



**Hewlett Packard  
Enterprise**

# **HPE OneView 4.10.04 Update Release Notes**

## **Abstract**

This document describes changes in HPE OneView software to help administrators understand the benefits of obtaining the 4.10.04 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: P10346-002c  
Published: March 2019  
Edition: 4

## 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..... 4**
  - Introduction..... 4
  - Changes delivered in HPE OneView 4.10.04 for virtual appliances ..... 5
  - Changes delivered in HPE OneView 4.10.04 for HPE Synergy.....6
  - HPE OneView 4.10.04 issues and suggested actions for virtual appliances..... 8
  - HPE OneView 4.10.04 issues and suggested actions for HPE Synergy..... 9
  - Appliance installation instructions..... 10
  - Update paths.....10
  - Update prerequisites.....10
  - Update instructions..... 10
    - Back up the appliance after updating it..... 11
    - Upgrading virtual hardware on virtual machine ..... 11
  
- Documentation addendum..... 13**
  - Certificate management..... 13
  - Scanning tool reports a weak SSH cipher issue ..... 13
  
- Websites..... 15**
  
- Support and other resources..... 16**
  - Accessing Hewlett Packard Enterprise Support..... 16
  - Accessing updates..... 16
  - Customer self repair..... 17
  - Remote support..... 17
  - Warranty information..... 17
  - Regulatory information..... 18
  - Documentation feedback..... 18

# Release description and installation instructions

## Introduction

This document provides release information for HPE OneView version 4.10.04.

- ❗ **IMPORTANT:** The HPE OneView version 4.10.04 replaces version 4.10.03 and includes all the changes introduced in version 4.10.03. Note that HPE OneView version 4.10.03 is no longer available.

Intended audience	Related information
Virtual appliance users	<ul style="list-style-type: none"><li>• <b><u>Changes delivered in HPE OneView 4.10.04 for virtual appliances</u></b> on page 5</li><li>• <b><u>Support and other resources</u></b> about related products and how to find technical documentation</li></ul>
HPE Synergy users	<ul style="list-style-type: none"><li>• <b><u>Changes delivered in HPE OneView 4.10.04 for HPE Synergy</u></b> on page 6</li><li>• <b><u>Support and other resources</u></b> about related products and how to find technical documentation</li></ul>
Users who are installing a new appliance	<ul style="list-style-type: none"><li>• <b><u>Appliance installation instructions</u></b></li><li>• <b><u>HPE OneView 4.10.04 issues and suggested actions for virtual appliances</u></b> on page 8</li><li>• <b><u>HPE OneView 4.10.04 issues and suggested actions for HPE Synergy</u></b> on page 9</li></ul>
Users who are updating from an earlier version of an HPE OneView appliance	<ul style="list-style-type: none"><li>• <b><u>Update prerequisites</u></b> on page 10</li><li>• <b><u>Update instructions</u></b> on page 10</li></ul>

- ❗ **IMPORTANT:**
- 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**.
  - This product may contain references to unreleased products or features and Hewlett Packard Enterprise reserves the right at any time not to commercially release or support any such products or features.

# Changes delivered in HPE OneView 4.10.04 for virtual appliances

---

❗ **IMPORTANT:** \* indicates that the issue was resolved in HPE OneView version 4.10.03. These changes are also applicable in HPE version 4.10.04.

