Hewlett Packard Enterprise

HPE OneView 4.00.09 Update Release Notes

Abstract

This document describes changes in HPE OneView software to help administrators understand the benefits of obtaining the 4.00.09 software update. This release is intended for administrators who configure, manage, and troubleshoot HPE ProLiant servers, HPE Virtual Connect, and storage systems using HPE OneView.

Part Number: P05469-002b
Published: June 2018
Edition: 3

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft® is a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Contents

Release description and installation instructions

Introduction

This document provides release information for HPE OneView version 4.00.09.

Intended audience	Related information
Virtual appliance users	• **Changes delivered in HPE OneView 4.00.09 for Virtual Appliance** on page 4 • **Support and other resources** about related products and how to find technical documentation
HPE Synergy users	• **Changes delivered in HPE OneView 4.00.09 for HPE Synergy** on page 5 • **Support and other resources** about related products and how to find technical documentation
Users who are installing a new appliance	• **Appliance installation instructions** • **HPE OneView 4.00.09 issues and suggested actions for virtual appliances** on page 7 • **HPE OneView 4.00.09 issues and suggested actions for HPE Synergy** on page 9
Users who are updating from an earlier version of an HPE OneView appliance	• **Update prerequisites** on page 13 • **Update instructions** on page 14

IMPORTANT: The release notes file embedded with the release distribution file (for c7000, `Z7550-96498.bin` / for HPE Synergy, `Z7550-96496.bin`) incorrectly refers to the release version as 4.00.08. The HPE OneView version 4.00.08 is now re-versioned as HPE OneView version 4.00.09 to accommodate the last-minute changes in the update kit.

Also, the release notes file embedded with the release distribution file might not include changes that were added after the update kit was created.

The latest versions of release notes are always available at **HPE OneView documentation**.

Changes delivered in HPE OneView 4.00.09 for Virtual Appliance

- Adds new DigiCert root and intermediate certificates to the HPE OneView trust store. These new certificates are required for Remote Support feature of HPE OneView. They enable communications from HPE OneView

to the HPE Remote Support Data Centers, which are using these new certificates starting in November of 2018.

- Adds the following HPE OneView Remote Support:
  - Personally Identifiable Information (PII) at rest has been encrypted.
  - The basic data collection is no longer available to view in the Remote Support UI. This new feature ensures that unencrypted PII data is not exposed, to comply with privacy regulations. Customers can contact HPE support to see an example of collected data or see the **Security and Privacy** white paper.
- Resolves an issue with the State Change Message Bus (SCMB) that sometimes prevented appliance startup.
- Adds support for iLO 5 firmware 1.20 or later to support new SNMPv3 user mapping.
- Resolves the issue that occurs when a volume is created using the scopes of the profile instead of only the intersecting scopes of the user and profile.
- Resolves the issue that occurs when multiple scripts are running concurrently and a change to the SAN attachment of a profile appears to succeed when it was actually blocked from making the change due to another change happening concurrently.
- Resolves the issue where the action to regenerate CHAP credentials is not being restricted to users based on role.
- Resolves the issue where a compliance alert is falsely generated for a server profile when an attachment is removed from a profile template.
- Resolves the issue where HPE OneView configures port monitoring with network analyzer port as eighth port in the HPE Virtual Connect 16Gb 24-Port FC Module, which leads to configuration error in interconnect.
- Resolves an issue where no active alert is created against server hardware for expired iLO certificates (both CA signed and self-signed) during an update from HPE OneView 3.10.xx to 4.00.xx.
- Resolves the issue where the iLO IP address of a rack-based server or blade server in c7000 enclosure is changed but refreshing server was not updating the new iLO IP address and the refresh was failing.
- Resolves the issue when a 3PAR pool in HPE OneView has had all of its volumes moved to another pool through the management console of storage system, the pool in HPE OneView cannot be unmanaged (moved to the discovered state) or removed.
- Resolves the issue where there is no way to clean up a 3PAR pool in HPE OneView that is showing incorrect information regarding volumes present in the pool, when in fact the pool has been deleted from the storage system. There is now a repair call that can be used to correct the problem.

