Hewlett Packard
Enterprise

HPE OneView 4.0 Release Notes for HPE Synergy

Abstract

This document describes new features, installation and update instructions, and known limitations for HPE OneView 4.0 for HPE Synergy. This release is intended for administrators who configure, manage, and troubleshoot compute modules, interconnects, and storage systems on HPE Synergy using HPE Synergy Composer powered by HPE OneView.

Part Number: P01319-001
Published: December 2017
Edition: 1

Legal Notice

Confidential computer software. Valid license from HPE 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.

The information contained herein is subject to change without notice. The only warranties for HPE 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. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgements

Google® is a registered trademark of Google Inc. Microsoft® and Windows® are trademarks of the Microsoft Group of companies. VMware® is a registered trademark of VMware Inc.

Warranty

Hewlett Packard Enterprise will replace defective delivery media for a period of 90 days from the date of purchase.

Contents

Release description and installation instructions

Introduction

This document provides release information for HPE OneView 4.0 for HPE Synergy.

Intended audience	Related information
All users	• **Key features** • **Documentation addendum** • **Support and other resources** about related products and how to find technical documentation
Users who are installing a new appliance	• **Appliance installation instructions** • **Issues and suggested actions** for using HPE OneView 4.0 for HPE Synergy

For the latest updates in information, visit **Hewlett Packard Enterprise Information Library**.

Changes delivered in HPE OneView 4.0 for HPE Synergy

- Resolves an issue with dialog buttons when using Chrome version 53.0.
- Resolves potential traffic loss on Multi-Module Link Aggregation (MLAG) when all stacking links are down and HPE Synergy Interconnect Modules (ICMs) are configured for dual unit stacking.
- Resolves an issue with the **UEFI iSCSI Boot Policy** field on the **Edit BIOS Settings** page not being applied.
- Resolves an issue where HPE OneView displayed an incorrect firmware version number for the I/O adapters of the HPE Synergy D3940 Storage Module on the logical interconnect (LI) and logical enclosure (LE) view pages.
- Resolves an issue where performing simultaneous firmware updates on multiple SAS logical interconnects only updated the first and might have failed for the rest.

New features in HPE OneView 4.0 for HPE Synergy

Security

- Scope Based Access Control

  SBAC extends today's role based access control by restricting a role (e.g. Server, Storage, or Network Admin) to operate only on a subset of resources managed by the appliance. The subset of resources is defined by the Scope feature which is a logical group of resources. For example, a Server Administrator named Sarah can only manage the server's in the "Production" scope.

- 2-Factor Authentication (CAC/PIV)

  Provides the ability to authenticate using smartcards. Smartcards supported include Common Access Card (CAC)/Personal Identity Verification (PIV) cards. The feature is integrated with HPE OneView's Active

Directory support. The users supply a PIN and their certificate on the smartcard to be matched/validated against their account in the directory.

- Certificate Management

  Certificate management improves the policies and procedures for managing certificate-based trust. For example, ability to manage the HPE OneView certificate trust store, support for certificate revocation, management of self-signed certificates, etc.

  HPE OneView 4.0 adds extensive certificate management features including:

  - Support of Certificate Authority (CA) signed certificates for iLOs, Onboard Administrators, Frame Link Modules, remote repositories, proxy servers, etc.
  - Support for Certificate Revocation Lists (CRLs)
  - Automatically trusting self-signed certificates during initial device discovery
  - Management of the HPE OneView certificate store
  - Alerts for certificate expiration related events
  - Security preferences to control the strictness of certificate validation

- SNMPv3

  Earlier versions of HPE OneView use SNMPv1 for health monitoring of server hardware. HPE OneView 4.0 supports health monitoring via the more secure SNMPv3 protocol. This feature is available for servers using iLO4 or later. HPE OneView automatically updates to use SNMPv3 during the next refresh event for the server (e.g. an HPE OneView reboot and an explicit refresh for a server). HPE OneView can also forward SNMP traps using SNMPv3. That includes any incoming SNMPv1 traps from the managed or monitored devices. Such traps are automatically converted to SNMPv3 and forwarded. Support for forwarding via SNMPv1 is preserved for backward compatibility.

Storage

- Boot from SAN configuration load balancing - connections and targets

  Enables boot from SAN (BFS) configuration to be specified in a server profile or server profile template such that connection primary/secondary assignment and storage system target port selection configuration will be load balanced uniformly over SANs and storage system targets resulting in full utilization of SAN and storage system infrastructure automatically. There is no more need to maintain multiple storage profile templates requiring administrators to track the alternating of boot configuration across servers.

- Volume template and property locking integration with SP/SPT

  Provides a consistent, unified storage volume management experience managing volumes across all of HPE OneView. Volume templates, property locking and all of the volume settings can be managed in volume templates, volumes, server profiles and server profile templates.

