

The information in this Readme pertains to the Novell ZENworks 11 Support Pack 4 release.

- ♦ [Section 1, "Installation," on page 1](#)
- ♦ [Section 2, "Planning to Upgrade to ZENworks 11 SP4," on page 1](#)
- ♦ [Section 3, "Upgrade," on page 2](#)
- ♦ [Section 4, "What's New," on page 2](#)
- ♦ [Section 5, "ZENworks Reporting," on page 2](#)
- ♦ [Section 6, "Known Issues," on page 3](#)
- ♦ [Section 7, "Additional Documentation," on page 15](#)
- ♦ [Section 8, "Legal Notices," on page 15](#)

1 Installation

For system requirements and installation instructions, see the [ZENworks 11 SP4 Server Installation Guide](#).

IMPORTANT

- ♦ Disable IPv6 on your device before installing ZENworks 11 SP4. The IPv6 for ZENworks 11 SP4 is not supported.
 - ♦ The `libXtst6-32bit-1.2.2-3.60.x86_64.rpm` is required if you are using SUSE Linux Enterprise Server 12 to install ZENworks 11 SP4.
 - ♦ ZENworks Agent installation using Yast Add-on is not supported for SUSE Linux Enterprise Server 12.
-

2 Planning to Upgrade to ZENworks 11 SP4

Use the following guidelines to plan for the upgrade to ZENworks 11 SP4 in your Management Zone:

- ♦ You must first upgrade the Primary Servers, then update the Satellite Servers, and finally the managed devices to ZENworks 11 SP4. Do not upgrade the managed devices and Satellite Servers (or add new 11 SP4 Agents in the zone) until all Primary Servers in the zone have been upgraded to 11SP4.

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 have been updated to ZENworks 10.3.4 or later, you can directly update the managed devices in the zone to ZENworks 11 SP4.

The system reboots once after you upgrade to ZENworks 11 SP4. However, a double reboot will be 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 to 11 SP4	Disabled	Disabled	Lite	Enabled
Fresh Install of 11 SP4	Disabled	Disabled	Lite	Enabled
Fresh Install of 11 SP4	Disabled	Disabled	Full	Enabled

IMPORTANT: All Primary Servers running ZENworks 11.2 or earlier should first be upgraded to ZENworks 11.3.0 or later before upgrading them to ZENworks 11.4. Satellite Servers and managed devices should be updated to 10.3.4 before updating them to ZENworks 11 SP4.

Table 2 ZENworks Cumulative Agent Update to 11 SP4: Supported Paths

Device Type	Operating System	Supported Versions	Unsupported Versions
Primary Server	Windows/Linux	v11.3 and later versions	Any version prior to 11.3
Satellite Server	Windows/Linux/Mac	v10.3.4 and later versions	Any version prior to 10.3.4
Managed Device	Windows	v10.3.4 and later versions	Any version prior to 10.3.4
	Linux	v11.0 and later versions	NA
	Mac	v11.2 and later versions	NA

3 Upgrade

For detailed information on prerequisites and instructions for upgrading Primary Servers, Satellites, and managed devices, see the [ZENworks 11 SP4 Upgrade Guide](#).

4 What's New

For information about the new features in ZENworks 11 SP4, see [What's New in 11 SP4](#).

5 ZENworks Reporting

The newer version of ZENworks Reporting 5 is not being released with ZENworks 11 SP4 and would be released later. In the meantime, ZENworks Reporting 5 released earlier would continue to work with ZENworks 11 SP4.

6 Known Issues

This section contains information about issues that might occur while you work with ZENworks 11 SP4.

- ♦ [Section 6.1, “Installation,” on page 3](#)
- ♦ [Section 6.2, “Upgrade,” on page 4](#)
- ♦ [Section 6.3, “Appliance,” on page 6](#)
- ♦ [Section 6.4, “Configuration Management,” on page 7](#)
- ♦ [Section 6.5, “Endpoint Security Management,” on page 13](#)
- ♦ [Section 6.6, “Full Disk Encryption,” on page 14](#)
- ♦ [Section 6.7, “Patch Management,” on page 15](#)

6.1 Installation

This section contains information about issues that you might encounter while installing ZENworks 11 SP4.

