

ZENworks 2017 Update 1 Lighthouse Readme

May 2017



The information in this Readme pertains to the ZENworks 2017 Update 1 Lighthouse release.

- ♦ [Section 1, "What's New in ZENworks 2017 Update 1," on page 1](#)
- ♦ [Section 2, "Updating to ZENworks 2017 Update 1," on page 3](#)
- ♦ [Section 3, "Known Issues," on page 3](#)
- ♦ [Section 4, "Additional Documentation," on page 8](#)
- ♦ [Section 5, "Legal Notice," on page 8](#)

1 What's New in ZENworks 2017 Update 1

This release includes the following new features:

- ♦ **IPv6 Support:** ZENworks 2017 Update 1 enables you to configure ZENworks to use IPv6 as the protocol for communication. This includes support for L4 switch configuration.

NOTE: ZENworks Primary Servers need to have both IPv4 and IPv6 enabled. However, the Satellite Servers and managed devices can have IPv4, IPv6 or both enabled.

- ♦ **Support for Apple's Device Enrollment Program:** ZENworks now supports the Apple Device Enrollment Program (DEP). With this release, you can create a DEP Server by linking the ZENworks MDM Server to your Apple DEP account. Further, you can enroll your DEP-enabled devices, renew the DEP token, as well as remove the DEP Server from the management zone.
- ♦ **Enrollment of supervised iOS devices and the inclusion of additional restrictions:**
ZENworks now supports the enrollment of iOS devices in the supervised mode through the Apple Device Enrollment Program or by using the Apple Configurator.
Additional settings have been introduced in the Device Control Policy to apply restrictions on these supervised devices.
- ♦ **Messaging using Firebase Cloud Messaging:** You can now migrate from the Google Cloud Messaging (GCM) Service to the Firebase Cloud Messaging (FCM) Service. To test this feature, you need to update the ZENworks Agent app to the Update 1 version.
- ♦ **Configuration of app parameters:** ZENworks lets you pre-configure supported apps for iOS devices by specifying key-value pairs or by uploading a configuration file obtained from the app vendor.
- ♦ **Configure a HTTP Proxy Server for an MDM Server:** You can now define a HTTP Proxy Server to enable an MDM Server to connect to the Internet through the proxy server. These proxy servers are used by the MDM Servers to contact the APNs Server, GCM Server, and managed mobile devices.
- ♦ **Language support for email notifications:** Multi-language support for email notifications sent to mobile devices is now available with this release. The Mobile Enrollment Policy lets you specify the language in which these notifications are to be sent. You can also edit the email message in your preferred language.

- ♦ **Configure ActiveSync Logon Attribute in the User Source:** ZENworks now lets you edit the User Source (LDAP directory) attribute that will be used to authenticate to the ActiveSync Server, while synchronizing emails on devices.
- ♦ **Pinning and Unpinning Bundles:** ZENworks Application (ZAPP) now enables you to pin and unpin bundles to the Desktop, Taskbar and Start menu tiles.
- ♦ **Bundle License Tracking:** Using the ZENworks Bundle License Tracking feature, you can track the number of installations of inventory products through a bundle.
- ♦ **System Update enhancements:** The system update enhancements will enable you to:
 - ♦ **View the deployment status in a zone:** After deploying a system update in the zone, users can view the deployment status of Primary Servers by using the `https://<host_name>:7444/systemupdate/sustatus` link. The filter options enable users to limit the number of results displayed, based on the build version and deployment status.
 - ♦ **View the deployment status by device:** The new search feature enables users to narrow down the deployments status results based on the device name, device type and status.
- ♦ **Patch Management enhancements:** Patch Management enhancements will enable you to:
 - ♦ **Delay disabling of superseded patches:** In the Subscription Service Content Download settings, you can choose to delay the disabling of superseded patches for up to 90 days or postpone them indefinitely for patches included in patch policies.
 - ♦ **View and modify how data is shown in a new Dashboard:** View and change how Patch Management data is shown in a redesigned dashboard.
- ♦ **Full Disk Encryption enhancements:** Full Disk Encryption enhancements will enable you to:
 - ♦ **Encrypt UEFI enabled devices:** Employ Full Disk Encryption policies on devices that are equipped and enabled to use UEFI firmware. This enhancement also includes the use of GUID partition tables (GPT) to define and encrypt up to 128 volumes per disk.
 - ♦ **Use additional smart card readers:** Create new Disk Encryption policies with enhanced hardware compatibility for pre-boot authentication. This feature includes a new auto-setting that checks for compatibility, as well as the capability to modify the DMI configuration during policy application in the event of a hardware compatibility issue.