Changes delivered in HPE OneView 4.00.09 for HPE Synergy

- Adds new DigiCert root and intermediate certificates to the HPE OneView trust store. These new certificates are required for Remote Support feature of HPE OneView. They enable communications from HPE OneView to the HPE Remote Support Data Centers, which are using these new certificates starting in November of 2018.
- Adds the following HPE OneView Remote Support:

    - Personally Identifiable Information (PII) at rest has been encrypted.
    - The basic data collection is no longer available to view in the Remote Support UI. This new feature ensures that unencrypted PII data is not exposed, to comply with privacy regulations. Customers can contact HPE support to see an example of collected data or see the **Security and Privacy** white paper.

- Resolves the issue where a Logical Interconnect (LI) Parallel firmware update for the HPE Virtual Connect SE 40Gb F8 was not allowed with servers 'powered on' if Logical Interconnect was in a nonredundant configuration (A-side or B-side) or in a redundant configuration with a firmware mismatch condition causing a stacking failure/non-redundant configuration.
- Resolves an issue with the State Change Message Bus (SCMB) that sometimes prevented appliance startup.
- Adds support for iLO 5 firmware 1.20 or later to support new SNMPv3 user mapping.
- Resolves the issue where clicking the "X" button in the **Port Monitor Edit** window does not remove the monitored port from the list.
- Resolves the issue that occurs when a volume is created using the scopes of the profile instead of only the intersecting scopes of the user and profile.
- Resolves the issue that occurs when multiple scripts are running concurrently and a change to the SAN attachment of a profile appears to succeed when it was blocked from making the change due to another change happening concurrently.
- Resolves the issue where the action to regenerate CHAP credentials is not being restricted to users based on role.
- Resolves the issue where a compliance alert is falsely generated for a server profile when an attachment is removed from a profile template.
- Resolves the issue where the server profile template **Edit** page displays password values in encrypted format though the values were not provided.
- Resolves the issue where subsequent edits of passwords left blank in the Image Streamer OS deployment plan will incorrectly indicate that a password is set.
- Resolves the issue where an In-Service Software Upgrade (ISSU) firmware failed due to not applying the configuration after standby interconnect module got upgraded.
- Resolves the issue when the locale is set to Japanese, due to disk partition error, an incorrect alert appears in HPE OneView on every restart and Image Streamer fails to start up.
- Resolves an issue where no active alert is created against server hardware for expired iLO certificates (both CA signed and self-signed) during an update from HPE OneView 3.10.xx to 4.00.xx.
- Resolves a certificate sync issue between active and standby nodes of the HPE OneView cluster.
- Resolves an issue with HPE OneView cluster formation when a new enclosure is added to the ring and the HPE OneView Composer is moved from an existing enclosure to the newly added enclosure.
- Resolves an issue where HPE OneView Top level Domain (TLD) that is longer than six characters causes invalid domain name in the Add IPv4 subnet and address range.
- Resolves the guidapp service timeout issue, where each allocation request transaction takes approximately 132 milliseconds to 581 milliseconds, causing IPv4 addresses to not be assigned to compute nodes and/or interconnects.
- Resolves the issue when a 3PAR pool in HPE OneView has had all its volumes moved to another pool through the Management Console of storage system, the pool in HPE OneView cannot be unmanaged (moved to the discovered state) or removed.

- Resolves the issue where there is no way to clean up a 3PAR pool in HPE OneView that is showing incorrect information regarding volumes present in the pool, when in fact the pool has been deleted from the storage system. There is now a repair call that can be used to correct the problem.
- Resolves an issue where Frame Link Module fails to communicate to HPE OneView, if IP or hostname is changed on HPE OneView that is associated with CA signed certificate.

