MICRO FOCUS

Release Notes

ZENworks 2020 Readme

October 2019

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

Readme Updates

The following table contains information on the documentation content changes that were made in this Readme after the initial release of ZENworks 2020:

Table 1 Readme Updates

Date	Readme Item Added or Updated
November 11, 2020	The following Known Issue has been included in the Readme:"Unable to apply ZENworks updates on an Appliance Server" on page 5
October 28, 2019	The following section has been included in the Readme: "Important" on page 2
April 2, 2020	The following known issue has been included in the Readme: "The Check for Updates feature is not working after upgrading to ZENworks 2020" on page 4
June 18, 2020	The following known issue has been included in the Readme: "Issues with enrolling or managing iOS and Android devices after an upgrade to ZENworks 2020" on page 12

Date	Readme Item Added or Updated
15 July, 2020	The following known issue has been included in the Readme: "Zones with wildcard certificates have the following issues:" on page 11
5 August, 2020	The following known issue has been included in the Readme: - "This appliance requires additional disks is displayed as a warning while migrating the Appliance from ZENworks 2017 to ZENworks 2020" on page 6 - "Unable to proceed with appliance migration when zone administrator credentials are specified" on page 5

Important

(Conditional) If you are upgrading from ZENworks 2017 Update 4 FRU1 (17.4.1), and you have downloaded the ZENworks 2020 build prior to 28th October 2019, before proceeding with the upgrade, ensure that you read the following information:

- If you have downloaded ZENworks 2020 but not deployed it in your zone as yet, ensure that you DO NOT deploy it before reading the following TID 7024215.
- If you have already deployed ZENworks 2020 or are in the process of deploying it, you need to contact Micro Focus Customer Center.

NOTE: If you are not upgrading from ZENworks 2017 Update 4 FRU 1 or if you have downloaded the ZENworks 2020 build post 28th October 2019, this information is not applicable to you and you can proceed with the upgrade.

Installation

For installation instructions, see the *ZENworks Server Installation* reference. For system requirements details, see the *ZENworks 2020 System Requirements*.

Upgrade

Planning to Upgrade to ZENworks 2020

Use the following guidelines to plan for the upgrade to ZENworks 2020 in your Management Zone:

- If your zone is using the Sybase database, then upgrading to ZENworks 2020 is a two-step process. You need to first migrate the database and then perform the upgrade. The migration can be performed by using the ZENworks ISO or by using the new Database Migration Utility.
- As part of the upgrade, you must first upgrade the Primary Servers, then update the Satellite Servers, and finally the managed devices to ZENworks 2020. Do not upgrade the managed devices and Satellite Servers (or add new 2020 Agents in the zone) until all Primary Servers in the zone have been upgraded to ZENworks 2020.

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.

- If the managed devices or Satellite Servers have been updated to ZENworks 11.3.x or a later version, you can directly update the managed devices in the zone to ZENworks 2020.

  The system reboots once after you upgrade to ZENworks 2020. However, a double reboot will be required in the following scenarios:

Table 2 *Double Reboot Scenarios*

Scenario	ZENworks Endpoint Security	Full Disk Encryption	Location Services	Client Self Defense
Upgrade from 2017.x to 2020 and fresh Install of ZENworks 2020	Disabled	Disabled	Lite	Enabled
Fresh Install of ZENworks 2020	Disabled	Disabled	Full	Enabled

IMPORTANT: All Primary Servers running ZENworks 11.4.x or earlier should first be upgraded to ZENworks 2017 before upgrading them to ZENworks 2020. Satellite Servers and managed devices should be updated to ZENworks 11.3.x before updating them to ZENworks 2020.