- ♦ [Section 6.1.1, “The `linux-ioa-update.xml` file remains on a Windows server after the ZENworks rollback is completed,” on page 3](#)
- ♦ [Section 6.1.2, “When reinstalling ZENworks after a rollback, the installation fails or hangs,” on page 3](#)
- ♦ [Section 6.1.3, “After uninstalling ZENworks a failed message is displayed,” on page 3](#)
- ♦ [Section 6.1.4, “Installation fails on Microsoft SQL database with different authentication modes,” on page 4](#)

6.1.1 The `linux-ioa-update.xml` file remains on a Windows server after the ZENworks rollback is completed

If you roll back ZENworks on a Windows server, then the `linux-ioa-update.xml` file remains on the server.

Workaround: After the ZENworks rollback is completed, delete the `linux-ioa-update.xml` file manually:

- 1 Go to `%ZENWORKS_HOME%\install\downloads\rpm`.
- 2 Delete the `linux-ioa-update.xml` file.

6.1.2 When reinstalling ZENworks after a rollback, the installation fails or hangs

When you reinstall ZENworks after a rollback the installation fails or hangs.

Workaround: After you roll back ZENworks, delete the `%ZENWORKS_HOME%` environment variable and then reinstall ZENworks.

6.1.3 After uninstalling ZENworks a failed message is displayed

After you uninstall ZENworks, a failed message is displayed instead of a success message.

Workaround: Ignore the failed message.

6.1.4 Installation fails on Microsoft SQL database with different authentication modes

Installation fails on Microsoft SQL database, if you use different authentication modes for database administrator and access user.

Recommended: Use the same authentication mode (**Windows Authentication** or **SQL Authentication**) for both database administrator and access user.

6.2 Upgrade

This section contains information about issues that you might encounter while upgrading to ZENworks 11 SP4.

- ♦ [Section 6.2.1, “Upgrade from ZENworks 11.3.x to ZENworks 11 SP4 with the MS SQL database might take several minutes to several hours,” on page 4](#)
- ♦ [Section 6.2.2, “Upgrade from ZENworks 11.3.x to ZENworks 11 SP4 might fail if MSSQL Mirroring is enabled,” on page 4](#)
- ♦ [Section 6.2.3, “Full Disk Encryption fails to upgrade on self-encrypting \(OPAL\) drives,” on page 5](#)
- ♦ [Section 6.2.4, “The ZENworks 11 SP4 Upgrade might fail when ImageDataBridge.dll is loaded by the Explorer process,” on page 6](#)

6.2.1 Upgrade from ZENworks 11.3.x to ZENworks 11 SP4 with the MS SQL database might take several minutes to several hours

While upgrading from ZENworks 11.3.x to ZENworks 11 SP4 with the Microsoft SQL database, the upgrade might take several minutes to several hours to replace the deprecated data types in some of the large tables.

It might seem that the upgrade process has stopped. However, it continues to run in the background. Do not close the Upgrade Wizard during the process.

Workaround: None.

NOTE: You can monitor the upgrade process by executing the following query in the ZENworks database:

```
SELECT * FROM DeprecatedDataTypesLog ORDER BY ENDTIME DESC
```

6.2.2 Upgrade from ZENworks 11.3.x to ZENworks 11 SP4 might fail if MSSQL Mirroring is enabled

During the upgrade from ZENworks 11.3.x to ZENworks 11 SP4, the database recovery model is changed from full to simple. If MSSQL database mirroring is enabled, the upgrade might fail.

Workaround: Disable the mirroring operation during the upgrade, or, if the upgrade fails, manually run the configuration action by executing the `novell-zenworks-configure -c MSSQLReplaceDeprecatedTypesConfigureAction` command.

6.2.3 Full Disk Encryption fails to upgrade on self-encrypting (OPAL) drives

Full Disk Encryption does not upgrade on devices with self-encrypting (OPAL) drives. This failure does not affect enforcement of the current Disk Encryption policy. The Disk Encryption policy is still effective and enforced properly. However, new ZENworks 11 SP4 Full Disk Encryption options will not be available on the device until the workaround is performed.