IMPORTANT: The two features above require the removal of Disk Encryption policies and complete volume decryption on encrypted devices prior to updating the devices to ZENworks 2017 Update 1. Once the devices are decrypted, you can apply a new Disk Encryption policy.

- ♦ **Enable new agent events for disk encryption status:** In the Agent Events Configuration, you can enable two new settings that prompt Agent Event messages when encryption or decryption of disk volumes starts.
- ♦ **Endpoint Security enhancements:** Endpoint Security enhancements will enable you to:
 - ♦ **Enable Secure Boot on UEFI devices:** Windows Secure Boot is fully supported on UEFI enabled devices not using Full Disk Encryption.
 - ♦ **View more properties of USB scanned devices:** The Device Scanner tool provides more comprehensive details about USB devices in the device list after the scan completes.

2 Updating to ZENworks 2017 Update 1

Perform the following steps to update your zone to ZENworks 2017 Update 1:

- 1 Download the ZENworks 2017 Update 1 ZIP file (`ZENworks_17.1.0_Update.zip`).
- 2 After downloading the ZIP file, in the command prompt run the `zman sui <system_update_name.zip>` command.
- 3 Provide the ZENworks administrator credentials. The update will be imported to the zone.
Using ZENworks Control Center you can track the import status.
- 4 After importing the system update, complete the system update process, and then assign the update to all the servers and managed devices.

NOTE: You must first deploy the system update to all the Primary Servers in the zone, and then to the managed devices.

If you are using Full Disk Encryption on managed devices, see the **Important** callout under *Full Disk Encryption enhancements* in Section 1.

3 Known Issues

This section contains information about issues that might occur while you work with ZENworks 2017 Update 1:

- ♦ [Section 3.1, “System Update,” on page 3](#)
- ♦ [Section 3.2, “ZENworks Configuration,” on page 4](#)
- ♦ [Section 3.3, “ZENworks Agent,” on page 6](#)
- ♦ [Section 3.4, “ZENworks Application,” on page 6](#)
- ♦ [Section 3.5, “Remote Management,” on page 6](#)
- ♦ [Section 3.6, “ZENworks Imaging,” on page 7](#)
- ♦ [Section 3.7, “ZENworks Appliance,” on page 7](#)
- ♦ [Section 3.8, “Mobile Management,” on page 7](#)

3.1 System Update

- ♦ [Section 3.1.1, “On SLES 11 SP3 and 11 SP4 devices, ZENworks services might not start automatically after the system update,” on page 3](#)

3.1.1 On SLES 11 SP3 and 11 SP4 devices, ZENworks services might not start automatically after the system update

After you perform a system update on SLES 11 SP3 or SP4 devices, the ZENworks services might not start automatically.

Workaround: Manually restart the ZENworks Monitor service by using the `/etc/init.d/novell-zenmntr start` command. After the ZENworks Monitor service is started, the server and loader services will start automatically.

3.2 ZENworks Configuration

- ♦ Section 3.2.1, “When a new ZENworks 2017 Primary Server is added to a ZENworks 2017 Update1 or later, IPv6-enabled zone, the closest servers might have IPv6 URLs in an incorrect format,” on page 4
- ♦ Section 3.2.2, “On Windows 2012 R2 devices, the network adapter is removed when the IPv4 and IPv6 values are changed using the zisedit command,” on page 4
- ♦ Section 3.2.3, “On a SLES 11 device, Location and Network Environments detection might fail with the DHCP address,” on page 4
- ♦ Section 3.2.4, “ZENworks Java applications might not work on a Windows device on which the IPv4 interface is uninstalled,” on page 4
- ♦ Section 3.2.5, “While performing a Change CA, validation of a chained certificate fails if the certificate chain is in the wrong order,” on page 5
- ♦ Section 3.2.6, “pgadmin3 does not start on a SLES device,” on page 5

3.2.1 When a new ZENworks 2017 Primary Server is added to a ZENworks 2017 Update1 or later, IPv6-enabled zone, the closest servers might have IPv6 URLs in an incorrect format

When you add a new ZENworks 2017 Primary Server to a ZENworks 2017 Update 1, IPv6-enabled zone, the closest servers might have an incorrect IPv6 URL format.