---

- Resolves an issue where a transient fibre channel outage may occur during the HPE OneView upgrade for the HPE Virtual Connect 16Gb 24-port Fibre Channel Module for c-Class BladeSystem.
- Resolves an issue where a Server Profile error and alert message may be displayed if the Server Profile contains a firmware baseline and the server contains a hard drive that uses an eight character firmware version string.
- Resolves an issue where the Fibre Channel uplink port speed changes from 16 Gb/s to 120 Gb/s during HPE OneView upgrade from 4.00.09 to 4.10.01.
- Resolves an issue where after the firmware is updated, HPE OneView does not display an inconsistent alert (One or more firmware components inconsistent with specified firmware baseline) when there is a mismatch between the installed and baseline component version during a forced server profile creation.
- Resolves an issue where the Stack Overflow error is displayed during the appliance startup. This error prevents HPE OneView from updating to version 4.10.01 or 4.10.03. Also resolves an issue where the Stack Overflow error is displayed when the appliance is restarted after updating HPE OneView to version 4.10.01 or 4.10.03.
- The default alert filter for email notifications is now set to critical or warning alerts instead of all alerts. To receive email notification for all alerts, navigate to **Settings > Email Notification > Add Alert Email Filter** under the **Alert Criteria** section and select **All alerts** option.
- **Important notes about updating servers with SPP 2018.06.0 or newer**
  - Resolves an issue where the server profile task is terminated during a firmware update due to a server eFuse that occurs during the update. This eFuse is caused by an imminent CPLD change in the SPP 2018.06.0.
  - Resolves an issue where after an online firmware update using SPP 2018.06.0, the server stays in a powered off state. \*
- Resolves an issue where the server refresh operation fails for rack and c7000 blade servers when the IP address of the managed server's iLO is changed. In this issue:
  - For rack and c7000 blade servers, if the IP address of the managed server's iLO is changed before updating to HPE OneView 4.00.XX, refreshing the server does not update the new IP address after the HPE OneView update. This causes the server refresh operation to fail.
  - For c7000 blade servers, if the IP address of the managed server's iLO is changed, refreshing the server does not update the new IP address after HPE OneView 4.00.XX is updated. This causes the server refresh operation to fail. \*
- Resolves an issue where the remote support `CollectionCleanupModule` stops working and the collections are not cleaned, preventing the appliance update. \*
- Resolves an issue where the logical unit number (LUN) and target port details of a profile cannot be changed in the GUI during profile creation from a profile template. \*
- Resolves an issue where `No SAN could be definitively found` is displayed when a profile template with a boot from SAN volume attachment defined is edited or an unassigned server profile is created in a multiple enclosure environment. \*

- Resolves GUI performance issues when multiple users view server profiles with more than 100 volume attachments each. \*
- Resolves performance issues related to applying server profiles with more than 100 volume attachments. \*
- Resolves an issue where the profile create or edit operation hangs and displays `Unexpected internal error occurred` when a SAN attachment is added. \*
- Resolves an issue where SAN connectivity of the fabric is lost due to removal of 3PAR target aliases from all zones based on stale data. \*
- Resolves an issue where enclosure group configuration scripts are not manageable after HPE OneView is updated from 3.10 to 4.10. \*
- Resolves an issue where the HPE OneView update from 4.0 to 4.1 fails due to duplicate entries in the hypervisor cluster profiles database. \*
- Resolves an issue where users are unable to edit the hypervisor cluster profile when the **Manage vSwitch** option is not selected. \*
- Resolves an issue where vCenter inventory updates are not synced if the vCenter is disconnected in the hypervisor cluster profile. \*
- Resolves an issue where users are unable to edit the hypervisor cluster profile if there is no shared storage available in the server profile template. \*
- Resolves an issue where the hypervisor cluster profiles remediate operation does not wait for SUT to complete online firmware update. \*
- Resolves an issue where the **Smart Search** field is reordered incorrectly and `no email alerts` message is displayed when the **Email Alerting Advanced** text box is used to filter alerts. \*
- Adds support for the new part number P08475-B21 on HPE Virtual Connect 16Gb 24-port Fibre Channel Module for c-Class BladeSystem. The previous part number (751465-B21) continues to be supported. The interconnect hardware is identical for both part numbers. \*
- Adds support for the new part number P08476-B21 on HPE Virtual Connect 16Gb 24-port Fibre Channel TAA Module for c-Class BladeSystem. The previous part number (778720-B21) continues to be supported. The interconnect hardware is identical for both part numbers. \*

## Changes delivered in HPE OneView 4.10.04 for HPE Synergy

---

❗ **IMPORTANT:** \* indicates that the issue was resolved in HPE OneView version 4.10.03. However, these changes are applicable in HPE version 4.10.04 also.