Table 3 *ZENworks Cumulative Agent Update to 2020: Supported Paths*

Device Type	Operating System	Supported Versions	Unsupported Versions
Primary Server	Windows/Linux	v2017 and later versions	Any version prior to 2017
Satellite Server	Windows/Linux/Mac	v11.3.x and later versions	Any version prior to 11.3.x
Managed Device	Windows	v11.3.x and later versions	Any version prior to 11.3.x
	Linux	v11.3.x and later versions	NA
	Mac	v11.3.x and later versions	NA

For detailed information on prerequisites and instructions for upgrading Primary Servers, Satellites, and managed devices to ZENworks see the *ZENworks Upgrade Guide*.

What’s New

For information about the new features in ZENworks 2020, see the *ZENworks What’s New Reference*.

Known Issues

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

- “Installation and Upgrade” on page 4
- “Appliance” on page 4

Installation and Upgrade

Content on ZENworks Installer might not be Displayed Properly

On SLES devices, the text on the ZENworks installer screen might not be displayed properly.

Workaround: Download and install the `fetchmsttfonts` package on the device from the following location: https://software.opensuse.org/package/fetchmsttfonts

The Check for Updates feature is not working after upgrading to ZENworks 2020

After upgrading to ZENworks 2020, when you log into ZENworks Control Center, navigate to the **System Updates** tab, and in the **Available System Updates** panel, click **Action** > **Check for Updates**, an error is displayed.

Workaround: Refer to TID 7024521 in the Micro Focus Knowledgebase.

Agent spokes are disabled when the Suite License option is selected during the ZENworks 2017 (evaluation version) upgrade

While upgrading a ZENworks 2017 server (evaluation version) to ZENworks 2020, if you enable the Suite License option, the agent spokes are disabled and the devices might be rebooted.

Workaround: Within ZCC, navigate to **Configuration** > **Device Management** > **ZENworks Agent**, and enable the required agent features. You can also change the reboot options.

Appliance

Unable to apply ZENworks updates on an Appliance Server

If you migrated a Linux Primary Server to an appliance Server, which does not have the ApplianceServer role, then the system update fails.

Workaround:

- Before importing the system update into the zone, ensure that you add the ApplianceServer role to the server.
- If you have already imported the update, add the ApplianceServer role, retry the Preparing stage, and then apply the updates.
- If you have already upgraded some devices in the zone and the appliance server to which you have migrated the Linux Primary Server, is not upgraded, then contact Micro Focus Customer Support for more information.

To add the ApplianceServer role, perform the following:

Connect to the database and execute the following query:

```
insert into zzenserverroles(id, Roles, position) values
(<GUID>,'ApplianceServer',(select max(position) + 1 from zzenserverroles where id
= <GUID> ));
```

Where <GUID> is the old Primary Server GUID that is being replaced.

Assume e9c2c75196f7dc7bb25e6134b03cfdfd is the GUID of the Primary Server, then depending on the database, specify the GUID as shown below:

- For PostgreSQL: '\xe9c2c75196f7dc7bb25e6134b03cfdfd'
- For MS SQL: 0xe9c2c75196f7dc7bb25e6134b03cfdfd
- For Oracle: 'E9C2C75196F7DC7BB25E6134B03CFDFD'

To confirm if the ApplianceServer role has been added to the server, run the following query: "select * from zzenserverroles where id = <primary server guid>"

Unable to proceed with appliance migration when zone administrator credentials are specified

After migrating the database from Sybase to PostgreSQL, the appliance migration from ZENworks 2017 to ZENworks 2020 fails when you specify the zone administrator username as “administrator”.

Workaround: As the PostgreSQL database is case sensitive and this Migration page requires Zone Administrator username to be case sensitive. Hence, specify the zone administrator username as “**Administrator**” instead of “**administrator**”.

This appliance requires additional disks is displayed as a warning while migrating the Appliance from ZENworks 2017 to ZENworks 2020

During the migration of the appliance from ZENworks 2017 to ZENworks 2020, a warning message is displayed indicating that the appliance requires additional disks, even if the second disk (vastorage) from the ZENworks 2017 appliance is already attached.

Workaround: For workaround steps, see TID 7024440 in the Support Knowledgebase.