HPE OneView 4.00.09 issues and suggested actions for virtual appliances

- **Issue**

  Server profile schema cannot be retrieved using X-Api-version 600.

  Suggested action

  This API is known to not work in the 4.0 release, and is being considered for removal in a future release of HPE OneView. HPE OneView recommends not to use this API.

- **Issue**

  HPE OneView imports and applies profile to an incorrectly programmed HPE Synergy 480 Gen9 with Multi MXM Expansion Module when it must not.

  Symptom

  When a new profile is created from the **Create Profile** dialog in the server hardware page for an HPE Synergy 480 Gen9 with Multi MXM Expansion Module, it fails with this error:

  ```
  Device bay XX of enclosure {"name":"XXXXXX", "uri":"/rest/enclosures/XXXXXXX"}
  is unavailable for a profile to be assigned.
  ```

  Further, when the blade is removed and a profile is created and assigned to the bay and then the blade is reinserted into the same bay, the profile is applied successfully, but incorrectly, to the server.

  Cause

  The primary cause for this issue is an incorrectly programmed "Form factor" on the Field Replaceable Unit (FRU) of some of the HPE Synergy 480 Gen9 Multi MXM Expansion Modules.

  Suggested action

  To correct the problem with the FRU, contact your authorized HPE support representative.

- **Issue**

  Update fails with an "Unknown Error" and the following alert is shown in the UI.

  ```
  [ERROR] The appliance upgrade has failed because the appliance web server
  certificate is about to expire soon.
  [RESOLUTION] Regenerate a new appliance self-signed certificate or re-import a
  new CA signed appliance certificate and then retry the upgrade.
  ```

  Cause

- Appliance certificate might have expired before the update.
- Appliance detected an expired certificate before or during the update and might have reverted to an older certificate or regenerated a new certificate.
- Appliance certificate might be about to expire in less than 24 hours.

Suggested action

1. Check if the appliance certificate is valid and regenerate the certificate if required. To ensure the validity of the certificate, verify:
   - If the certificate is expired or about to expire in another 24 hours
   - If the certificate is an SHA1 certificate
   - If the certificate is missing any of the organizational information configured earlier for the certificate. Some information can be missing if the appliance certificate expires and the appliance is restarted before an updated certificate is installed
   - If you had installed a CA signed certificate previously, but the current appliance certificate is not the one you had installed. The incorrect certificate might appear if the appliance certificate expires and the appliance is restarted before an updated certificate is installed

     In all these cases, regenerate the self-signed appliance certificate or import a new CA signed certificate.
2. Regenerate a new appliance self-signed certificate or reimport a new CA signed appliance certificate.
3. Retry the update.

- **Issue**

  Certificate configuration is lost after update from HPE OneView 4.00.x to 4.00.09.

  Cause

  After appliance is updated from HPE OneView 4.00.x to 4.00.09, user applied certificate configuration under **Settings** > **Security** > **Certificates** would be lost.

  Suggested action

  Go to **Settings** > **Security** > **Certificates** and reapply the user configuration.

- **Issue**

  Unnamed certificates get saved with thumbprint after update from HPE OneView 4.00.x to 4.00.09.

  Cause

  Any certificate that did not have an alias name in the HPE OneView trust store before the update will be given the certificate thumbprint as the alias name.

  Suggested action

  No action required.

- **Issue**

  After port monitoring is configured with network analyzer port as eighth port in the HPE Virtual Connect 16Gb 24-Port FC Module, the operational state of interconnect changes to **`Configuration error`**.

Suggested action

No action required. After update to the 4.00.09 patch, the above behavior will not be seen. The HPE Virtual Connect 16Gb 24-Port FC Module will be in **`Configured`** state.