---

- Resolves an issue where a transient fibre channel outage may occur during the HPE OneView upgrade for the HPE Virtual Connect SE 16Gb Fibre Channel Module for Synergy.
- Resolves an issue where a Server Profile error and alert message may be displayed if the Server Profile contains a firmware baseline and the server contains a hard drive that uses an eight character firmware version string.
- Resolves an issue where the Fibre Channel uplink port speed changes from 16 Gb/s to 120 Gb/s during HPE OneView upgrade from 4.00.09 to 4.10.01.
- Resolves an issue where after the firmware is updated, HPE OneView does not display an inconsistent alert (`One or more firmware components inconsistent with specified`

firmware baseline) when there is a mismatch between the installed and baseline component version during a forced server profile creation.

- The default alert filter for email notifications is now set to critical or warning alerts instead of all alerts. To receive email notification for all alerts, navigate to **Settings > Email Notification > Add Alert Email Filter** under the **Alert Criteria** section and select **All alerts** option.

- Resolves an issue where a `This appliance, cannot communicate with its frame. As a result, it cannot form an appliance cluster` message is displayed when an older backup of HPE OneView is restored after a factory reset. Due to this error, a second factory reset of the Frame Link Modules and refresh of the enclosures after the restore must be performed to enable HPE OneView to re-establish a connection with the Frame Link Modules.

- **Important note about updating HPE Synergy with SPP 2018.06.0 or newer**

Resolves an issue where the server profile task is terminated during a firmware update due to a server eFuse that occurs during the update. This eFuse is caused by an imminent CPLD change in the SPP 2018.06.0. \*

- Resolves an issue where an `Incorrect password` error is displayed when the password is changed and then a new hypervisor host is added to an existing hypervisor cluster profile with Image Streamer. \*
- Resolves an issue where the HPE OneView kiosk browser was allowing the addition of components such as blade iLO using a non Federal Information Processing Standard (FIPS) or Commercial National Security Algorithm (CNSA) cipher when HPE OneView is in FIPS or CNSA mode. \*
- Resolves an issue where the interconnects are not configured and remain in `Added With Errors` state and cannot be recovered even by reapplying the configuration. \*
- Resolves an issue where the remote support `CollectionCleanupModule` stops working and the collections are not cleaned, preventing the appliance update. \*
- Resolves an issue where the logical unit number (LUN) and target port details of a profile cannot be changed in the GUI during profile creation from a profile template. \*
- Resolves an issue where `No SAN could be definitively found` is displayed when a profile template with a boot from SAN volume attachment defined is edited or an unassigned server profile is created in a multiple enclosure environment. \*
- Resolves GUI performance issues when multiple users view server profiles with more than 100 volume attachments each. \*
- Resolves performance issues related to applying server profiles with more than 100 volume attachments. \*
- Resolves an issue where the profile create or edit operation hangs and displays `Unexpected internal error occurred` when a SAN attachment is added. \*
- Resolves an issue where SAN connectivity of the fabric is lost due to removal of 3PAR target aliases from all zones based on stale data. \*
- Resolves an issue where the HPE OneView update from 4.0 to 4.1 fails due to duplicate entries in the hypervisor cluster profiles database. \*
- Resolves an issue where users are unable to edit the hypervisor cluster profile when the **Manage vSwitch** option is not selected. \*
- Resolves an issue where vCenter inventory updates are not synced if the vCenter is disconnected in the hypervisor cluster profile. \*
- Resolves an issue where users are unable to edit the hypervisor cluster profile if there is no shared storage available in the server profile template. \*

- Resolves an issue where the hypervisor cluster profiles remediate operation does not wait for SUT to complete online firmware update. \*
- Resolves an issue where the **Smart Search** field is reordered incorrectly and no email alerts message is displayed when the **Email Alerting Advanced** text box is used to filter alerts. \*
- Resolves an issue where a `More Licenses required` message is displayed during the licensing operation after HPE OneView is updated to 4.1. \*

## HPE OneView 4.10.04 issues and suggested actions for virtual appliances

---

❗ **IMPORTANT:** \* indicates that the issue was observed in HPE OneView version 4.10.03. However, these issues also exist in HPE version 4.10.04.