Appliance fails to reboot after changing an attached disk

A newly deployed appliance may not boot properly if it has been booted once and then had the vastorage disk changed.

Workaround: Deploy a new appliance from the OVA file and then attach the vastorage disk.

After migrating to ZENworks 2020 Appliance, ZCC username is case sensitive

After migrating to ZENworks 2020 appliance, ZCC username is case sensitive.

Workaround: To make the ZCC username case-insensitive, in the `searchconfig.xml` file, modify the *caseInsensitiveAdminSearch* key to true.

The `searchconfig.xml` file is available in the following location:

- **On Linux:** `/etc/opt/novell/zenworks/datamodel/search/`
- **On Windows:** `%ZENWORKS_HOME%\conf\datamodel\search`

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.

Citrix ICA does not work with XenApp version 7.15

From Citrix XenApp version 7.15, the ZENworks thin client ICA application does not work.The Citrix Receiver that ZENworks uses to launch an ICA app has changed and backward compatibility is not supported.

Workaround: None: This issue is specific to the Citrix product and Citrix has indicated that it will be fixed in a subsequent release.

Bundles

Data displayed in Bundle dashlets might be incorrect or missing if the agent is not updated to ZENworks 2020

In the following scenarios, certain values displayed in the Bundle dashlets are either incorrect or missing:

- In any deployment status dashlet (Distribute, Install or Launch) of a bundle whose parent bundle is assigned to an agent older than the ZENworks 2020 version, the Installing Parent Bundle and Launching Parent Bundle columns do not display any values.
- If you assign a bundle to an agent older than the ZENworks 2020 version and then upgrade the ZENworks Server to the 2020 version, the Assignment Status of the bundle in the Device Assignment status dashlet is displayed as Pending even though the bundle is installed successfully.

Workaround: Update the ZENworks agent to ZENworks 2020.

NOTE: To view valid data across all Bundle dashlets, it is recommended that you update the agents in your zone to ZENworks 2020.

For a disabled bundle, data is not displayed in the Assignment Status dashlet

When a bundle that is assigned to users or devices is disabled, then in the Assignment Status dashlet no data is displayed, even though the assignment exists.

Workaround: None.

Bundle data is not displayed when Install Bundle quick task is executed for iOS or Corporate bundles from a bundle deployment status dashlet

When the **Install Bundle** quick task is executed for an iOS App, iOS Profile, or Corporate bundle, from any one of the bundle deployment status (distribution or install) dashlets, then the data for a device on which the quick task is executed is not displayed in the dashlet.

Workaround:

- For an iOS App bundle, a device refresh will display the updated device data. To refresh the device, you can either execute the **Refresh Device** quick task from the Assignment Status dashlet of the bundle or wait for the scheduled device refresh.
- For an iOS Profile or Corporate bundle, increment the version of the bundle by publishing a new version of the bundle.

Bundle dashlet data might not be up to date if the Vertica database is configured

If you have configured the Vertica database in your zone, the data displayed across Bundle dashlets might not be the latest data.

Workaround: Click the icon to refresh a bundle dashlet. Wait for 10 minutes for the existing RDBMS to sync with Vertica with the latest data. Refresh the dashlet again.

On expanding the Device Assignment Status or User Assignment Status dashlet of a newly assigned bundle, the values for certain filters are not populated

After assigning a bundle to devices or users, when you immediately navigate to the Device Assignment or User Assignment status dashlets and expand it, the following filters do not display any values:

- The **Device Assignment**, **Bundle Assignment**, **Agent Version** and **Operating System** filters in the Device Assignment Status dashlet.
- The **Device Assignment**, **Bundle Assignment**, and **Agent Version** filters in the User Assignment Status dashlet.

Workaround: Collapse the dashlet and expand it again. As a best practice, before expanding the assignment status dashlets of a newly assigned bundle, it is recommended that you click the Refresh Dashlet icon in the collapsed view of the bundle.