Executing the `zac zc` command enables you to view the zone configuration. However, executing the `zac zc -l` command might not list the IPv6 URLs in the correct format.

Workaround: Execute the `zman lrr -f` command on a server that is upgraded to the latest version.

3.2.2 On Windows 2012 R2 devices, the network adapter is removed when the IPv4 and IPv6 values are changed using the zisedit command

After installing the agent on a Windows 2012 R2 device, when you boot the device using PXE or Boot CD, and run the zisedit command with the following settings, the network adapter is removed from the network connections:

1. Set the DHCP and DHCP6 values to off.
2. Change the IPv4 and IPv6 values.

Workaround: Configure the IPv4 and IPv6 values separately.

3.2.3 On a SLES 11 device, Location and Network Environments detection might fail with the DHCP address

If a network is configured using NetworkManager on a SLES 11 device, the Client IP address Network service might not match with IPv6 DHCP address. Hence, location and network environment detection fails.

Workaround: Configure the network using the `ifup` method.

3.2.4 ZENworks Java applications might not work on a Windows device on which the IPv4 interface is uninstalled

When you uninstall the IPv4 interface using the `netsh interface ipv4 uninstall` command on a Windows device, then ZENworks Java applications such as ZCC Helper might not work.

Workaround: The IPv4 stack needs to be configured in addition to the IPv6 stack.

For more information, refer to the following links:

- ♦ <http://www.oracle.com/technetwork/java/javase/8-known-issues-2157115.html>
- ♦ http://bugs.java.com/bugdatabase/view_bug.do?bug_id=8040229

3.2.5 While performing a Change CA, validation of a chained certificate fails if the certificate chain is in the wrong order

While changing the external Certificate Authority, if the new certificate file includes the certificate chain in a wrong order, then certificate validation fails. For example, instead of Server > SubCA > RootCA, if the chain is in the following order: SubCA > Server > RootCA., the certificate will be considered as invalid.

Workaround: Re-create the server certificate chain (with certificates in the specified order) using your preferred method. One of the simplest ways of doing it as follows:

- 1 Save each certificate as a separate file in the base64 format.
- 2 Open each certificate in a text editor. The content will be similar to the content below:

```
-----BEGIN CERTIFICATE-----  
<cert data>  
-----END CERTIFICATE-----
```

- 3 Create a new file and name it as server.cer.
- 4 Copy the text from each certificate file into the server.cer file so that the certificates are all in one file, in the following order:

```
-----BEGIN CERTIFICATE-----  
<Server cert data>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<SubCA cert data>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<RootCA cert data>  
-----END CERTIFICATE-----
```

- 5 Save the server.cer file.
- 6 Use the server.cer file as the new certificate and complete the steps to change the external Certificate Authority (CA).

3.2.6 pgadmin3 does not start on a SLES device

When you open pgadmin3 on a SLES device, one of the following errors might be displayed:

- ♦ *pgadmin3: error while loading shared libraries: libiconv.so.2: cannot open shared object file: No such file or directory*
- ♦ *./pgadmin3: symbol lookup error: /usr/lib64/libgdk-x11-2.0.so.0: undefined symbol: pango_font_map_create_context*

Workaround: Execute the following command in the terminal before opening pgadmin3:

```
Export LD_LIBRARY_PATH="/usr/local/lib64:/usr/local/lib:/lib64:/lib:/usr/lib64:/usr/lib:/opt/novell/zenworks/share/pgsql/lib:/opt/novell/zenworks/share/pgsql/pgAdmin3/lib"
```

3.3 ZENworks Agent

- ♦ [Section 3.3.1, “When you restart the agent on an older managed device and the Primary Server host name resolves to an IPv6 address, then the managed device might not register to the zone,” on page 6](#)

3.3.1 When you restart the agent on an older managed device and the Primary Server host name resolves to an IPv6 address, then the managed device might not register to the zone

On a managed device, when cache is cleared and the device is restarted, the agent reads server URLs from the `initial-web-service` file. If the server URL contains a host name which resolves to an IPv6 address, then the SSL host name verification fails. Hence, the older agents might not be registered.