- **Issue**

  In the online help page, links to sub page of *Troubleshooting appliance issues* and *Interconnects* are broken. The links to the following pages are broken and return the `404 not found` error:

  - *Interconnects > Enable remote support for an interconnect*
  - *Troubleshooting > Troubleshooting appliance issues > Appliance is offline, manual action is required*

  Suggested action

  Navigate to another topic and click **Next** or **Previous** to navigate back to the broken topic.

- **Issue**

  References to Smart Update Tools user guides are incorrect in HPE OneView 4.0 documents.

  Suggested action

  Visit **Hewlett Packard Enterprise Information Library** to find the appropriate guide for your platform.

- **Issue**

  When creating a server profile from a profile template, before saving the profile, user cannot edit the SAN attachment path details (target ports).

  Symptom

  When creating a server profile from a profile template, before initially saving the profile, the GUI for the SAN attachment details is not properly initialized. During this pre-save edit session, several SAN attachment and path fields are not rendered in the GUI, and attempting to edit the target port assignments for the paths will not work.

  Cause

  This is a GUI only issue. The data of the profile from the profile template is actually complete, and will be saved correctly to match the profile template. Once the profile is saved initially, the subsequent editing of the profile works normally, including all the SAN attachment details and path target ports.

  Suggested action

  Create and save the server profile from the profile template, providing a name for the new profile. It is recommended to leave the server hardware assignment unassigned initially for performance reasons. Once the profile is saved, you can immediately edit the profile, making all the desired changes.

HPE OneView 4.00.09 issues and suggested actions for HPE Synergy

- **Issue**

  Logical Enclosure (LE) Orchestrated or Parallel firmware update of an interconnect module in a nonredundant logical interconnect cannot be done without powering off all the servers. When the user wants to update an interconnect module using LE orchestrated/parallel method in a nonredundant logical interconnect with only one interconnect module or a DUS stacking failure, the user must power off all the

servers. Powering of all the servers is not recommended as the servers might be running workloads and powering off the servers would cause traffic loss.

Suggested action

Perform a Logical Interconnect (LI) Parallel firmware update to update the interconnect module.

- **Issue**

  Server profile schema cannot be retrieved using X-Api-version 600.

  Suggested action

  This API is known to not work in the 4.0 release, and is being considered for removal in a future release of HPE OneView. HPE OneView recommends not to use this API.

- **Issue**

  Remote Support is failing after HPE OneView restore operation. When HPE Synergy scale backup restore operation is performed, HPE OneView restores successfully but HPE OneView IPv4 network configuration is not restored.

  Cause

  HPE OneView restore action does not reapply the IPv4 network configuration, which prevents remote support from enabling and connecting to the backend.

  Suggested action

  - Disable remote support globally, if it is not already.
  - Set the networking IP address.
  - Re-enable remote support.
  - Refresh enclosures.

- **Issue**

  HPE OneView imports and applies profile to an incorrectly programmed HPE Synergy 480 Gen9 with Multi MXM Expansion Module when it must not.

  Symptom

  When a new profile is created from the **Create Profile** dialog in the server hardware page for an HPE Synergy 480 Gen9 with Multi MXM Expansion Module, it fails with this error:

  ```
  Device bay XX of enclosure {"name":"XXXXXX", "uri":"/rest/enclosures/XXXXXXX"}
  is unavailable for a profile to be assigned.
  ```

  Further, when the blade is removed and a profile is created and assigned to the bay and then the blade is reinserted into the same bay, the profile is applied successfully, but incorrectly, to the server.

  Cause

  The primary cause for this issue is an incorrectly programmed "Form factor" on the Field Replaceable Unit (FRU) of some of the HPE Synergy 480 Gen9 Multi MXM Expansion Modules.

  Suggested action

  To correct the problem with the FRU, contact your authorized HPE support representative.

- **Issue**

  Inconsistent or loss of configuration in HPE OneView when there is a MultiActive event.