Workaround: To successfully upgrade the Full Disk Encryption components:

- 1 Make sure the device is running the ZENworks 11.3.2 FRU1 version of the ZENworks Adaptive Agent.
Versions of the agent prior to this version have an issue with removing policies from the device. The device must be at version 11.3.2 FRU1 for this workaround.
- 2 Remove the Disk Encryption policy from the device. To do so:
 - 2a Remove the policy assignment in ZENworks Control Center.
 - 2b Refresh the device.
 - 2c Reboot when prompted.
 - 2d Check the ZENworks Full Disk Encryption dialog box (Z-icon > **Full Disk Encryption** > **About**) to verify that no policy is applied.
- 3 Remove the Full Disk Encryption Agent from the device. To do so:
 - 3a Log in to ZENworks Control Center.
 - 3b To uninstall the agent from a single device, click **Devices**, click the device to display its details, click the **Settings** tab, click **Device Management**, then click **ZENworks Agent**.
or
To uninstall the agent from all device's in a device folder, click **Devices**, select the check box next to the device folder and click **Details** to display the folder details, click the **Settings** tab, click **Device Management**, then click **ZENworks Agent**.
or
To uninstall the agent from all device's in the zone, click **Configuration**, click **Device Management** (under Management Zone Settings), then click **ZENworks Agent**.
 - 3c (Conditional) If you are uninstalling from a single device or a device folder, click **Override** to enable the settings to be modified.
 - 3d Under Agent Features, deselect the **Installed** check box for Full Disk Encryption.
 - 3e Click **OK** to save the change.
 - 3f Perform an agent refresh on the target device (or devices).
The refresh takes longer than normal as the Full Disk Encryption Agent is removed. When the refresh completes, you can view the ZENworks Adaptive Agent's property pages (double-click the Z-icon in the notification area) to verify that **Full Disk Encryption** is no longer listed. In addition, the Full Disk Encryption Agent is no longer available in the **Start** menu.
- 4 If you haven't already done so, upgrade your ZENworks Primary Servers and upgrade the ZENworks Adaptive Agent on the device.
- 5 Install the Full Disk Encryption Agent on the device. To do so:
 - 5a Follow the process in Step 2, but select the **Installed** check box for Full Disk Encryption.
 - 5b Perform an agent refresh on the target device (or devices).
- 6 Assign the Disk Encryption policy to the device and refresh the device to enforce the policy.

6.2.4 The ZENworks 11 SP4 Upgrade might fail when ImageDataBridge.dll is loaded by the Explorer process

When the ImageDataBridge.dll file is loaded by the Explorer process while upgrading from ZENworks 11.3.x to ZENworks 11 SP4, the upgrade might fail or the ImageDataBridge.dll file might not get updated to the latest version.

Workaround: Either deploy the system update again or manually verify that the ImageDataBridge.dll file is updated to the latest version.

6.3 Appliance

This section contains information about issues that you might encounter while using ZENworks 11 SP4 Appliance.

- ◆ [Section 6.3.1, “The ZENworks Appliance Migration utility will not copy data from mounted folders,” on page 6](#)
- ◆ [Section 6.3.2, “After the ZENworks Appliance configuration the RemoteConnectFailureException error might be displayed,” on page 6](#)
- ◆ [Section 6.3.3, “While restarting the ZENworks Appliance an error message is displayed,” on page 7](#)
- ◆ [Section 6.3.4, “Creating the database by using the setup.sh -c --zcminstall command does not work in the ZENworks Appliance,” on page 7](#)
- ◆ [Section 6.3.5, “Deploying the ZENworks Appliance .ova file on the Citrix XENServer might take several hours,” on page 7](#)
- ◆ [Section 6.3.6, “Unable to launch ZENworks Control Center from the ZENworks Appliance Summary page in case of multiple IP addresses,” on page 7](#)
- ◆ [Section 6.3.7, “While configuring ZENworks you might get the NullPointer exception,” on page 7](#)

6.3.1 The ZENworks Appliance Migration utility will not copy data from mounted folders

If the ZENworks 11 SP3 Appliance has mounted an external content repository, the ZENworks Appliance Migration utility will not copy the data from the mounted folders. In this scenario, the File or Folder not found exception might appear.

Workaround: Any errors displayed by the ZENworks Appliance Migration utility can be ignored. Mount the external content repository to the ZENworks 11 SP4 Appliance and continue with the migration process.