Security

- "The CVE patches Not Installed count might be incorrect after you modify the Vendors list in the Subscription Service Content Download page" on page 8
- "In Internet Explorer 11, the scroll might not respond in the CVE Distribution dashlet, if items per page are too many" on page 9
- "Some information in the Device Patches page and the Exploitable Devices pages is not displayed for ZENworks 2017.x agents" on page 9
- "Multi-user encrypted folders may be inaccessible to some users when employing the Microsoft Data Encryption Policy" on page 9
- "Fixed Disk Folder encryption is not supported in this release for folders using Micro Focus Filr" on page 9
- "The Disk Encryption Policy is not encrypting some models of UEFI enabled devices" on page 10

The CVE patches Not Installed count might be incorrect after you modify the Vendors list in the Subscription Service Content Download page

After you modify the number of Vendors selected in the **Subscription Service Content Download** page, and run the CVE and Patch subscriptions, and then click the Vulnerable count in the CVE Severity Distribution or Top CVEs dashlet, the **CVE Patches Not Installed** count might not match the number of patches listed in the **Patches** page.

Workaround: None

In Internet Explorer 11, the scroll might not respond in the CVE Distribution dashlet, if items per page are too many

While using the CVE Distribution dashlet in Internet Explorer 11, if the items per page are 1000, then the page scroll might not respond.

Workaround: Perform any one of the following:

- Use any other ZENworks supported browser.
- Limit the items per page to 25.

Some information in the Device Patches page and the Exploitable Devices pages is not displayed for ZENworks 2017.x agents

After applying a patch on a ZENworks 2017.x device, the Patches page of the device does not display the **Installed On** and **Installed By** information and the Exploitable Devices page does not display the **Remediated On** information.

Workaround: None. This information is not displayed for ZENworks 2017.x agents.

Multi-user encrypted folders may be inaccessible to some users when employing the Microsoft Data Encryption Policy

Multi-user folder encryption is not currently supported when applying the Microsoft Data Encryption Policy on devices with Fixed Disk Folder encryption enabled. If a shared folder is encrypted on a device using this policy feature, only the user logged into the device when the policy is first applied will have access to the files.

Workaround: The following items can be used by the administrator or user to copy and decrypt the folder:

- ZENworks Folder Decryption Tool provided with this release
- Folder encryption certificates created by the policy
- Administrator Decryption Password that was created with the policy

For more information, see “Troubleshooting Endpoint Security” in the *ZENworks Endpoint Security Policies Reference*.

Fixed Disk Folder encryption is not supported in this release for folders using Micro Focus Filr

ZENworks Microsoft Data Encryption policy has an option to encrypt fixed disk folders by managing the Microsoft Encrypting File System (EFS). EFS requires files not be in use during encryption, which prevents encryption of Micro Focus Filr folders because of how Filr manages and controls files. We will look for solutions to this issue in a future release.

The Disk Encryption Policy is not encrypting some models of UEFI enabled devices

When you apply the Disk Encryption policy to UEFI enabled devices, you may see the encryption fail on certain device models due to the device not booting from the Secure Boot option in the boot menu. The policy is designed to make Secure Boot the boot priority in the boot options menu as a requirement for encryption on UEFI enabled devices, but cannot override this configuration on some vendor models when the boot options are locked.

Workaround: Use the applicable option below as a workaround to this issue:

- *Before applying the Disk Encryption Policy:* If a device is not configured for Secure Boot, ensure the boot option lock is disabled, so the policy can change the device to Secure Boot when you enforce the policy.
- *If you have already applied the Disk Encryption Policy:* Disable the boot option lock and change the default boot setting to Secure Boot on applicable devices.

Vertica

- "Kafka will stop syncing data with Vertica when the existing RDBMS is replaced with the RDBMS of another vendor" on page 10
- "Kafka-connect will be unable to auto reconnect to the RDBMS, if the RDBMS is down for more than an hour" on page 10

Kafka will stop syncing data with Vertica when the existing RDBMS is replaced with the RDBMS of another vendor

When you replace the existing RDBMS with that of another vendor (such as replacing PostgreSQL with the Oracle database), the Kafka connectors will stop working and can no longer sync data with the Vertica database.