Cause

A MultiActive condition occurs where two Virtual Connect SE 40Gb F8 for Synergy interconnects have a same stacking domain role of the Master interconnect.

Suggested action

- Rectify the stacking connections if there are stacking cable issues.
- Update firmware for compatibility if interconnects have mismatched and incompatible firmware versions.
- Reset interconnect if interconnect is blocking the internal stacking ports due to an internal error.
- If issue persists, call HPE OneView Support.

- **Issue**

  Update fails with an "Unknown Error" and the following alert is shown in the UI.

  ```
  [ERROR] The appliance upgrade has failed because the appliance web server
  certificate is about to expire soon.
  [RESOLUTION] Regenerate a new appliance self-signed certificate or re-import a
  new CA signed appliance certificate and then retry the upgrade.
  ```

  Cause

  - Appliance certificate might have expired before the update.
  - Appliance detected an expired certificate before or during the update and might have reverted to an older certificate or regenerated a new certificate.
  - Appliance certificate might be about to expire in less than 24 hours.

  Suggested action

  1. Check if the appliance certificate is valid and regenerate the certificate if required. To ensure the validity of the certificate, verify:
     - If the certificate is expired or about to expire in another 24 hours
     - If the certificate is an SHA1 certificate
     - If the certificate is missing any of the organizational information configured earlier for the certificate. Some information can be missing if the appliance certificate expires and the appliance is restarted before an updated certificate is installed
     - If you had installed a CA signed certificate previously, but the current appliance certificate is not the one you had installed. The incorrect certificate might appear if the appliance certificate expires and the appliance is restarted before an updated certificate is installed

       In all these cases, regenerate the self-signed appliance certificate or import a new CA signed certificate.
  2. Regenerate a new appliance self-signed certificate or reimport a new CA signed appliance certificate.
  3. Retry the update.

- **Issue**

  Certificate configuration is lost after update from HPE OneView 4.00.x to 4.00.09.

Cause

After appliance is updated from HPE OneView 4.00.x to 4.00.09, user applied certificate configuration under **Settings** > **Security** > **Certificates** would be lost.

Suggested action

Go to **Settings** > **Security** > **Certificates** and reapply the user configuration.

- **Issue**

  Unnamed certificates get saved with thumbprint after update from HPE OneView 4.00.x to 4.00.09.

  Cause

  Any certificate that did not have an alias name in the HPE OneView trust store before the update will be given the certificate thumbprint as the alias name.

  Suggested action

  No action required.

- **Issue**

  Editing a server profile that has the Image Streamer deployment plan with NIC configuration fails if network is changed in the connection used by the NIC.

  Symptom

  When you edit a server profile that has the Image Streamer deployment plan with NIC configuration and you edit a connection used by the NIC attribute to modify only the network, then it fails with the following error:

  ```
  Error: Network uri is not associated with the selected connection.
  ```

  This issue does not apply for REST API user as network URI needs to be updated in the OS Deployment Settings of the profile by the REST client.

  Cause

  When an edit is made to a connection used by a NIC attribute in the server profile only to modify the network linked to the connection, this edit is not tracked for updating NIC configuration in the server profile.

  Suggested action

  When you edit the connection to change the network, make sure you also modify the connection name to reflect the changed network.

- **Issue**

  In the online help page, links to sub page of *Troubleshooting appliance issues* and *Interconnects* are broken. The links to the following pages are broken and return the `404 not found` error:

  - *Interconnects* > *Enable remote support for an interconnect*
  - *Troubleshooting* > *Troubleshooting appliance issues* > *Appliance is offline, manual action is required*

  Suggested action

  Navigate to another topic and click **Next** or **Previous** to navigate back to the broken topic.

- **Issue**

  References to Smart Update Tools user guides are incorrect in HPE OneView 4.0 documents.

  Suggested action

Visit **Hewlett Packard Enterprise Information Library** to find the appropriate guide for your platform.