6.3.2 After the ZENworks Appliance configuration the RemoteConnectFailureException error might be displayed

After the ZENworks Appliance configuration the RemoteConnectFailureException error might be displayed.

Workaround: Open the terminal and execute the `rcvabase-datamodel status` command. If the status indicates that the `rcvabase-datamodel` service is not running, start the service by executing the `rcvabase-datamodel start` command, and then execute the `rcvabase-jetty restart` command to restart the `rcvabase-jetty` service.

Or

Restart ZENworks Appliance.

6.3.3 While restarting the ZENworks Appliance an error message is displayed

While restarting the ZENworks Appliance the following error message might be displayed:

```
ERROR: transport error 202: bind failed: Address already in use
```

Workaround: Ignore the error message.

6.3.4 Creating the database by using the `setup.sh -c --zcminstall` command does not work in the ZENworks Appliance

In ZENworks Appliance, database creation by using the `setup.sh -c --zcminstall` command does not work when you launch the ZENworks installer (`usr/share/ZCMInstaller`).

Workaround: None

6.3.5 Deploying the ZENworks Appliance .ova file on the Citrix XENServer might take several hours

While deploying the ZENworks Appliance .ova file on the Citrix XENServer might take several hours

Workaround: None

6.3.6 Unable to launch ZENworks Control Center from the ZENworks Appliance Summary page in case of multiple IP addresses

If you have multiple IP addresses in a server and try to launch ZENworks Control Center from the ZENworks Appliance Summary page, then it might pick up the inactive IP address and unable to access ZENworks Control Center.

Workaround: Launch ZENworks Control Center manually with hostname or active IP address.

6.3.7 While configuring ZENworks you might get the `NullPointerException` exception

While configuring ZENworks you might get the `NullPointerException` exception.

Workaround: Refresh the web browser and configure ZENworks.

6.4 Configuration Management

This section contains information about issues that you might encounter while using ZENworks 11 SP4 Configuration Management.

- ♦ [Section 6.4.1, “Additional Primary Server uses the same port as another Primary Server,” on page 8](#)
- ♦ [Section 6.4.2, “A blank screen is displayed during a remote login to SLES 12 or SLED 12 devices,” on page 8](#)
- ♦ [Section 6.4.3, “Unable to pull updates after system update re-deployment,” on page 9](#)
- ♦ [Section 6.4.4, “The Certificate Remint Tool might not be available on all Primary Servers,” on page 9](#)
- ♦ [Section 6.4.5, “Workstation type devices can be added as members of server groups and vice versa,” on page 9](#)
- ♦ [Section 6.4.6, “Imaging Satellite Servers \(11.3.1 or earlier\) unable to communicate with the first Primary Server,” on page 10](#)

- ◆ Section 6.4.7, “The Remint Server Certificate option is available even though the server certificate has expired,” on page 10
- ◆ Section 6.4.8, “Registration of new devices fails after upgrading the server from ZENworks 11.3.x to ZENworks 11 SP4,” on page 10
- ◆ Section 6.4.9, “The Check for updates option is not available in the ZENNotify icon on the console session of a Primary Server,” on page 10
- ◆ Section 6.4.10, “The Remint system update is being assigned to Primary Servers or managed devices that are added after the zone CA is activated,” on page 10
- ◆ Section 6.4.11, “Managed Devices are not able to communicate with Satellite Servers that have the Authentication Role,” on page 11
- ◆ Section 6.4.12, “Lenovo and HP Tablet PCs with Windows 8 or Windows 8.1 operating system might crash or display an incorrect serial number after the agent installation.,” on page 11
- ◆ Section 6.4.13, “The ZENworks property page is blank on a Mac OS X 10.7.x platform,” on page 11
- ◆ Section 6.4.14, “The startup location audit fails in the Sybase database (constraint violation exception),” on page 12
- ◆ Section 6.4.15, “RHEL Imaging Servers fail to communicate with ZENworks 11 SP4 Primary Servers,” on page 12
- ◆ Section 6.4.16, “SLES 12 Imaging Servers fail to communicate with ZENworks 11 SP4 Primary Servers,” on page 12
- ◆ Section 6.4.17, “Issues with ZENworks Remote Management Blank Screen Operation,” on page 13
- ◆ Section 6.4.18, “Unable to remote control 11.3.x or older managed devices from a ZENworks 11 SP4 server,” on page 13
- ◆ Section 6.4.19, “When you launch a bundle with a display message launch action, the message is not displayed properly,” on page 13

6.4.1 Additional Primary Server uses the same port as another Primary Server

During the installation of a Primary Server, it uses the same port as an existing Primary Server. This happens when the port, used by parent Primary Server, is free on the additional Primary Server. If the port is busy, it prompts you to use another port.