---

- **Important note about updating to HPE OneView version 4.10.04**

### Issue

The memory range for a virtual machine (VM) must be more than 8 Gb and less than 32 Gb before attempting an update to HPE OneView 4.10.04. However, the minimum requirement for the VM memory size is 16 Gb.

The memory range restriction remains in affect even after the update to HPE OneView 4.10.04 is completed successfully. This restriction will be removed in a future release.

### Suggested action

Shut down the virtual appliance, reconfigure the VM to 16 Gb before updating HPE OneView to 4.10.04. See Customer Notification: [a00058523](#) for more information. \*

- **Issue**

HPE OneView displays a `Critical Alert` instead of a `Warning Alert` indicating a firmware mismatch when the logical interconnect configuration is reapplied before firmware activation. This issue occurs during a logical interconnect firmware upgrade with **Stage Only** option selected.

### Suggested action

No action required. Proceeding with the firmware update clears the alert. \*

- **Issue**

In the HPE OneView online help, the link to **Certificate screen details** incorrectly points to the **Settings** page of **Security**.

### Suggested action

From the **Settings: Security** page, navigate to **Security panel screen details > Certificates screen details** to view the details of the Certificates screen.

---

**NOTE:** This issue will be fixed in future releases of HPE OneView.

---

- **Issue**

HPE OneView crashes when an HPE ProLiant DL server with a large number of external hard disk drives is added to the HPE OneView appliance.

### Suggested action

None. This issue will be fixed in future releases of HPE OneView.



# HPE OneView 4.10.04 issues and suggested actions for HPE Synergy

---

❗ **IMPORTANT:** \* indicates that the issue was observed in HPE OneView version 4.10.03. However, these issues also exist in HPE version 4.10.04.

---

- **Issue**

If an HPE Image Streamer deployment plan with **String type Custom Attribute** containing a \ character in the regular expression (regex) pattern is used then, the server profile will not be created.

**Suggested action**

Remove the \ character in the regex pattern of the **String type Custom Attribute**. \*

- **Issue**

An `Incorrect password` error is displayed when the password is changed and then a new hypervisor host is added to an existing hypervisor cluster profile with HPE Image Streamer.

---

**NOTE:** This issue is fixed in the HPE OneView 4.10.03 patch. The following steps are applicable only if older HPE Image Streamer artifact bundles are being used.

---

**Cause**

The management NIC is configured first and then the password is configured. The cluster Resource Manager (RM) detects that the management NIC is configured and attempts to add the hypervisor to the vCenter but the operation fails since the password is not yet customized in the hypervisor.

**Suggested action**

Ensure that the password customization step is performed before the NIC customization step in the HPE Synergy Image Streamer build plan. Alternatively, retry the operation by using the latest artifact bundles for VMware ESXi published by HPE. \*

- **Issue**

During a server profile creation with OS deployment settings containing NIC configurations using auto constraint through REST API, the server profile is created even if the required DNS IP address is not available in the subnet.

**Cause**

The server profile does not validate the availability of the DNS IP address in the subnet associated with a network used by the NIC in the OS deployment settings.

**Suggested action**

Ensure that the required number of DNS IP addresses are available in the subnet as per the HPE Image Streamer deployment plan. \*

- **Issue**

HPE OneView displays a `Critical Alert` instead of a `Warning Alert` indicating a firmware mismatch when the logical interconnect configuration is reapplied before firmware activation. This issue occurs during a logical interconnect firmware upgrade with **Stage Only** option selected.

**Suggested action**

No action required. Proceeding with the firmware update clears the alert. \*

- **Issue**

In the HPE OneView online help, the link to **Certificate screen details** incorrectly points to the **Settings** page of **Security**.

#### **Suggested action**

From the **Settings: Security** page, navigate to **Security panel screen details > Certificates screen details** to view the details of the Certificates screen.

---

**NOTE:** This issue will be fixed in future releases of HPE OneView.

---

- **Issue**

HPE OneView crashes when an HPE ProLiant DL server with a large number of external hard disk drives is added to the HPE OneView appliance.

#### **Suggested action**

None. This issue will be fixed in future releases of HPE OneView.