- **Issue**

  When creating a server profile from a profile template, before saving the profile, user cannot edit the SAN attachment path details (target ports).

  Symptom

  When creating a server profile from a profile template, before initially saving the profile, the GUI for the SAN attachment details is not properly initialized. During this pre-save edit session, several SAN attachment and path fields are not rendered in the GUI, and attempting to edit the target port assignments for the paths will not work.

  Cause

  This is a GUI only issue. The data of the profile from the profile template is actually complete, and will be saved correctly to match the profile template. Once the profile is saved initially, the subsequent editing of the profile works normally, including all the SAN attachment details and path target ports.

  Suggested action

  Create and save the server profile from the profile template, providing a name for the new profile. It is recommended to leave the server hardware assignment unassigned initially for performance reasons. Once the profile is saved, you can immediately edit the profile, making all the desired changes.

Appliance installation instructions

To install HPE OneView 4.00.09 on a new appliance, download and install as instructed in the *HPE OneView Installation Guide*.

Update paths

For the virtual appliance, you can update to HPE OneView 4.00.09 from HPE OneView 4.00.05 or later.

Update prerequisites

These prerequisites apply when you update the virtual appliance to HPE OneView 4.00.09:

- You have installed the HPE OneView 4.00.05 or later version on your appliance.
- You are logged in to the appliance as a user with Infrastructure Administrator privileges.
- No other users are logged in to the appliance and no one logs in during the update.
- Before you begin the update process, use the appliance UI or REST APIs to back up the appliance:
  - Appliance UI: **Settings** > **Actions** > **Create backup** and **Settings** > **Actions** > **Download backup**
  - REST APIs: `/rest/backups` and `/rest/backups/archive`

  NOTE: See the HPE OneView online help topic *Back up an appliance* if you need assistance.

- Before you update the virtual appliance, create a VM snapshot of your appliance.

Update instructions

To update an appliance to version 4.00.09:

Procedure

1. Ensure you have met the **prerequisites**, including backing up the appliance.
2. Download the *HPE OneView 4.00.09 update* (`Z7550-96498.bin`) image file from the **HPE Software Depot** to your local computer. For HPE Synergy, the update (`Z7550-96496.bin`) image file is in **HPE Synergy Software Release** at **www.hpe.com/downloads/synergy**.

   NOTE: For HPE Synergy, if your configuration has Image Streamer present, the update of HPE OneView and Image Streamer must be completed within a 24-hour period.

3. Log in to your appliance and select **Settings** > **Actions** > **Update appliance**.
4. Move the `Z7550-96498.bin` file to the appliance UI screen either by dragging and dropping or browsing to it.

   NOTE: See the HPE OneView online help topic *Update the appliance* if you need assistance.

5. Click **Upload and Install** to start the update process.

Back up the appliance after updating it

After updating your appliance, remember to create a new backup file. The platform type, hardware model, and the major and minor numbers of the appliance firmware must match to restore a backup. The format of the appliance firmware version is as follows:

majornumber.minornumber.revisionnumber-buildnumber

The revision and build numbers do not need to match.

You can only restore backup files created with an HPE OneView 4.00 or later appliance with the identical hardware model.

IMPORTANT: Backups performed on versions prior to HPE OneView 4.00.05 cannot be restored to an appliance updated to the 4.00.09 release.

Make sure to perform new backups after updating to HPE OneView 4.00.09.

Documentation addendum

The following information was made available after publication and does not appear in the HPE OneView 4.0 documentation.

Certificate handling during HPE OneView 4.0 update and during automatic hardware discovery

HPE OneView 4.0 introduces improved security features related to certificate checking for all HTTPS/TLS communications with managed or monitored devices. One of those new features includes improved alerting and policy controls for communicating with devices that have expired certificates. When updating to HPE OneView 4.0, to preserve compatibility with the previous versions of 4.0, HPE OneView will post alerts for devices with expired certificates but continue to allow communications with those devices by default. For example, during the 4.0 update, server hardware iLOs with expired certificates will result in alerts but those devices will continue to be monitored or managed. The same applies to automatic device discovery operations, such as the initial hardware setup of a HPE Synergy frame link topology.