6.4.2 A blank screen is displayed during a remote login to SLES 12 or SLED 12 devices

As an administrator, when you try to perform a remote login from ZENworks Control Center to a device that has a SLES 12 or SLED 12 operating system, if the user is already logged in to the remote device, a blank screen is displayed.

Workaround: To login to the device successfully, ensure that the user on the remote device is logged out before performing a remote login.

6.4.3 Unable to pull updates after system update re-deployment

If a system update fails and goes to the `FINISHED_WITH_ERROR` state, and if the system update redeployment followed by the `zac zeus-refresh` command is done immediately, the system update does not start again. The update remains in the `ERROR` state.

When the `FINISHED_WITH_ERROR` status is updated to the Primary Server by ZENUpdater, ZeUS might not have refreshed. The ZeUS service would have started, but the refresh happens approximately 10 to 15 minutes after the startup of the service. Therefore, if you redeploy the update immediately after the failure is reported, when ZeUS refreshes, it fetches the assignment, but assumes that the update is currently ongoing and therefore reports the status as `FINISHED_WITH_ERROR`.

Workaround: When the system update completes `k` errors, if you need to immediately re-deploy the update, without having to wait for 10 to 15 minutes, after the error is reported, run the `zac zeus-refresh` command before re-deploying.

6.4.4 The Certificate Remint Tool might not be available on all Primary Servers

During a Change Certificate Authority (CA), Remint CA or Server Remint process, the Certificate Remint Tool (CRT) might not be available on all Primary Servers.

Workaround: Based on the scenario, perform the relevant steps:

- ◆ If you are performing a Remint CA, the CRT will be available on the current CA server.
- ◆ If you are changing the CA to Internal, the CRT will be available on the server that is selected as the new CA server.
- ◆ If you are changing the CA to External, the CRT will be available on the ZENworks Control Center server on which you are performing the operation.
- ◆ If you are performing a Server Remint, and if the CA is Internal, the CRT will be available on the current CA server.
- ◆ If you are performing a Server Remint and the CA is External, the CRT will be available on the server on which you launched the operation.

6.4.5 Workstation type devices can be added as members of server groups and vice versa

While copying relationships from one device (source device) to another (target device), the wizard allows you to make the target device a member of the Static Device group, to which the source device belongs.

Due to this behavior, it is possible to add a server type device to a Static Workstation group and a workstation type device to a Static Server group. Hence, all assignments made to a Static Server group will flow down to the workstation type device, and vice versa, which may not be relevant.

You need to ensure that you copy assignments only between the same device types. For example, from servers to servers and workstations to workstations. Do not copy assignments from server folders, server groups, or servers to workstation folders, workstation groups or workstations respectively, and vice versa

Workaround: Manually delete the device from the static device group.

6.4.6 Imaging Satellite Servers (11.3.1 or earlier) unable to communicate with the first Primary Server

Due to the POODLE vulnerability fix, older Imaging Satellite Servers (11.3.1 or earlier) are not able to communicate with the ZENworks 11 SP4 Primary Server.

Workaround: Perform one of the following actions:

- ◆ Apply this [POODLE](#) patch to the Imaging Satellite Servers that are not able to communicate. This can be applied even after upgrading the first Primary Server to 11.4 as communication in the Imaging context is only impacted.

OR

- ◆ Upgrade all the Imaging Satellite Servers to ZENworks 11 SP4.

6.4.7 The Remint Server Certificate option is available even though the server certificate has expired

The **Remint Server Certificate** feature is not supported for expired server certificates. However, even when a server certificate expires, the **Remint Server Certificate** option is displayed. When you click this option, you are not able to proceed with the remint.