Workaround: To sync data between the new RDBMS and Vertica, you need to create new connectors, but all existing trending data in the Vertica database will be lost. To create new connectors, execute the bulk data migration configure action with the force option, that is, run the command `novell-zenworks-configure -c VerticaDBMigrate -Doption=force` from the command line utility.

IMPORTANT: This action will replace all the data in Vertica with the data in the new RDBMS due to which all existing trending data will be lost.

Kafka-connect will be unable to auto reconnect to the RDBMS, if the RDBMS is down for more than an hour

If the RDBMS is down for more than an hour, then the kafka-connect service, which is responsible for streaming data between the RDBMS and Kafka, will be unable to connect to the RDBMS.

Workaround: Run the `systemctl restart zenworks-connect.service` command to restart the kafka-connect service.

Remote Management

- “Remote controlling a ZENworks 2017 Update 3 agent with the new viewer displays a blank screen” on page 11

Remote controlling a ZENworks 2017 Update 3 agent with the new viewer displays a blank screen

A blank screen is displayed when you remote control a ZENworks 2017 Update 3 agent using the new Remote Management viewer (experimental support).

Workaround: Uncheck the **Use new Remote Management Viewer** check box to remote control any agent that is not yet upgraded to 17.4 or later.

ZENworks Agent

- “ZENworks icon display issue on SLES 12 SPX and SLES 15 SPX devices” on page 11
- “Zones with wildcard certificates have the following issues:” on page 11

ZENworks icon display issue on SLES 12 SPX and SLES 15 SPX devices

The ZENworks icon is not displayed on the desktop menu bar of SLES 12 SPX and SLES 15 SPX managed devices or Primary Servers. However, when the ZENworks icon is run manually, a message “Another instance of ZENworks icon is running” is displayed.

Workaround: You need to enable the TopIcon Plus extension. Refer to the following steps to install the extension:

1. Specify *https://extensions.gnome.org* in the Firefox browser.
2. Specify **TopIcons Plus** in the **search for extensions** field.
3. Click the link **Click here to install browser extension**.
4. Specify *https://extensions.gnome.org/local/*that will list the installed extensions.
5. Search for the TopIcons Plus extension and enable it.
6. Verify whether the ZENworks icon is displayed in the system tray.

Zones with wildcard certificates have the following issues:

- **Agents on the Linux Primary Servers have empty CSRs:** In a zone with wildcard certificates, the agent on the Linux Primary Server does not list any CSRs.
- **JoinProxy details are not updated on the Linux Primary Server and in ZCC:** In a zone with wildcard certificates, the JoinProxy details are not updated on the Linux Primary servers and while remote controlling a managed device, even if the managed device is connected through JoinProxy, the JoinProxy details are not displayed in ZCC. The `No Primary Server is available to update Joinproxy information into database` message is logged in the `zen-join proxy` log file, and in the Technician Application, the Server status is displayed as `Closest Server not available`.

Workaround: On the agent, run the zac cache-clear command and restart the agent service. For more information on ZAC commands, see ZENworks Command Line Utilities Reference.

Mobile Management

- "Issues with enrolling or managing iOS and Android devices after an upgrade to ZENworks 2020" on page 12

Issues with enrolling or managing iOS and Android devices after an upgrade to ZENworks 2020

After upgrading the zone to the ZENworks 2020 release version, you might face issues while enrolling or managing iOS and Android devices.

Workaround: As the ZENworks MDM server is in the DMZ, ensure that you open the ZooKeeper ports 6789, 6790 and 6791 between the Primary Server on the network and the MDM Server in the DMZ. For more information, you can also refer to the TID 7024455.

Additional Documentation

This Readme lists the issues specific to ZENworks 2020. For all other ZENworks 2020 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/.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.