## Appliance installation instructions

To install HPE OneView 4.10.04 on a new appliance, download and install as described in the *HPE OneView Installation Guide*.

## Update paths

For a virtual appliance, you can update to HPE OneView 4.10.04 from HPE OneView 3.10.04 or later.

## Update prerequisites

These prerequisites apply when you update the appliance to HPE OneView 4.10.04:

- You have installed HPE OneView 3.10.04 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 a virtual appliance, create a VM snapshot of your appliance.

## Update instructions

To update an appliance to version 4.10.04:

#### **Procedure**

1. Ensure that you have met the **prerequisites**, including backing up the appliance.
2. Download the *HPE OneView 4.10.04 update* image file from the **HPE Software Depot** to your local computer. For HPE Synergy, the update image file is in **HPE Synergy Software Release** at [www.hpe.com/downloads/synergy](http://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 image 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**.
6. When the file upload and verification is complete, read and accept the license agreement and then click **Update** 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 4.10 or later appliance with the identical hardware model.

---

**!** **IMPORTANT:** Backups performed on versions prior to HPE OneView 4.10 cannot be restored to an appliance updated to the 4.10.04 release or vice versa.

Make sure to perform new backups after updating to HPE OneView 4.10.04.

---

## Upgrading virtual hardware on virtual machine

HPE OneView incorporates the appropriate updates to mitigate against the Spectre and Meltdown vulnerabilities.

HPE OneView itself is not vulnerable to Spectre/Meltdown; the security updates are incorporated in HPE OneView for completeness.

In a VMware environment, the hardware version of a virtual machine determines which virtual hardware features are available to a virtual machine. This is referred to as the "VM version" or "Compatibility" of a VM in the VMware user interface. VMware requires that a virtual machine has hardware version 11 or later in order for all the appropriate Spectre/Meltdown hypervisor host hardware fixes to be properly virtualized for use by guest VMs. A new installation of the HPE OneView virtual appliance supports virtual hardware version 11.

For an upgrade installation, the administrator must manually perform a one-time update of the hardware version for the HPE OneView virtual appliance if at less than hardware version 11.

The following example uses the VMware vSphere Client to perform the update.

1. Check the hardware version of the current HPE OneView virtual appliance. If it less than version 11, continue with the steps below.
2. Gracefully shut down the virtual appliance.
3. To update the hardware version of the virtual appliance, right-click the virtual machine and select the menu option to upgrade virtual hardware. The interface differs slightly depending on the version and type of VMware vSphere Client:

- a. For the locally installed VMware vSphere Client, the option is **Upgrade Virtual Hardware**.
- b. For the VMware vSphere Web Client, select **Compatibility > Upgrade VM Compatibility**.

---

**NOTE:** The Upgrade Virtual Hardware or Upgrade VM Compatibility options only appear if the virtual hardware on the virtual machine is not the latest supported version.

---

- c. Select a compatibility option of VMware ESXi 6.0 or later. Note that VMware ESXi 6.0 corresponds to hardware version 11.
- d. To continue with the virtual hardware upgrade, click **Yes**.
- e. Power on the HPE OneView virtual appliance.

# Documentation addendum

The following information was made available after publication and does not appear in the HPE OneView 4.1 documentation.

## Certificate management

The certificate that is generated by default on a newly installed appliance is an RSA certificate. Currently, only RSA certificates are supported for the appliance certificate.

### Prebundled certificates

HPE OneView prebundles the following root and intermediate CA certificates that are required for the secure and trusted communication with the remote support server:

- Verisign Root CA - VeriSign Class 3 Public Primary Certification Authority - G5
- Symantec Intermediate CA - Symantec Class 3 Secure Server CA - G4
- Verisign Root CA - VeriSign Universal Root Certification Authority
- Symantec Intermediate CA - Symantec Class 3 Secure Server SHA256 SSL CA
- DigiCert Root CA - DigiCert Global Root G2
- DigiCert Intermediate CA - DigiCert Global CA G2

### Certificate revocation lists

HPE OneView raises alerts when certificate revocation lists (CRLs) are about to expire or have expired. These notifications are disabled by default. Hewlett Packard Enterprise recommends that you enable CRL expiry notification so that up-to-date CRLs are uploaded to the appliance on time and strict revocation checking is done.