Workaround: None. Ignore the **Remint Server Certificate** option when a server certificate expires.

6.4.8 Registration of new devices fails after upgrading the server from ZENworks 11.3.x to ZENworks 11 SP4

When the subordinate certificate authority is set as the zone certificate authority, and the server is upgraded to 11.4, registration of new devices will fail.

Workaround: Change the certificate authority to the root CA. For more information, see [Changing the Certificate Authority](#) in the *ZENworks 11 SP4 SSL Management Reference*.

6.4.9 The Check for updates option is not available in the ZENNotify icon on the console session of a Primary Server

The **Check for updates** option is not displayed in the ZENNotify icon if the console session is established remotely using the `/console` option.

Workaround: To achieve the same functionality, you need to run the `zac zeus-refresh` command.

6.4.10 The Remint system update is being assigned to Primary Servers or managed devices that are added after the zone CA is activated

After the CA is activated during a zone CA remint, if a new Primary Server or managed device is added to the zone, the remint system update is automatically assigned to the device. For Primary Servers this will happen even though the Primary Server's certificate has been issued by the new CA.

Workaround: None. Let the system update complete.

6.4.11 **Managed Devices are not able to communicate with Satellite Servers that have the Authentication Role**

If the Microsoft [KB3061518](https://support.microsoft.com/en-us/kb/3061518) (<https://support.microsoft.com/en-us/kb/3061518>) security update is applied on the managed devices, they will not be able to communicate with their Authentication Satellite Servers. This issue occurs in internal CA zones and external CA zones using DSA certificates.

To address the [Logjam](https://weakdh.org/) (<https://weakdh.org/>) vulnerability, a fix has been incorporated in the 11 SP4 Authentication Satellite Servers. However, this fix requires the SSL server certificates of Authentication Satellite Servers to be reminded after upgrading to 11 SP4. If the Satellite Server certificate remind has not been completed, the managed devices will continue to get authenticated if the closest server rules (CSR) contain any of the earlier versions of the Authentication Satellite Servers (prior to 11 SP4) or 11 SP4 Primary Servers.

NOTE: If the Satellite Server has other roles configured apart from the Authentication role, the managed devices will lose communication for these roles as well.

Workaround: Perform either of the following:

- ◆ Upgrade the Primary Servers to 11 SP4 and remind the certificates of the Authentication Satellite Servers. For more information on reminding certificates, see [Reminting Server Certificates](#) in the [ZENworks 11 SP4 SSL Management Reference](#).

OR

- ◆ Run the following zac command:
 - ◆ On Windows Authentication Satellite Servers: `zac asr -t all`
 - ◆ On Linux Authentication Satellite Servers: `zac rsc`


6.4.12 **Lenovo and HP Tablet PCs with Windows 8 or Windows 8.1 operating system might crash or display an incorrect serial number after the agent installation.**

After installation of the ZENworks Adaptive Agent, Lenovo and HP Tablet PCs with older versions of Intel Atom processors that have Windows 8 or Windows 8.1 operating system might crash while trying to register to the Management Zone. If the agent does successfully register to the Management Zone after the installation, an incorrect serial number might be displayed in the system component.

IMPORTANT: Novell recommends that you test the deployment on all target device models before deploying to any production devices.

Workaround: None.

6.4.13 **The ZENworks property page is blank on a Mac OS X 10.7.x platform**

When you double-click the  icon on a Macintosh OS X 10.7.x device, the ZENworks property page is blank.

Workaround: Upgrade Macintosh OS X 10.7.x to 10.8 or a later version.

6.4.14 The startup location audit fails in the Sybase database (constraint violation exception)

In the Sybase database, while processing the startup location audit events, the audit process fails with the following error message:

```
com.novell.zenworks.datamodel.audit.AuditDataModelException:  
org.hibernate.exception.ConstraintViolationException: ((Sybase())(JDBC  
Driver())(SQL Anywhere())Column 'FK_ZSTARTUP_LOC_TARGET_ENVT' in table  
'CA_STARTUP_LOC' cannot be NULL
```

Workaround: To audit the startup location in the Sybase database, do the following:

