ZENworks 2020 Update 1 Readme

June 2020

The information in this Readme pertains to the ZENworks 2020 Update 1 release.

What's New in ZENworks 2020 Update 1

For information on the new features included in this release, see What's New in ZENworks 2020 Update 1.

Planning to Deploy ZENworks 2020 Update 1

Use the following guidelines to plan for the deployment of ZENworks 2020 Update 1 in your Management Zone:

- If you are using Disk Encryption on ZENworks 2017 or earlier Full Disk Encryption agents and you want to update those agents to ZENworks 2020 Update 1, there are extra steps you MUST take before updating the ZENworks Agent on those managed devices to ZENworks 2020 Update 1. These steps include decrypting applicable devices, removing and then deleting the pre-17.1 Disk Encryption policy, and deploying a new Disk Encryption policy after updating the ZENworks Agent.

  For comprehensive instructions to update Full Disk Encryption agents from 17.0 or earlier versions, see the *ZENworks 2020 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 2020 Update 1. Do not upgrade the managed devices and Satellite Servers (or add new 2020 Update 1 Agents in the zone) until all Primary Servers in the zone have been upgraded to ZENworks 2020 Update 1.

  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 2020 Update 1 to the following devices:

Device Type	Operating System	Minimum ZENworks Version
Primary Servers	Windows and Linux	ZENworks 2020 and subsequent versions
Satellite Servers	Windows, Linux and Mac	ZENworks 11.3.x and subsequent versions
Managed Devices	Windows	ZENworks 11.3.x and subsequent versions
	Linux	ZENworks 11.3.x and subsequent versions
	Mac	ZENworks 11.3.x and subsequent versions

- The system reboots once after you upgrade to ZENworks 2020 Update 1. However, a double reboot will be required in the following scenarios:
  - If you update from 11.3.x to ZENworks 2020 or a subsequent version (2020 Update 1) 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 2020 or a subsequent version (2020 Update1), 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.

  IMPORTANT: Managed Devices running versions prior to 11.3.x must first be upgraded to 11.3.x. The system reboots after the upgrade to 11.3.x and then reboots again when the ZENworks 2020 Update 1 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.	6.2 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	To import the zip file to the content system.	6.2 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.	6.2 GB

Downloading and Deploying ZENworks 2020 Update 1

For instructions on downloading and deploying ZENworks 2020 Update 1, see the *ZENworks System Updates Reference*.

To use the **Check for Updates** action within ZCC, to view the list of available updates, you need to first re-register the System Update Entitlement by performing the steps detailed in the following section:

Re-registering the System Update Entitlement to activate the ZENworks license

1. Log into ZENworks Control Center (ZCC).
2. Navigate to **Configuration** > **Infrastructure Management** > **System Update Settings**.
3. In the System Update Entitlement section, click the **Configure** link against the **Entitlement State** field.
4. Specify the **Email Address** and the **Activation Code**.

   The Activation Code will be available in the Micro Focus Customer Center under **System Update Entitlement** or **ZENworks Configuration Management Activation Code**.
5. Click **Activate**. After the license is activated, you can view the available system updates in the **System Updates** page by clicking **Actions** > **Check for Updates**.

   For more information, refer to TID 7024521.

If your Management Zone consists of Primary Servers with a version prior to ZENworks 2020, you can deploy ZENworks 2020 Update 1 to these Primary Servers only after all of them have been upgraded to ZENworks 2020. For instructions, see the *ZENworks Upgrade Guide*.

For administrative tasks, see the ZENworks 2020 Update 1 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 "Planning to Deploy ZENworks 2020 Update 1" on page 1 before you download and deploy the ZENworks 2017 Update 1 update.

Do not deploy ZENworks 2020 Update 1 until all Primary Servers in the zone have been upgraded to ZENworks 2020

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 if the update is assigned to all the servers.

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, based on the deployment schedule.

For the list of supported Managed Device and Satellite Server versions in a Management Zone with ZENworks 2017 Update 1, see Supported Managed Devices and Satellite Server Versions.

Issues Resolved in ZENworks 2020 Update 1

Some of the issues identified in previous releases have been addressed in this release. For a list of the resolved issues, see TID 7024523 in the Support Knowledgebase.

Continuing Issues in ZENworks 2020 Update 1

Some of the issues that were discovered in previous versions of ZENworks 2020 Update 1 have not yet been resolved. Review the following Readme documents for more information:

- ZENworks 2020 Readme

Known Issues in ZENworks 2020 Update 1

This section contains information about issues that might occur while you work with ZENworks 2020 Update 1:

ZENworks Patch Management

After upgrading to ZENworks 2020 Update 1 the Deployment Bundle details for custom patches created in versions prior to Update 1 are not displayed in the Patch Relationships tab

After you upgrade to ZENworks 2020 Update 1, for the custom patches created in a previous version of ZENworks, the Deployment Bundle details are not displayed in the Relationships tab of the custom patch.