For CRL revocation checking of the certificate that belongs to *www.hpe.com*, you must upload CRLs for the following:

- VeriSign Class 3 Public Primary CA
- VeriSign Universal Root CA
- Symantec Class 3 Secure Server CA
- Symantec Class 3 Secure Server SHA256 SSL CA
- DigiCert Root CA - DigiCert Global Root G2
- DigiCert Intermediate CA - DigiCert Global CA G2

---

**!** **IMPORTANT:** The CRLs for HPE OneView appliance certificate and the user's client certificates must be up-to-date to use the two-factor authentication feature. An `Invalid or no certificate. Contact your administrator for assistance` message is displayed if the CRLs have expired.

---

For information on uploading CRLs, see the *HPE OneView Online Help*.

## Scanning tool reports a weak SSH cipher issue

Security vulnerability scanning tools such as Nessus report that HPE OneView's ssh server supports Cipher Block Chaining (CBC) ciphers and that these ciphers may allow an attacker to recover plaintext

messages from the ciphertext. These scanners report reference to CVE-2008-5161 which describes an issue with the Secure Shell protocol discovered in 2008.

### **Suggested action**

No action is required at this time.

This is a false positive from the scanners. This SSH protocol vulnerability was fixed in 2009 which predates HPE OneView. All HPE OneView versions have an SSH server that is not vulnerable to this issue. Scanners like Nessus also note that they only check for the presence of CBC cipher support but they do not actually check for vulnerable software versions (See <https://www.tenable.com/plugins/nessus/70658>). Not only is the cipher not vulnerable in all modern SSH implementations, CBC ciphers are required to be supported by security standards such as Common Criteria's Network Device Collaborative Protection Profile (See [https://www.niap-ccevs.org/MMO/PP/cpp\\_nd\\_v2.0e.pdf](https://www.niap-ccevs.org/MMO/PP/cpp_nd_v2.0e.pdf)).

For additional details regarding CVE-2008-5161, see <http://community.arubanetworks.com/t5/Wireless-Access/SSH-and-AES-CBC/td-p/248919>

# 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](#).

# 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](http://www.hpe.com/support/hpesc)

### **Hewlett Packard Enterprise Support Center: Software downloads**

[www.hpe.com/support/downloads](http://www.hpe.com/support/downloads)

### **Software Depot**

[www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)

- To subscribe to eNewsletters and alerts:

[www.hpe.com/support/e-updates](http://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](http://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](http://www.hpe.com/services/getconnected)

#### HPE Proactive Care services

[www.hpe.com/services/proactivecare](http://www.hpe.com/services/proactivecare)

#### HPE Proactive Care service: Supported products list

[www.hpe.com/services/proactivecaresupportedproducts](http://www.hpe.com/services/proactivecaresupportedproducts)

#### HPE Proactive Care advanced service: Supported products list

[www.hpe.com/services/proactivecareadvancedsupportedproducts](http://www.hpe.com/services/proactivecareadvancedsupportedproducts)

#### Proactive Care customer information

##### Proactive Care central

[www.hpe.com/services/proactivecarecentral](http://www.hpe.com/services/proactivecarecentral)

##### Proactive Care service activation

[www.hpe.com/services/proactivecarecentralgetstarted](http://www.hpe.com/services/proactivecarecentralgetstarted)

## Warranty information

To view the warranty information for your product, see the links provided below:

#### HPE ProLiant and IA-32 Servers and Options

[www.hpe.com/support/ProLiantServers-Warranties](http://www.hpe.com/support/ProLiantServers-Warranties)

#### HPE Enterprise and Cloudline Servers

[www.hpe.com/support/EnterpriseServers-Warranties](http://www.hpe.com/support/EnterpriseServers-Warranties)

#### HPE Storage Products

[www.hpe.com/support/Storage-Warranties](http://www.hpe.com/support/Storage-Warranties)

#### HPE Networking Products

[www.hpe.com/support/Networking-Warranties](http://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](http://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](http://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](http://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](http://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](mailto: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.