ZENworks 2017 Update 2 Readme

February 2018

The information in this Readme pertains to the ZENworks 2017 Update 2 release.

1 Important

Prior to installing the update, please read the following information:

- If you have downloaded ZENworks 2017 Update 2 but not deployed it in your zone as yet, ensure that you DO NOT deploy it. Please DELETE ZENworks 2017 Update 2 and only deploy ZENworks 2017 Update 2a to avoid the issue documented in TID 7022612.
- If you have already deployed or are in the process of deploying ZENworks 2017 Update 2, you need to contact customer support or refer to TID 7022612. After taking the required action, you can continue with the deployment of ZENworks 2017 Update 2 and ignore ZENworks 2017 Update 2a.

2 What’s New in ZENworks 2017 Update 2

For information on the new features included in this release, see What’s New in ZENworks 2017 Update 2.

3 Planning to Deploy ZENworks 2017 Update 2

Use the following guidelines to plan for the deployment of ZENworks 2017 Update 2 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 2.

  If you are updating the Full Disk Encryption Agent from ZENworks 2017 Update 1 to Update 2, 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 2 from a version earlier than ZENworks 2017 Update 1, see the ZENworks 2017 Update 1 - 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 2. Do not upgrade the managed devices and Satellite Servers (or add new 2017 Update 2 Agents in the zone) until all Primary Servers in the zone have been upgraded to ZENworks 2017 Update 2.

  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 2 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 2. However, a double reboot will be required in the following scenarios:
  - If you update from 11.x to ZENworks 2017 or 2017 Update 2 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, 2017 Update 1 or 2017 Update 2, 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 2, you must first remove the policy and decrypt the device, which requires a device reboot. You then update the device to 2017 Update 2, 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 2 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.	5.5 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	To import the zip file to the content system.	5.5 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.	5.5 GB

4 Downloading and Deploying ZENworks 2017 Update 2

For instructions on downloading and deploying ZENworks 2017 Update 2, 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 2 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 2 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 3, “Planning to Deploy ZENworks 2017 Update 2,” on page 1 before you download and deploy the ZENworks 2017 Update 2 update.

Do not deploy ZENworks 2017 Update 2 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 2, see Supported Managed Devices and Satellite Server Versions.

5 Issues Resolved in ZENworks 2017 Update 2

Some of the issues identified in previous releases have been addressed in this release. For a list of the resolved issues, see TID 7022513 in the Support Knowledgebase.

6 Continuing Issues in ZENworks 2017 Update 2

Some of the issues that were discovered in versions prior to ZENworks 2017 Update 2 and have not yet been resolved. Review the following Readme documents for more information:

- ZENworks 2017 Readme
- ZENworks 2017 Update 1 Readme

7 Known Issues

This section contains information about issues that might occur while you work with ZENworks 2017 Update 2:

7.1 Issues with the Gmail app installed within the work profile

When the Gmail app is remotely configured on a device enrolled in the work profile mode, using the managed configurations feature, the following issues might occur:

- The app cannot be hidden if the device becomes non-compliant

- Changes made to the managed configuration of the Gmail app are not effective on an enrolled device
- The app does not uninstall automatically when the associated bundle is unassigned

Workaround: None. This is a Google limitation.

7.2 Licenses are not reclaimed when bundles are unassigned and the associated devices do not sync with ZENworks

ZENworks does not reclaim an app license automatically if the associated bundle is unassigned from either of the following:

- A device that does not sync with the ZENworks Server
- A user, and one of the devices associated with the user does not sync with the server. In this case, the license is not reclaimed until all the devices associated with this user sync with the ZENworks Server

Workaround: To reclaim the license, unenroll the device from ZENworks.

7.3 On Windows 10 devices the system update reboot settings for locked devices might not work as configured

As a part of the system update deployment process, even though you uncheck the `Reboot device when the device is locked` option, Windows 10 devices that are locked, might get rebooted after the system update is completed. This issue is related to the Windows 10 native APIs (`OpenInputDesktop` /`SwitchDesktop`), which return random values when the device is locked.

Workaround: None

7.4 SNMP discovery incorrectly identifies the latest Windows operating system as Windows 8.1

Microsoft has deprecated SNMP, so when you perform SNMP discovery from ZENworks, it might detect the latest Windows operating system as Windows 8.1 even if it is a later version.

