

# ZENworks 2020 Update 2 Readme

August 2021

The information in this Readme pertains to the ZENworks 2020 Update 2 release.

- ♦ [“What’s New” on page 1](#)
- ♦ [“Planning to Deploy ZENworks 2020 Update 2” on page 1](#)
- ♦ [“Downloading and Deploying ZENworks 2020 Update 2” on page 3](#)
- ♦ [“Continuing Issues in ZENworks 2020 Update 2” on page 3](#)
- ♦ [“Known Issues in ZENworks 2020 Update 2” on page 4](#)
- ♦ [“Additional Documentation” on page 6](#)
- ♦ [“Legal Notice” on page 6](#)

## What’s New

For information on the new features in ZENworks 2020 Update 2, see the [What’s New in ZENworks 2020 Update 2](#).

## Planning to Deploy ZENworks 2020 Update 2

Use the following guidelines to plan for the deployment of ZENworks 2020 Update 2 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 2, there are extra steps you **MUST** take before updating the ZENworks Agent on those managed devices to ZENworks 2020 Update 2. 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 upgrade the Primary Servers, then update the Satellite Servers, and finally the managed devices to ZENworks 2020 Update 2. Do not upgrade the managed devices and Satellite Servers (or add new 2020 Update 2 Agents in the zone) until all Primary Servers in the zone have been upgraded to ZENworks 2020 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 2020 Update 2 to the following devices:

**Table 1** ZENworks Cumulative Update to 2020 Update 2: Supported Paths

Device Type	Operating System	Supported Versions	Unsupported Versions
Primary Server	Windows/Linux	V2020 and 2020 Update 1	Any version prior to 2017 and 2017 Update x
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

- ♦ The system reboots once after you upgrade to ZENworks 2020 Update 2. 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 or 2020 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 2020 or a subsequent version (2020 Update 1 or 2020 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.

**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 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
<b>Windows:</b> %zenworks_home%\install\downloads <b>Linux:</b> opt/novell/zenworks/install/downloads	To maintain agent packages.	6.2 GB
<b>Windows:</b> %zenworks_home%\work\content-repo <b>Linux:</b> /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 2

For instructions on downloading and deploying ZENworks 2020 Update 2, 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:

If your Management Zone consists of Primary Servers with a version prior to ZENworks 2020, you can deploy ZENworks 2020 Update 2 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 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 [“Planning to Deploy ZENworks 2020 Update 2” on page 1](#) before you download and deploy the ZENworks 2017 Update 1 update.

**Do not deploy ZENworks 2020 Update 2 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](#).

---

**NOTE:** If you have deployed ZENworks 2020 Update 2 Lighthouse Appliance build on Microsoft Hyper-V, XEN on SLES, or Citrix XenServer and want to update to the ZENworks 2020 Update 2 FCS build, please contact Micro Focus Customer Support, and then perform the steps mentioned in the [Updating the ZENworks 2020 Update 2 Lighthouse build to ZENworks 2020 Update 2 FCS](#)

---

## Continuing Issues in ZENworks 2020 Update 2

Some of the issues that were discovered in prior versions of ZENworks 2020 Update 2 have not yet been resolved. Review the following Readme documents for more information:

- ♦ [ZENworks 2020 Update 1 Readme](#)

# Known Issues in ZENworks 2020 Update 2

This section contains information about issues that might occur while you work with ZENworks 2020 Update 2:

- ♦ [“ZENworks 2020 Update 1 is listed after installing or upgrading to ZENworks 2020 Update 2 or later Version” on page 4](#)
- ♦ [“Unregistering a device object that is enrolled via ZENAgent and MDM will not delete the device object from ZCC” on page 4](#)
- ♦ [“xenstored.service fails during reboot” on page 4](#)
- ♦ [“The Antimalware Tab Does Not Display Data for MDM Devices” on page 5](#)
- ♦ [“Install or Upgrade on a Linux Primary Server Completes with a Warning and ZCC is not accessible” on page 5](#)
- ♦ [“Unable to Deploy an Appliance on VMware vSphere” on page 5](#)
- ♦ [“After migrating the appliance, an error is logged in the sshd.service status file” on page 5](#)
- ♦ [“Ondemand content is not downloaded from the Antimalware Cloud Server to ZENworks OCM Primary Servers with IPv6” on page 6](#)
- ♦ [“Network scan with invalid credentials incorrectly displays a successful scan on the Antimalware Agent” on page 6](#)

## ZENworks 2020 Update 1 is listed after installing or upgrading to ZENworks 2020 Update 2 or later Version

When you install or upgrade to ZENworks 2020 Update 2 or later version, and configure the System Update entitlement and check for the updates in the System Updated page, then ZENworks 2020 Update 1 will be displayed.

