System Update (11.4.3) for ZENworks 11 SP4 Readme

October 2016

Novell

The information in this Readme pertains to the 11.4.3 system update for ZENworks 11 SP4.

1 Important Reasons to Update to ZENworks 11.4.3

Some of the important issues that were observed in previous releases and fixed in this release are:

- The new Change Password feature enables you to change the directory or local Windows password using the ZENworks icon. This feature is supported only for eDirectory users.
- The Calculation of Primary Users on the agents has been enhanced. This feature enables you to reset the Primary User Calculation based on the number of logins and specific dates.
- Removed the dependency of Mirage drivers on ZENworks for smooth migration and upgrade to the Windows 10 anniversary update.
- The SuSE Subscription failure issue has been resolved by including support for new fields introduced by SuSE.
- ZENworks regularly removes data that is unnecessary and older than 7 days. However, in previous releases, this data was not cleared due to various issues. These issues have been addressed in this release. For more information, see TID 7018246 in the Novell Support Knowledgebase.
- Issue while downloading the System Update from Primary WAN bypassing the Satellite Server has been addressed.

2 Planning to Deploy Version 11.4.3

Use the following guidelines to plan for the deployment of ZENworks 11.4.3 in your Management Zone:

- Apply the pre-requisite update “Post 11SP4 Update Prereq” to the ZENworks 11 SP4 servers before upgrading to ZENworks 11.4.3. However, if the server is already upgraded to the ZENworks 11.4.1 or 11.4.2 version, then this pre-requisite update need not be applied.

- If you are using Full Disk Encryption on OPAL drives in native hardware-encryption mode (no software encryption applied), you MUST remove the Disk Encryption policy from those managed devices before you update them to ZENworks 11.4.3.

  If you are using software encryption with OPAL drives (via the *Enable software encryption of OPAL compliant self-encrypting drives* setting in the policy), you DO NOT need to remove the policy before updating the managed devices.

- The system reboots once after you upgrade to ZENworks 11.4.3. The reboot is applicable only for Windows devices. However, a double reboot is required in the following scenarios:

Table 1 *Double Reboot Scenarios*

Scenario	ZENworks Endpoint Security	Full Disk Encryption	Location Services	Client Self Defense
Upgrade from 10.3.4 or above to 11.4.3	Disabled	Disabled	Lite	Enabled
Fresh Install of 11.4.3	Disabled	Disabled	Lite / Full	Enabled

IMPORTANT: Any managed device running versions prior to 10.3.4 must first be upgraded to ZENworks 10.3.4 or a subsequent version.

The system reboots after the upgrade to ZENworks 10.3.4 and then reboots again when the 11.4.3 update is deployed.

Table 2 *ZENworks Cumulative Agent Update to 11.4.3: Supported Paths*

Managed Device Type	Operating System	Supported Versions	Unsupported Versions
Primary Server	Windows/Linux	v11.4.*x*	Any version prior to v11.4.x
Satellite Server	Windows/Linux/Mac	v10.3.4 and subsequent versions	Any version prior to v10.3.4
Managed Device	Windows	v10.3.4 and subsequent versions	Any version prior to v10.3.4
	Linux	v11.0 and subsequent versions	NA
	Mac	v11.2 and subsequent versions	NA

- 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`	To maintain agent packages.	5 GB
Linux: `opt/novell/zenworks/install/downloads`		

Location	Description	Disk Space
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	To import the zip file to the content system.	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 GB

- You must deploy version 11.4.3 first to the Primary Servers, then to the Satellite Servers, and finally to the managed devices. Do not deploy this update to managed devices and Satellite Servers (or deploy new 11.4.3 Agents in the zone) until all Primary Servers in the zone have been upgraded to 11.4.3.

  NOTE: When the agents start communicating with the ZENworks servers before the Primary Servers are upgraded, the agents receive inconsistent data that might impact the zone. Therefore, the Primary Servers should be upgraded within a short duration, ideally within few minutes of each other.