Workaround: None

7.5 A Windows device with Windows 10 updates might not boot

When you restore the image of a Windows device with Windows 10 updates, using the Legacy NTFS driver, the restored device might not boot the operating system.

Workaround: Perform any one of the following:

- Take and restore an image of the device using the Tuxera driver.
- Take and restore an image of the device in the .zmg format using WinPE.

7.6 Prerequisite check fails on Scientific Linux devices

When you update a Scientific Linux 7.x device with ZENworks 2017 Update 2, the prerequisite check fails.

Workaround: Disable the Remote Management Spoke, and then deploy the update.

7.7 Unable to boot the operating system by selecting the Windows boot manager option from the ZEN partition menu

When secure boot is enabled on the device, and you select the Windows boot manager option from the ZEN partition menu to boot the operating system, the following error message is displayed: *ZENworks is unable to load Windows through ZENPartition. You need to either disable Secure Boot or select Windows Boot Manager from the Boot Menu*.

Workaround: Perform any of the following:

- Reboot the device and select Windows boot manager from the boot menu
- Disable secure boot

7.8 Quick Task status is not updated when proxy is used for Wake on LAN

When a proxy is used to send the Wake on LAN quick task to a managed device, the Quick Task Status dialog box displays a failed message even if the quick task has succeeded.

Workaround: None

7.9 When you run an inventory scan on a Windows 10 device an exception is included in the log file

When you run the full inventory scan on a Windows 10 device, during software collection, the following exception is included in the ZMD message log:

The specified path, file name, or both are too long. The fully qualified file name must be less than 260 characters, and the directory name must be less than 248 characters.

Workaround: In the Windows 10 Local Group Policy Editor, enable the win32 long paths option.

To enable the win32 long paths option on a managed device:

1. Click the Start Menu and enter *gpedit.msc* in the search field.
2. In the Local Group Policy Editor window, go to **Computer Configuration** > **Administrative Templates** > **System** > **Filesystem**
3. In the right pane, double-click **Enable win32 long** paths.
4. In the **Enable win32 long paths** window, select Enabled and then click **OK**.
5. Restart the device.

NOTE: To **Enable win32 long paths** on all managed devices in the zone, in ZCC, create a **Windows Group Policy** to enable win32longpaths and assign it to all the managed devices in the zone.

For more information, see the Windows Group Policy section in the ZENworks Configuration Policies Reference.

7.10 When you edit a domain that is configured with the Microsoft SQL Server database and a resource file you are prompted for a valid port even though the Instance name is specified

If you edit a domain that is configured with the Microsoft SQL server database and a resource file, the `specify a valid port` message is displayed even though the `Instance name` is specified.

Workaround: Delete the `Instance name` and re-enter the `Instance name`.

7.11 ZENworks Passive Mode login fails after reboot or shutdown and restart on Windows 10 devices with the Fall Creators Update

On Windows 10 managed devices with the Fall Creators Update (Build 1709), you will not be logged in passively after performing a reboot or shutdown and restart of the device because the Winlogon Automatic Restart Sign-On (ARSO) is set as Default for user startup.

Workaround: Disable ARSO using a registry or a group policy. If you are not using a policy, a registry bundle can be created to set the registry before assigning it to devices. For more information, see TID 7022379 in the Support Knowledge Base.

7.12 Hard power down of Windows 10 device after updating to Windows 10 version 1709 causes blue screen on devices with Disk Encryption enforced

After upgrading Windows 10 to version 1709 from an earlier version, the user turns off the device using the Power button. When the device is powered on again, it blue screens.This scenario only occurs when Windows 10 cumulative updates are not kept current in Windows 10 versions 1607 and 1703 prior to upgrading to Windows 10 v1709, and only on devices using Disk Encryption. A power down using the Windows menu does not produce this issue.

Workaround: Ensure Windows 10 devices that use Full Disk Encryption are fully patched with Windows updates prior to upgrading to Windows 10 version 1709.

8 Additional Documentation

This Readme lists the issues specific to ZENworks 2017 Update 2 release. For all other ZENworks 2017 documentation, see the *ZENworks 2017 documentation website*.

9 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/.