**Workaround:** Ignore the listed updated (ZENworks 2020 Update 1).

## Unregistering a device object that is enrolled via ZENAgent and MDM will not delete the device object from ZCC

When you try to unregister a device object that is enrolled via ZENAgent and MDM using the `zac unr -f` command, the device object will unregister locally but is not deleted from ZCC and the MDM device remains unchanged.

**Workaround:** None

## xenstored.service fails during reboot

After deploying an appliance on Citrix XenCenter (using the `xva.tar.gz` file), the `xenstored.service` fails to start during the boot process. However, the `xenstored.service` will eventually start and run with all services.

**Workaround:** None

## The Antimalware Tab Does Not Display Data for MDM Devices

As the Antimalware agent is installed only on the ZENworks Agent, the MDM enrolled devices do not display any data in the Antimalware tab.

Workaround: None

## Install or Upgrade on a Linux Primary Server Completes with a Warning and ZCC is not accessible

When you install or upgrade to ZENworks 2020 Update 2 on a Linux Primary Server, you may see a warning that some of the services are not running. Additionally, you may not be able to access ZCC. This might be because the ZENworks Server service takes time to start after install or upgrade.

**Workaround:** Retry accessing ZCC after a few minutes. If the issue persists after an hour of installing or upgrading the primary server, please contact Micro Focus Customer Center.

## Unable to Deploy an Appliance on VMware vSphere

Deploying the ZENworks Appliance on VMware vSphere 6.7 fails with a *"TypeError: Cannot read property 'keyValue' of undefined"* error.

**Workaround:** Perform the following steps:

1. Download the embedded host client from the following link:  
<https://flings.vmware.com/esxi-embedded-host-client>
2. Upload the downloaded VIB file into the datastore, and then install the file using the following command:  
[root@ESXI~] esxcli software vib install -v /vmfs/volumes/<your\_datastore>/esxui-signed-12086396.vib
3. After successfully installing the VIB, restart the appliance deployment.

## After migrating the appliance, an error is logged in the sshd.service status file

After restarting the sshd.services on the migrated appliance, the sshd.service status will log the following error:

```
Could not load host key: /etc/ssh/ssh_host_dsa_key
```

```
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=  
rhost=<appliance_server_IP> user=root
```

**Workaround:** To restart the sshd.service without errors, take a back up of /etc/ssh/sshd\_config and copy the sshd\_config file from the build to the /etc/ssh location.

The attached sshd\_config file will enable the rsa, ecdsa and ed25519 hostkeys , will retain the disabled dsa keys as is and will increase the size of KexDHMin and ServerKeyBits from 1024 to 2048.

## Ondemand content is not downloaded from the Antimalware Cloud Server to ZENworks OCM Primary Servers with IPv6

ZENworks primary servers using IPv6 and configured as ondemand content masters (OCM) are not getting content downloaded from the Antimalware Cloud Server. This content is required to keep malware definitions and the Antimalware Agent current on devices that have ZENworks Antimalware enforced.

**Workaround:** ZENworks Antimalware must be deployed on a network using IPv4 communications.

## Network scan with invalid credentials incorrectly displays a successful scan on the Antimalware Agent

If the Antimalware Network Scan Policy is created using invalid network credentials, the Antimalware Agent will show a successful scan at the scheduled scan time in the Agent Status Console on devices that have the policy assigned, even though the scan does not actually occur.

**Workaround:** Ensure you create the policy with valid network credentials, so the policy's targets can be scanned.

## Additional Documentation

This Readme lists the issues specific to ZENworks 2020 Update 2. For all other ZENworks 2020 Update 2 documentation, see the [ZENworks 2020 Update 2 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/>.

© Copyright 2008 - 2021 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.