- The Update For ZENworks 11 SP4 (11.4.3) supercedes ZENworks 11.4.1 and 11.4.2.
- You can directly deploy ZENworks 11.4.3 to Satellite Servers and managed devices that have ZENworks 10.3.4 or a subsequent version installed.
- If updating on a Windows 10 operating system or a Windows server with Agent Self Defense enabled, the feature must be disabled before the update. See:
  - Section 7.3, “System update to ZENworks 11.4.3 from an earlier ZENworks version fails on a Windows 10 device,” on page 5
  - Section 7.7, “Blue screen failure occurs on Windows servers during updates,” on page 6

3 Downloading and Deploying Version 11.4.3

For instructions on downloading and deploying version 11.4.3 as an update, see the *ZENworks 11 SP4 System Updates Reference*.

If your Management Zone consists of Primary Servers with a version prior to ZENworks 11 SP4, you can deploy ZENworks 11.4.3 to these Primary Servers only after all of them have been upgraded to ZENworks 11 SP4 and the “Post 11SP4 Update Prereq” has been applied to all these servers. For instructions, see the *ZENworks 11 SP4 Upgrade Guide*.

NOTE: If the ZENworks 11.4.1 or 11.4.2 version is already deployed on the Primary Servers, then the pre-requisite update need not be applied to deploy ZENworks 11.4.3 on the Primary Server.

Since there are no updates to ZENworks Patch Management, the version is displayed as 11.4.2 in the configuration page.

For information about the Post 11SP4 Update Prereq, see Post ZENworks 11 SP4 Update Prerequisites.

For administrative tasks, see the Novell ZENworks documentation website (https://www.novell.com/documentation/zenworks114/).

September 2016 PRU (version 3.6.A.16) has been base-lined as part of 11.4.3 release.

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 2, “Planning to Deploy Version 11.4.3,” on page 1 before you download and deploy the 11.4.3 update.

Do not deploy ZENworks 11.4.3 until all Primary Servers in the zone have been upgraded to ZENworks 11 SP4

This update requires schema changes to be made to the database. Only one Primary Server should have its services running during the initial patch installation so 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 remaining servers can start their services and apply the update simultaneously.

When you postpone a system update and log out of the managed device, the system update is applied on the device. Prior to ZENworks 11.4.3, in the same scenario, the system update would get aborted.

For the list of supported Managed Device and Satellite Server versions in a Management Zone with 11.4.3, see Managed Device and Satellite Version Support Matrix.

4 Windows Secure Boot

Secure Boot is a Windows feature that can be enabled in Windows devices that have UEFI firmware. Support for Secure Boot in ZENworks 11 SP4 has the limitations described below:

Endpoint Security Management and Location Awareness: If Endpoint Security Management or Location Awareness are enabled in your zone, make sure that Secure Boot is disabled on devices before performing a new installation of the ZENworks Agent. You do not need to do this when updating an existing ZENworks Agent on a device.

Full Disk Encryption: UEFI firmware, and by extension Windows Secure Boot are not supported for Full Disk Encryption.

5 Issues Resolved in Version 11.4.3

Some of the issues identified in previous releases have been addressed in this release. For a list of the resolved issues, see TID 7017820 in the Novell Support Knowledgebase.

6 Continuing Issues in ZENworks 11.4.3

Some of the issues that were discovered in previous versions of ZENworks 11 SP4 have not yet been resolved. Review the following Readme documents for more information:

- ZENworks 11 SP4 Readme
- System Update (11.4.1) for ZENworks 11 SP4 Readme
- System Update (11.4.2) for ZENworks 11 SP4 Readme

7 Known Issues in Version 11.4.3

7.1 ZEUS fails to apply the System Update, if the Agent TrustStore contains a different root Certificate Authority in the Windows Primary Servers.