- iSCSI CHAP credential regeneration

  Enables re-generation of iSCSI data path CHAP credentials across server & storage systems to support data center password rotation policies.

Virtual Connect

- LACP on s-channels - When combined with Multi-Module LAG (MLAG) on uplink ports, provides true end-to-end link aggregation from the compute node to the upstream network infrastructure. This capability is an integral part of the frictionless firmware update capability for Master/Satellite architecture. It provides seamless failover between adapter ports and enhances server traffic load-balancing. It allows server administrators to use switch assisted NIC teaming policies.
- Mixed-speed Master/Satellite ICM Configurations - This capability allows Synergy customers to fully populate their racks with up to 4x Synergy frames and tailor compute modules bandwidth requirements to the need of their applications combining 10 Gb and 20 Gb traffic within the same set of frames and interconnects.
- SmartLink and non-Redundant Configs - For VC on Synergy, an Active/Active configuration is an Ethernet network configuration that allows active traffic on the same VLAN to egress multiple VC interconnect modules and provides full use of all uplink ports (no uplink port in standby mode), doubles the available bandwidth while maintaining redundancy when combined with SmartLink capability and provides seamless failover in case one of the interconnects' uplink ports is disconnected from the production network. SmartLink is essential for VC modules to automatically drop links to the server profile connections if all uplink ports for networks assigned to those connections lose their uplink ports.
- Pause flood detection and protection - Ethernet switch interfaces use a pause frame based flow control mechanism to throttle data flow from link partners. When a pause frame is received on a flow control enabled interface, the transmit operation is stopped. All other traffic is queued up. A steady stream of pause frames received for extended periods of time will cause queuing resources to become exhausted. This condition can severely impact the switch operation on all interfaces and ability of the switch to process control protocol traffic. This capability monitors all of the switch ports for pause flood condition and prevents resource exhaustion on the switch.
- Synergy Non-Disruptive Firmware Update - In configurations providing full end-to-end redundancy including redundant server profile connection configuration, redundant upstream switch connectivity and Logical Interconnect uplink sets with LAGs enabling dynamic "path failover", this feature provides non-disruptive firmware update where Synergy networking infrastructure can be updated without network errors or network performance degradation for applications running on host compute modules.
- Private Network support - Private network provides network security by limiting server-to-server traffic flow for a given network. Server ports or server profile connections associated with a private network cannot communicate directly with each other within the same Layer 2 Ethernet domain. All traffic that has another server as a destination must egress through an uplink port and be routed through an external layer 3 router.
- Increase VLAN scale for network sets - Larger numbers of explicit VLANs improve Synergy networking use cases, specifically interoperability with Cisco ACI, this feature lifts the 162 limit per network set and will allow dynamic scaling of network set limits based on the LIG/LI size.
  - 1x frame LIG/LI - 1000 VLANs
  - 2x frame LIG/LI - 500 VLANs
  - 3x frame LIG/LI - 333 VLANs
  - 4x frame LIG/LI - 250 VLANs
  - 5x frame LIG/LI - 200 VLANs
- Connections without assigned network - Server administrators can reserve server 'port' and assign networks later while server power is on. This promotes the following use cases:
  - Server connectivity pre-provisioning - customer knows number of connections (NIC ports) the server will require, but does not want server to be 'chatty' on the production networks during OS provisioning.
  - Eliminates need to power off a server to add connectivity to production workloads.

    - Allocation of virtual MACs and WWNs prior to server acquisition and OS install further optimizes customer processes.
    - Allows user to disable profile connection without powering off the server.

- Configuration performance improvements - improvements in ability to discover and configure Synergy resources faster than in previous releases, improves time to create a Logical Enclosure by 60%, reduces the time that it takes to create a server profile by 75%.
- Remote Support - Remote support for Synergy Interconnects. Hardware faults will automatically trigger support cases.
- HPE Virtual Connect SE 16Gb 24-port Fibre Channel Module for HPE Synergy firmware (4.00.33 or higher required)
    - HPE Virtual Connect SE 16Gb FC Module for HPE Synergy port trunking - This capability maximizes the IO performance and reduces downtime due to single or multiple link failures, eliminates throughput dependency for the IO completion on a single physical link and provides nearly the aggregate performance of all the links that participate in the trunk. While eliminating single or multiple points of failure, traffic continues to flow even if a link or multiple links within a trunk are compromised.
    - Adds support for port monitoring.
    - Removes the use of some older and weaker SSH and TLS Ciphers: aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc, DES-CBC3-SHA.
    - Resolves security vulnerabilities for CVE-2016-0800, CVE-2016-6515, CVE-2015-8325, CVE-2015-0291, and CVE-2016-2183.

Appliance installation/update instructions

For installation instructions, refer to documents available at **www.hpe.com/info/synergy-docs**.

The update is in the Release Set at **www.hpe.com/downloads/synergy**.