1 Log in to the audit database.

2 Run the following queries:

```
if exists (select * from sysconstraint where  
constraint_name='FK_ZSTARTUP_LOC_TARGET_ENVT')  
    alter table CA_STARTUP_LOC  
        drop constraint FK_ZSTARTUP_LOC_TARGET_ENVT  
GO  
IF NOT EXISTS (  
    SELECT *  
    FROM sysconstraint  
    WHERE constraint_name = 'FK_ZSTARTUP_LOC_TARGET_ENVT'  
    )  
    ALTER TABLE CA_STARTUP_LOC ADD CONSTRAINT FK_ZSTARTUP_LOC_TARGET_ENVT  
    FOREIGN KEY (TARGETGUID1) REFERENCES ZNWENV_REF ON DELETE CASCADE
```

6.4.15 RHEL Imaging Servers fail to communicate with ZENworks 11 SP4 Primary Servers

Because of the previous version of openssl in RHEL servers, ZENworks 11.3.x or 11.4 on RHEL Primary or Satellite Imaging Servers might not be able to communicate with ZENworks 11 SP4 Primary Servers.

Workaround: Install the openssl-1.0.1e-30.e16_6.11.x86_64.rpm file on the RHEL Imaging Servers.

6.4.16 SLES 12 Imaging Servers fail to communicate with ZENworks 11 SP4 Primary Servers

The default version of openssl in SLES 12 servers breaks the communication with the 11 SP4 Primary Servers.

Workaround: Update the default version of openssl with the libopenssl11_0_0-1.0.1k-2.24.1.x86_64.rpm file.

6.4.17 Issues with ZENworks Remote Management Blank Screen Operation

- ♦ You may notice screen flickering and performance degradation while performing the Remote Management Blank Screen operation on a remote machine.
- ♦ The Remote Management Blank Screen operation is not available on a Windows 8.1 operating system and later, and this operation will also be disabled during the Remote Diagnostics operation.

6.4.18 Unable to remote control 11.3.x or older managed devices from a ZENworks 11 SP4 server

ZENworks 11 SP4 uses the SHA-256 algorithm to generate a self signed certificate, which is not supported by 11.3.x and older managed devices. Hence, the SSL handshake fails and the ZENworks 11 SP4 server cannot perform a remote operation on these older devices.

Workaround: Perform the following steps on the device from where the remote session is initiated:

- 1 In the `Session Security` section of the Remote Management policy, enable the **Allow connection when Remote Management Console does not have SSL certificate** option.
- 2 Create the `SkipOperatorCert` registry key in the `HKEY_CURRENT_USER\Software\Novell\ZCM\Remote Management\Viewer\Settings` path, with the `DWORD` type and any non-zero value.

6.4.19 When you launch a bundle with a display message launch action, the message is not displayed properly

On a SLES 12 device, when you launch a bundle with a display message launch action, zicon does not display the message properly in the system tray.

Workaround: None

6.5 Endpoint Security Management

This section contains information about issues that you might encounter while using ZENworks 11 SP4 Endpoint Security Management.

- ♦ [Section 6.5.1, “Safe Harbor Encryption for Fixed Disks Discontinued,”](#) on page 13
- ♦ [Section 6.5.2, “Encryption Support Discontinued for USB 1.x Devices,”](#) on page 14
- ♦ [Section 6.5.3, “Deletion of Files from Read-Only Devices with Storage Device Control Policy,”](#) on page 14

6.5.1 Safe Harbor Encryption for Fixed Disks Discontinued

The Safe Harbor Encryption setting is no longer included in new Data Encryption policies created in ZENworks 11 SP4 or newer versions.

If your policy includes this setting, it is because 1) the Data Encryption policy was created in a ZENworks 11 SP3 or earlier version and 2) the setting was enabled. You cannot modify the setting, but the setting will continue to be enforced on any device (regardless of ZENworks Adaptive Agent version) to which the policy is assigned. If you no longer want the setting applied to a device, you must assign the device a new Data Encryption policy that does not have the setting.

6.5.2 Encryption Support Discontinued for USB 1.x Devices

The Data Encryption policy no longer supports encryption of USB 1.x devices.

6.5.3 Deletion of Files from Read-Only Devices with Storage Device Control Policy

The Storage Device Control policy allows you to designate removable storage devices (USB drives, etc.) as read only. If a user deletes a file from a read-only device, the file disappears from Windows Explorer even though it is not deleted. The only way to see the file again is to remove and reinsert the device.

