

# ZENworks 2020 Update 3 Readme

November 2022

The information in this Readme pertains to the ZENworks 2020 Update 3 release:

- ♦ [“Installation” on page 1](#)
- ♦ [“Updating to ZENworks 2020 Update 3” on page 1](#)
- ♦ [“Downloading and Deploying ZENworks 2020 Update 3” on page 3](#)
- ♦ [“What’s New in ZENworks 2020 Update 3” on page 3](#)
- ♦ [“Known Issues in ZENworks 2020 Update 3” on page 4](#)
- ♦ [“Additional Documentation” on page 6](#)
- ♦ [“Legal Notice” on page 7](#)

## Installation

The current release does not support fresh installation. You need to install ZENworks 2020 Update 2 and then update to ZENworks 2020 Update 3.

## Updating to ZENworks 2020 Update 3

To update to ZENworks 2020 Update 3, ensure that your zone is in ZENworks 2020 Update 2.

Use the following guidelines to plan for the deployment of ZENworks 2020 Update 3 in your Management Zone:

- ♦ If you are using Disk Encryption on ZENworks 2020 or earlier Full Disk Encryption agents and you want to update those agents to ZENworks 2020 Update 3, there are extra steps you **MUST** take before updating the ZENworks Agent on those managed devices to ZENworks 2020 Update 3. 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 3 - Full Disk Encryption Update Reference](#).

- ♦ You must first update the Primary Servers, then update the Satellites, and finally update the managed devices to ZENworks 2020 Update 3. Do not update the managed devices and Satellites (or add new 2020 Update 3 managed devices in the zone) until all Primary Servers in the zone have been updated to ZENworks 2020 Update 3.

**NOTE:** Agents might receive inconsistent data from the zone until all Primary Servers are updated. Therefore, this part of the process should take place in as short a time as possible - ideally, immediately after the first Primary Server is updated.

- ♦ You can directly deploy version 2020 Update 3 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 3. 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 2 or 2020 Update 3) 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 Update 2 or 2020 Update 3), 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 3 system update is deployed.

- ♦ Prior to updating the System Update, ensure that you have a minimum of 50 GB of disk space to download and deploy the update. The table lists the free disk space required in the following locations:

| Location   | Description  | Disk Space |
|--|--|------------|
| <b>Windows:</b> %zenserver_home%\install\downloads<br><b>Linux:</b> opt/microfocus/zenworks/install/downloads                                      | To maintain agent packages.  | 14 GB      |
| <b>Windows:</b> %zenserver_home%\work\content-repo<br><b>Linux:</b> /var/opt/microfocus/zenworks/content-repo                                      | To import the zip file to the content system.  | 14 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.  | 14 GB      |

# Downloading and Deploying ZENworks 2020 Update 3

For instructions on downloading system update files from SDL, see [Manually Download Updates from Software and Licenses Download \(SLD\)](#) and for deploying to ZENworks 2020 Update 3, see [Deploying Updates](#).

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 administrative tasks, see the [ZENworks 2020 Update 3](#) 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 [“Updating to ZENworks 2020 Update 3” on page 1](#) before you download and deploy the ZENworks update.

## Do not deploy ZENworks 2020 Update 3 until all Primary Servers in the zone have been upgraded to ZENworks 2020 Update 2.

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.

## What's New in ZENworks 2020 Update 3

For information on the new features in ZENworks 2020 Update 3, see the [ZENworks What's New Reference](#).

# Known Issues in ZENworks 2020 Update 3

This section contains information about issues that might occur while you work with ZENworks 2020 Update 3:

- ♦ [“Unable to Upgrade to ZENworks 2020 Update 3 as the Server Certificate is missing Subject Alternative Name” on page 4](#)
- ♦ [“A registered Mac Intel device displays ARM details” on page 5](#)
- ♦ [“While updating ZENworks, HTTP 500 internal error might be displayed” on page 5](#)
- ♦ [“System Update might fail on Linux Primary Server during the Prepare stage” on page 5](#)
- ♦ [“While updating ZENworks, the request method POST not supported error might be displayed” on page 5](#)
- ♦ [“Patch settings are hidden even after activating the Patch Management license” on page 5](#)
- ♦ [“Patches are not populated on agents after migration to the new Patch Management system” on page 6](#)
- ♦ [“Content Download fails with Yum-repo using a non-SSL URL” on page 6](#)
- ♦ [“Blackedout Schedule Is Not Supported for Ondemand Cached Content” on page 6](#)
- ♦ [“An exception was displayed when backing up ZENworks Primary Server” on page 6](#)

## Unable to Upgrade to ZENworks 2020 Update 3 as the Server Certificate is missing Subject Alternative Name

If the server certificate has CN as an IP address and the Subject Alternative Names (SAN) do not include an IP address, the upgrade might fail during the prepare stage. Ensure that the value of SAN includes the IP address also.