Workaround: None

There might be a delay in the installation of other bundles when a Patch (vulnerability detection) scan is being performed on refresh

Performing a Patch scan (vulnerability detection) on refresh might take some time and thereby delay the installation of other bundles.

Workaround: As a best practice, it is recommended that you do not perform a Patch scan on refresh.

Patches that are pending download might get stuck in the "Queued" state during a subscription update, if disabled in the patch feed

Patches that are yet to be downloaded might get stuck in the “Queued” state, during a subscription update, if these patches were disabled in the patch feed due to supersedence.

Workaround: Log into ZCC, navigate to Security > Patch Download Details and in the Cache Status pane, click Action > Cancel Pending Downloads.

ZENworks Agent

ZENworks icon display issue on RHEL 8.0 devices

The ZENworks icon is not displayed on the desktop menu bar of RHEL 8.0 devices.

Workaround: None.

YUM Service

Issues with hosting the YUM service on ZENworks Primary Servers

The following issues might be observed while hosting the YUM service:

- If you are hosting the YUM service on a ZENworks 2017 appliance, it might become unusable after it is migrated to ZENworks 2020. Details of all the existing YUM repositories will get deleted and they will have to be re-created, post migration.
- If you are hosting the YUM service on a standalone ZENworks 2017 Linux Primary server, it might become unusable after upgrading it directly (without updating via ZENworks 2017.x) to ZENworks 2020. Details of the YUM repositories will not get deleted, but the YUM service will have to be reconfigured manually.

Workaround: If the YUM service becomes unusable post upgrade, contact Micro Focus Customer Care for information on how to re-configure it correctly.

ZENworks Full Disk Encryption

Single sign-on issues with PBA on managed devices with Windows 7 OS

For security reasons, single sign-on with pre-boot authentication (PBA) might not authenticate the Windows login on some managed devices that have Windows 7 operating systems.

Workaround: The user may need to press Ctrl+Alt+Del within one minute after authenticating with PBA for single sign-on to work. The user can still log in with their Windows credentials if single sign-on is skipped.

Additional partitions not getting encrypted on virtual machines (VM)

The Disk Encryption policy is designed to encrypt “fixed disks” only. For security reasons, additional partitions on VMs might get interpreted as “removable storage” drives if you choose the option to “encrypt all drives” when assigning the Disk Encryption Policy to these devices.

Workaround: Assign VMs with multiple volumes a drive letter in the Disk Encryption Policy configuration using the “Encrypt specific local fixed volumes” option instead of using the “Encrypt all local fixed volumes” option.

ZENworks Endpoint Security

Re-installation of the ZENworks Agent without a reboot may prevent the zeswifi driver from installing

A reboot is required anytime you install or uninstall the ZENworks Agent on a managed device. When installing the ZENworks agent on a device for a second time without a reboot in between, two reboots may be required after re-installation to install the zeswifi driver. Otherwise, you may have issues enforcing the Endpoint Security Wi-Fi Policy.

Vertica

Inconsistent data is displayed in the dashlets when the verticaDBMigrate configure action fails to complete during a system update in a multiple node Vertica cluster environment

During a system update to the ZENworks 2020 Update 1 release, the verticaDBmigrate configure action is run by an Appliance server in which Vertica is enabled. This action is run to migrate new tables from the RDBMS to the Vertica database that is added in the latest release. If there are multiple nodes in the Vertica cluster, then one of the nodes will run this configure action, while the remaining nodes as well as the non-appliance servers will complete the system update. However, if for any reason, the configure action has not completed on the server that is running it, then on accessing the dashlet data from the other servers in which system update is successfully completed, you might see inconsistent data for the new tables in the dashlets. These tables will obtain data from the RDBMS instead of the Vertica database.

Workaround: Manually run the verticaDBmigrate configure action on any of the Appliance servers in which Vertica is enabled. For more information on this configure action, see Migrating Data to Vertica in the *Vertica Reference Guide*.

ZENworks Inventory

Windows 10 20H2 devices are listed as Windows 10 2009 in the Inventory report

In the Inventory report, Windows 10 20H2 devices are listed as Windows 10 2009 devices.

Workaround. None. This issue will be resolved in the next update of ZENworks 2020.

Bundles

The Uninstall RPM action does not work for RHEL 8.x devices

The Uninstall RPM action of Linux bundles does not work on RHEL 8.x devices.

Workaround. None.

Additional Documentation

This Readme lists the issues specific to ZENworks 2020 Update 1 release. For all other ZENworks 2020 Update 1 documentation, see the *ZENworks 2020 documentation website*.

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/.