The policy controlling whether expired certificates are treated as errors or warnings is displayed on the **Settings** > **Security** screen. Certificate validation is enabled by default and the setting **`Check for expiration of self-signed certificates`** is disabled by default. This default is intended to simplify 4.0 updates and automatic discovery operations in the presence of expired certificates. It is highly recommended that any expired certificates be renewed as soon as possible, and expiration checking be enabled.

Note that this relaxed expiration checking user preference applies to self-signed certificates in general, but applies to expired CA-signed certificates only during a 4.0 update or automatic discovery operations. For any operations that require a user to validate the certificate of a device, such as adding an external firmware repository or adding a server hardware, an expired CA-certificate is an error and must be corrected before the device can be trusted.

Correcting expired certificates for an iLO

When remediating expired certificates for iLO 2, iLO 3, and iLO 4, perform one of the following:

Procedure

1. If you have your own public key infrastructure (PKI), issue an iLO certificate signing request and install a CA-signed certificate on the iLO. Make sure your CA-root certificate and any intermediate certificates are placed in the HPE OneView trust store. Use the **Settings** > **Security** > **Manage Certificates** > **Add Certificates** screen and paste in the base64-encoded CA-root certificate and any intermediates. Refresh or re-add the server hardware.
2. Update the expired self-signed certificate. iLO generates a new self-signed SSL certificate when iLO is reset to factory defaults or when the iLO hostname is changed. After updating the certificate, add it to the HPE OneView trust store using the **Settings** > **Security** > **Manage Certificates** > **Add Certificates** screen. Select the **`Add certificate from an IP address or hostname`** option and specify the IP address or hostname of the iLO and port 443. You could also select the **`Paste certificate`** option and paste the ILO self-signed certificate. In both cases, remember to select **Force trust leaf certificate**. Refresh or re-add the server hardware.

NOTE: iLO certificates display an **`Issued by`** field of **`Default Issuer (do not trust)`**. These certificates are always treated as self-signed and as such, the **Force trust leaf certificate** option is always used for iLOs not using PKI-issued CA-signed certificates.

3. Some iLO firmware revisions have a known issue where the default self-signed certificate is pre-expired. The **`Valid From`** date is earlier than the **`Valid To`** date in the certificate. See the following iLO customer advisory to fix the issue: **https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c03743622**.

Resolving Frame Link Module to HPE OneView communication failure issue

In HPE OneView 4.00.07, an issue prevents Frame Link Module communication to HPE OneView when FTS is performed or network settings are applied on HPE OneView which has CA signed certificate.

When FTS is performed or network settings are applied in HPE OneView, a new self-signed appliance certificate gets generated. Due to an issue in the product, this newly generated self-signed certificate is not getting propagated to Frame Link Module. That means, at this point, HPE OneView carries the newly generated self-signed certificate and Frame Link Module still carries prior CA signed HPE OneView certificate. So communication to HPE OneView from HPE Synergy Frame Link Module fails. As a result, blade/device insertion/deletion events do not get notified to HPE OneView. Customers might see incorrect or empty IP addresses associated with interconnects, servers, or any other devices in the HPE OneView GUI as well as REST API.

This issue has been resolved in HPE OneView 4.00.09 patch release onwards.

Websites

General websites

Hewlett Packard Enterprise Information Library

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

Storage white papers and analyst reports

Product websites

HPE BladeSystem enclosures

HPE OneView primary website

HPE OneView documentation

HPE OneView user forum

HPE ProLiant server hardware

HPE ProLiant education

HPE Storage products

HPE Synergy documentation

HPE Virtual Connect

For additional websites, see **Support and other resources**.

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.