Workaround: Manually add the IPv4-based URL to the `initial-web-service` file and then refresh the older agent.

3.4 ZENworks Application

- ♦ [Section 3.4.1, “ZAPP launches automatically after a reboot,” on page 6](#)

3.4.1 ZAPP launches automatically after a reboot

If you create a ZECF policy to hide the ZENworks tray icon and then you assign the policy to a device, when you reboot the device, ZAPP is launched automatically.

Workaround: Delete the `ZAPP` registry key:

- 1 Open the Registry Editor.
 - ♦ For 32-bit: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
 - ♦ For 64-bit: `HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run`
- 2 Delete the `ZAPP` registry key.

3.5 Remote Management

- ♦ [Section 3.5.1, “Open source VNC viewers are not supported when you remote control a Windows managed device using an IPV6 address,” on page 6](#)

3.5.1 Open source VNC viewers are not supported when you remote control a Windows managed device using an IPV6 address

On a Windows device, the ZENworks Agent cannot connect with open source viewers such as RealVNC, TightVNC and UltraVNC using an IPv6 address.

Workaround: To manage Windows devices using IPv6 addresses, use IPv6 compatible open source VNC viewers. Open source VNC viewers can be used to communicate with managed devices using IPv4 addresses.

3.6 ZENworks Imaging

- ♦ [Section 3.6.1, “RHEL 7 device boots in the maintenance mode after restoring the image,” on page 7](#)

3.6.1 RHEL 7 device boots in the maintenance mode after restoring the image

When you take an image of an RHEL 7 device with SELinux enabled, the device boots in the maintenance mode after restoring the image.

Workaround: Before taking the image, disable SELINUX:

1. Go to the `/etc/selinux` folder.
2. In the `config` file, set the SELINUX value as disabled.
3. Restart the device.

3.7 ZENworks Appliance

- ♦ [Section 3.7.1, “A blank page is displayed in the Internet Explorer 11 browser when you open the Terminal and File Explorer tile using an IPv6 address,” on page 7](#)

3.7.1 A blank page is displayed in the Internet Explorer 11 browser when you open the Terminal and File Explorer tile using an IPv6 address

When you open the Terminal and File Explorer tile in ZENworks Appliance using an IPv6 address, a blank page is displayed in the Internet Explorer 11 browser.

Workaround: Open the ZENworks Appliance using literal IPv6 addresses in UNC path names.

For example, `2001:db8::ff00:42:8329` can be written as `2001:db8::ff00:42:8329.ipv6-literal.net`

3.8 Mobile Management

This section contains information about issues that you might encounter while using the Mobile Management feature:

- ♦ [Section 3.8.1, “Creation of certain App Store bundles fails with the Right Truncation of String Data error,” on page 7](#)
- ♦ [Section 3.8.2, “On iOS devices the prompt to enter the email account password might not be displayed,” on page 8](#)

3.8.1 Creation of certain App Store bundles fails with the Right Truncation of String Data error

Bundle creation for certain App Store apps might fail and the **Right truncation of string data** error is displayed. This error occurs because the ZENworks Database currently does not support the Compatibility information published in the Apple App store for these specific apps.

Workaround: None.

3.8.2 On iOS devices the prompt to enter the email account password might not be displayed

When an email account is remotely configured on an iOS device using a Mobile Email Policy, then the prompt to enter the email account password might not be displayed.

Workaround: Manually specify the password by navigating to the Settings menu on the device.

4 Additional Documentation

This Readme lists the issues specific to ZENworks 2017 Update 1 release. For all other ZENworks 2017 Update 1 documentation, see the [ZENworks 2017 Update 1 documentation website](#).

5 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 © 2017 Micro Focus Software Inc. All Rights Reserved.