When you migrate to a new hardware by installing new Primary Servers with the same DNS name. ZEUS picks the certificate with the highest expiry date from the list of matched certificates and saves it in the TrustStore. So, the certificate with the nearest expiry date or expired is replaced with reminted certificates.

Workaround Ensure only a valid Certificate Authority is available in the TrustStore, and delete the existing certificates in the new Primary Servers.

7.2 Zicon is not visible after installing or updating ZENworks on Macintosh 10.9.x or earlier device

When you install the 11.4.3 agent or apply the 11.4.3 system update on devices running Macintosh 10.9.x or earlier versions, Zicon is not visible.

Workaround: Open the terminal and execute the following commands:

- `launchctl unload /Library/LaunchAgents/com.novell.zenworks.zicon.plist`
- `launchctl load /Library/LaunchAgents/com.novell.zenworks.zicon.plist`

7.3 System update to ZENworks 11.4.3 from an earlier ZENworks version fails on a Windows 10 device

When you update ZENworks to 11.4.3 on a Windows 10 device, if Agent Self Defense is enabled in ZENworks Control Center, the system update might fail with the following error:

There was an error while installing package setup.exe. MSI return code: 1603. Check the system-update.log on the device for details.

Workaround: Disable *ZENworks Agent Self Defense*, and then reboot the Windows 10 device before updating to ZENworks 11.4.3. After the system update is complete, you can re-enable *Agent Self Defense*.

7.4 RHEL IOA devices are not updated to 11.4.3

When you upgrade RHEL IOA devices on which SELinux is enabled, to ZENworks 11.4.3, the devices are not updated.

Workaround: Before upgrading the RHEL IOA devices, disable SELinux by performing any one of the following:

- To temporarily disable SELinux, type the `echo 0 >/selinux/enforce` command in the terminal as a root user.
- To permanently disable SELinux navigate to the `etc/selinux/config` file as a root user and modify the value of the SELINUX parameter to disable, and restart the device for changes to take effect.

7.5 Check Disk might run on a device with the Windows 10 Anniversary update installed

When you take or restore an image of a device with Windows 10 Anniversary update installed using a Legacy NTFS Driver, Check Disk might run while booting the operating system after restoring the image.

Workaround: Take or restore an image of a device using Tuxera driver.

7.6 Zicon is not visible on a fresh installation of the 11.4.3 agent on SLE 12 SP1

During a fresh installation of the ZENworks 11.4.3 agent on a SLE 12 SP1 device, the Zicon is not visible.

Workaround: Log out and log in to the agent.

7.7 Blue screen failure occurs on Windows servers during updates

Blue screen failures occur on Windows servers during Windows or ZENworks updates following reboot. This issue occurs when Agent Self Dense is enabled on the server.

Workaround: Before running any updates on Windows servers, navigate to the Servers folder and disable *Agent Self Defense* on the servers via *Servers (Details)*.

For help, see Modifying Configuration Settings on a Folder in the ZENworks Management Zone Setting Reference.

NOTE: Agent Self Defense is designed for ZENworks Endpoint Security Management on endpoint devices. Leaving Agent Self Defense disabled on all server devices is strongly recommended.

7.8 Only one volume is allowed to decrypt when using the ERD for multiple encrypted volumes

This issue occurs on devices with Windows x86 32 operating systems when Emergency Recovery Information (ERI) files are created before the device reboots. The option to decrypt additional volumes is not enabled on devices during decryption when a Disk Encryption policy is applied.

Workaround: See “Only one volume is allowed to decrypt when using the ERD for multiple encrypted volumes” in the *ZENworks 11 SP4 Troubleshooting Full Disk Encryption* reference.

7.9 ZENworks 11.4.3 update fails on SLES 12 SP1 Primary Servers

System update fails when you apply the ZENworks 11.4.3 update to SLES 12 SP1 servers.

Workaround: On the SLES 12 SP1 server, edit the `/etc/os-release` file and change the version_ID from 12.1 to 12. After applying the update, revert the version_ID.

8 Legal Notices

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/.