6.6 Full Disk Encryption

This section contains information about issues that you might encounter while using ZENworks 11 SP4 Full Disk Encryption.

- ◆ [Section 6.6.1, “Virtual and Thin-Client Environments Not Supported,” on page 14](#)
- ◆ [Section 6.6.2, “Switching Encryption Modes on Self-Encrypting Drives Results in KEK status unknown ! System Halted Error,” on page 14](#)
- ◆ [Section 6.6.3, “Full Disk Encryption fails to upgrade on self-encrypting \(OPAL\) drives,” on page 14](#)
- ◆ [Section 6.6.4, “DMI settings for existing policies not updated during upgrade,” on page 15](#)

6.6.1 Virtual and Thin-Client Environments Not Supported

Full Disk Encryption is not supported in virtual environments. When installing the ZENworks Adaptive Agent on virtual machines or on machines accessed through thin clients, do not enable Full Disk Encryption.

6.6.2 Switching Encryption Modes on Self-Encrypting Drives Results in KEK status unknown ! System Halted Error

On a device with a self-encrypting drive, if you apply a Disk Encryption policy that overrides the device's current **Enable software encryption of Opal compliant self-encrypting drives** setting (either enabling it or disabling it), the device black screens and displays a **KEK status unknown ! System Halted** error.

Full Disk Encryption does not support changing the software encryption setting on self-encrypting drives without removing the first policy completely and then applying the second policy (with the changed software encryption setting). To guard against this, the Disk Encryption policy does not allow you to change this setting (the **Enable software encryption of Opal compliant self-encrypting drives** option) after the policy is created. However, it is possible for you to create a second policy with the option set differently and have that policy become the device's effective policy (assigned directly to the device rather than through a device folder, placed higher in the device's policy list than the first policy, etc.). If this happens, the device black screens.

Workaround: Remove all Disk Encryption policy assignments from the device and ensure that removal is complete (disk unencrypted, PBA removed). Assign the Disk Encryption policy (with the correct software encryption setting) to the device.

6.6.3 Full Disk Encryption fails to upgrade on self-encrypting (OPAL) drives

For details, see [Section 6.2.3, “Full Disk Encryption fails to upgrade on self-encrypting \(OPAL\) drives,” on page 5](#) in the Upgrade known issues.

6.6.4 DMI settings for existing policies not updated during upgrade

New DMI settings have been added for this release to support additional devices. The new DMI settings are automatically included when a new Full Disk Encryption policy is created. During upgrade, however, the DMI settings in existing policies are not updated with the new settings. This is working as designed in order to preserve the state of your current policies and ensure that they continue to work on assigned devices.

If you want the new DMI settings added to existing policies, you must manually add them. To do so, cut and paste the settings from a newly created policy, from the `etc/opt/novell/zenworks/fde/dmi.ini` file on a Linux Primary Server, or the `novell/zenworks/conf/fde/dmi.ini` file on a Windows Primary Server.

6.7 Patch Management

This section contains information about issues that you might encounter while using ZENworks 11 SP4 Patch Management.

- ♦ [Section 6.7.1, “The context-sensitive help for Dashboarding and Trending does not adequately describe the Save Patch Status History option,” on page 15](#)

6.7.1 The context-sensitive help for Dashboarding and Trending does not adequately describe the Save Patch Status History option

The context-sensitive help for **Configuration > Patch Management > Dashboarding and Trending** does not adequately describe the **Save Patch Status History** option.

Workaround: This option saves a daily record of the patch status history in the database (it is also used by the Patch Management Dashboard Patch Compliance graph). Enterprises with more than 10 thousand nodes should not use this option, because when the data for all nodes and patches is saved, it can consume a large amount of space on your database, very quickly.

7 Additional Documentation

This Readme lists the issues specific to ZENworks 11 SP4. For all other ZENworks 11 SP4 documentation, see the [Novell ZENworks 11 SP4 documentation website](http://www.novell.com/documentation/zenworks114/) (<http://www.novell.com/documentation/zenworks114/>).

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/>.

Copyright © 2016 Novell, Inc. All Rights Reserved.