The following exception is logged in the loader-messages.log file:

```
java.security.cert.CertificateException: No subject alternative names present
    at sun.security.util.HostnameChecker.matchIP(HostnameChecker.java:160)
    at sun.security.util.HostnameChecker.match(HostnameChecker.java:104)
    at
sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:457)
    at
sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:431)
    at
sun.security.ssl.AbstractTrustManagerWrapper.checkAdditionalTrust(SSLContextImpl.java:1290)
    at
sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:1257)
    at
sun.security.ssl.CertificateMessage$T12CertificateConsumer.checkServerCerts(CertificateMessage.java:638)
```

**Workaround:** Remint the server certificate before initiating the upgrade.

## A registered Mac Intel device displays ARM details

In ZENworks 2020 Update 3, after migrating to the new patch feed, a registered Mac device with an Intel processor displays ARM patch information, after performing the patch maintenance.

Workaround: None

## While updating ZENworks, HTTP 500 internal error might be displayed

As part of System Update deployment, during the Configure Update phase, the HTTP 500 internal error might be displayed while configuring a new port for ZENworks Control Center.

**Workaround:**

- ♦ **On Windows:** Restart the ZENworks Updater Service (ZeUS) and continue with the update process.
- ♦ **On Linux:** Restart the service by running the `systemctl restart novell-zenworks-updater-service.service` command and continue with the update process.

This step is recommended to be followed for all Linux and Appliance primary servers in the zone.

## System Update might fail on Linux Primary Server during the Prepare stage

While deploying System Update on Linux Primary Server, the update fails during the Prepare stage, and the following error message is logged in loader-messages.log:

```
/opt/microfocus/zenworks/bin/run_preglobal_update:: OUT: FINE: Failed to Copy File Due to Exception :  
java.io.IOException: Destination '/var/opt/novell/zenworks/ZeUS/work/prepare/<system_update_guid>/  
webapps' directory cannot be created
```

Workaround: Run `permission.sh` and retry prepare on the server.

## While updating ZENworks, the request method POST not supported error might be displayed

As part of System Update deployment, during the Configure Update phase, the following error might be displayed while configuring a new port for ZENworks Control Center:

**HTTP ERROR 405 Request method POST not supported**

Workaround: Ignore the error and continue with the update process.

## Patch settings are hidden even after activating the Patch Management license

Some of the patch-related settings are hidden even after successfully activating the Patch Management license.

This might happen only when the administrator deactivates Patch Management and then reactivates Patch Management in the evaluation mode or by providing a key.

Workaround: After activating the license, log out and re-login to ZCC.

## Patches are not populated on agents after migration to the new Patch Management system

After updating to ZENworks 2020 Update 3, and migrating to the new Patch Management system, patches are not populated on the devices, and the following exception is logged in the patch-management.log file on the server:

*plr files fails to process with "patchsuperseded" violates foreign key constraint  
"fk\_patchsuperseded\_oldpatchid" exception*

The device GUID on which the issue is observed can be found right after the above exception message.

One of the reasons might be because the Patch Management is reset.

Workaround: On the agent, delete the scanstatus.json file available in the following location, and then run `zac ps`.

- On Linux: `/opt/novell/zenworks/zpm` directory
- On Windows: `%zenworks_home%\zpm`

## Content Download fails with Yum-repo using a non-SSL URL

After updating to ZENworks 2020 Update 3, when you create the Yum service for a Linux bundle, the content download fails, as a non-SSL URL is being used.

Workaround: Ensure that you use URLs with `"https"` instead of `"http"`.

## Blackouted Schedule Is Not Supported for Ondemand Cached Content

In ZENworks 2020 Update 3, the Blackouted schedule for the Ondemand cached content is not supported. Content that is already cached as part of Ondemand request and when it is served to managed devices from its local cache again, in this scenario, the blackouted schedule is not supported.

Workaround: None

## An exception was displayed when backing up ZENworks Primary Server

When trying to backup the ZENworks Primary Server on Windows by running the `zen-backup-restore.bat mode=backup file="C:\Program Files (x86)\Micro Focus\ZENworks\backup"` command, an `IOException` message was found in the log file.

Workaround: None

## Additional Documentation

This Readme lists the issues specific to ZENworks 2020 Update 3 release. For all other ZENworks related documentation, see the [ZENworks documentation site](#).

# 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.microfocus.com/en-us/legal>).

**© Copyright 2008 - 2022 Micro Focus or one of its affiliates.**

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.

