct Boot is not supported on Android P (9.0) devices

As acknowledged by Google, the Direct Boot feature does not work on Android P devices.

Workaround: None.

6.3 Device Keyguard settings do not work on devices where the ZENworks Agent app is upgraded from an earlier version to the 17.4.0. version

When the ZENworks Agent app on a device is upgraded to the 17.4.0 version, the Device Keyguard settings, enabled as part of the assigned Mobile Device Control policy, do not work on the device.

Workaround: Unenroll the device using the **Unenroll** quick task in ZCC and re-enroll it. Re-assign the same Mobile Device Control policy. The Device Keyguard settings will be successfully enabled on the device.

6.4 Device keyguard settings fails to apply on Android Lollipop and Marshmallow devices enrolled in the work profile mode

When the device keyguard settings are enabled as part of the Mobile Device Control Policy, the policy fails to apply on Android Lollipop and Marshmallow devices that are enrolled in the work profile mode. The status of the policy is displayed as failed in ZCC and the error message “You can not set trust agent configuration for a managed profile” is displayed in the device logs.

Workaround: None.

6.5 Unlock device quick task fails to apply on Android Lollipop and Marshmallow devices enrolled in the work profile mode

The Unlock Device quick task fails to apply on Android Lollipop and Marshmallow devices that are enrolled in the work profile mode. The status of the quick task is displayed as failed in ZCC and the error “You cannot reset password for managed profile” is displayed in the device logs.

Workaround: None.

6.6 After updating ZENworks, the novell-zenworks-xplat-uninstall RPM displays an incorrect version in ZDC

After the ZENworks Management Zone is upgraded, the novell-zenworks-xplat-uninstall RPM displays an incorrect version in ZDC.

Workaround: None.

Wait till the refresh action is performed on the Primary Server.

6.7 Unwanted Characters in the Intel AMT Devices Folder Name

In **ZCC** > **Devices** > **Discovered** tab, unwanted characters are displayed in the **Intel AMT Devices** folder name.

Workaround: None.

6.8 The Non-Trusted access control rule is not blocking network traffic on devices with the Endpoint Security Firewall Policy enforced

When an Access Control List (ACL) is configured with one or more Non-Trusted ACL rules in the Firewall Policy, network access based on the rule parameters will not be blocked.

Workaround: Use native Firewall port configurations to block network access.

6.9 ZENworks Passive Mode login does not work after upgrading to Windows v1709, v1803, or v1809

After upgrading the device to Windows 10 v1709 (Fall Creator Update), v1803 or Windows 10 v1809 (April 2018 Update), Passive Mode login to ZENworks does not work.

Workaround: Refer to TID 7022478 in the Micro Focus Knowledgebase.

6.10 Quick Tasks and System Updates are Not Executed on ZENworks Agents

When you assign a quick task or a system update to a ZENworks agent, the assigned task or update are not executed on the agent, and **TaskNotifier, "Got 503 from Server** error is logged in the ZeUS log.

To confirm the "TaskNotifier, "Got 503 from Server" error, perform the following:

1. On the agent, in the Technician Application (Right-click the **ZENworks icon**, select **Technician Application**), the Logging should be set to **Errors, Warning, Info, Debug**.
2. After changing the log level on the agent, assign any quick tasks or a system update.
3. The **TaskNotifier, "Got 503 from Server** error message is logged in the `zeus-messages.log` file (Location: `%ZENWORKS_HOME%\ZeUS\logs\`).

The **TaskNotifier, "Got 503 from Server** error indicates that the server refused the connection as the default capacity (10000) is nearly full.

This error occurs when the number of agents connecting to a server are more, when compared to *maxConnections* count in the `server.xml` file. By default, the *maxConnections* count is 10000.

Solution:

Add the *maxConnections* parameter count in the `server.xml` file.

To add the maxConnections count in the server.xml file:

1. In the following line of the server.xml file, add the parameter maxConnections="20000" as shown below:

   <!-- Define a non-SSL HTTP/1.1 Connector on port 80 --> <Connector acceptCount="1000" connectionTimeout="60000" maxConnections="20000" disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="600" minSpareThreads="25" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol" redirectPort="443" />

NOTE: By default, the parameter maxConnections count is 10000 and will not be listed in the server.xml file. If the count 10000 is not sufficient, then add the parameter and based on the number of agents in the zone increase the count. In this example, maxConnections count is 20000.

2. Restart the ZENworks services.

6.11 The novell-proxydhcp service might not work on RHEL 7.5 and 7.6 imaging satellite server

The *novell-proxydhcp* service might not work on RHEL 7.5 and 7.6, as the port 67 required by *the* service is used by the *dnsmasq* service.

Workaround: Run the `systemctl disable libvirtd.service` command, and then restart the device:

7 Additional Documentation

This document includes information specific to the ZENworks 2017 Update 4 release. For all other ZENworks 2017 documentation, see the *ZENworks 2017 documentation website*.

8 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/.