Back up the appliance after the update

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 HPE OneView 4.0 for HPE Synergy Composer with the identical hardware model.

Issues and suggested actions

The issues and known limitations in this release are described here.

Issue with SAN auto-zoning feature

SAN auto-zoning feature is incompatible with HPE Smart SAN for 3PAR target driven peer zoning.

Suggested action

When using HPE OneView SAN auto-zoning, do not simultaneously zone the SAN with 3PAR Smart SAN zoning.

CHAP name length limit

When configuring iSCSI connections in a server profile for a server containing Qlogic or Broadcom adapters, the CHAP name should not be more than 128 characters. The maximum CHAP name length for these adapters is not enforced by HPE OneView 4.0, and can cause the blade to fail to connect to the storage if exceeded.

Issue with server power state when performing Logical Interconnect firmware update

When performing a logical interconnect firmware update using the parallel activation method, server power state is not validated and the update is not blocked when some servers are powered on. The logical interconnect firmware update screen already provides clear indication of the potential outage.

Suggested action

Update the logical interconnect firmware via the firmware update action on the logical enclosure, selecting the **shared infrastructure** option, or power off the servers prior to the logical interconnect firmware update using the parallel activation method.

UEFI iSCSI Boot Policy field in Edit BIOS Settings page will not be applied

HPE OneView provides the ability to set and display the iSCSI Boot Policy field in **Edit BIOS Settings** page, however, this setting will be ignored.

Suggested action

Boot to RBSU and change the iSCSI Policy setting in the **Network Boot Option**.

High Availability (HA) warning alert for single HPE Synergy Composer configurations is not clearable

Hewlett Packard Enterprise strongly recommends configuring HPE Synergy systems in an approved High Availability configuration (HPE Synergy Composers). Users who intentionally opt to configure their system with a single HPE Synergy Composer will see a locked High Availability warning (yellow) alert and will be unable to clear that alert during the life of that configuration.

Suggested action

Move to a High Availability configuration as soon as possible. There is currently no method to disable the alert until an HA-conformant configuration is adopted.

Remote support data collection fails during server hardware removal and insertion

Performing server hardware removal and insertion during scheduled remote support data collections may cause collections to fail.

Suggested action

Schedule server hardware removal and insertion outside of a scheduled collection operation or change the planned time of the scheduled collection.

Remote support not enabled after a server is inserted

When a server with remote support enabled is removed and re-inserted into an enclosure, remote support may not be re-enabled for the server hardware. This can be seen by looking at the remote support configuration of the server hardware and seeing that the remote support status is shown as disabled.

Suggested action

Refresh the server hardware to re-enable remote support.

Issue during first-time setup of the HPE Synergy Composer

If an in-use IP is entered during the first-time setup of the HPE Synergy Composer, the in-use IP is not used but no alert is generated to warn the user that High Availability (HA) is not enabled.

Suggested action

Ensure all IP addresses configured during first-time setup of the HPE Synergy Composer are not in use within the management network.

Duplicate alerts seen in activity page when a server is powered on

When a server is powered on, duplicate (up to 4) **server powered on** and **server reset detected** lifecycle alerts may be seen on the activity page.

Suggested action

Ignore the duplicate lifecycle alerts.

Boot from SAN configuration settings may be lost when server hardware is removed and re-inserted

The default boot drive configuration may be lost and the server will not automatically boot when all of the following are true:

- The boot device is remote; e.g., a boot from a Storage Area Network (SAN) device or zoned local storage.
- The server profile boot mode is Unified Extensible Firmware Interface (UEFI).
- The operating system being used is either SUSE Linux Enterprise Server 11 SP3 and SP4 or Red Hat Enterprise Linux 6.x.

And one of the following occurs:

- The server hardware is replaced.
- The server hardware NVRAM is cleared.
- The server profile is moved to new server hardware.

Suggested action

See **CA c05306567** for full details and corrective actions.

Create/Create+/OK buttons do not work on server profile create/edit dialogs

After creating or editing a server profile that includes an OS deployment plan, a subsequent create/edit of a server profile that does not include an OS deployment plan may result in the **Create/Create+/OK** buttons on the dialog being unresponsive.

Suggested action

Refresh the browser and attempt the operation again. To prevent this situation, refresh the browser after any create/edit operation involving OS deployment plans.

Active Directory authentication error message

When adding Active Directory authentication to HPE OneView you may experience an error if the addresses for the Active Directory servers are specified using a DNS name rather than the numeric IP address. The error message is:

“Unable to reach directory server <DNS name> with configured port <port number>. Unable to ping directory server <DNS name>.”

Suggested action

Use a numeric IP address when adding a directory server to HPE OneView.

Recommended Cisco top-of-rack switch configuration for FCoE VLANs

When using HPE OneView to manage HPE Synergy interconnect modules configured with FCoE VLANs, it is recommended to use VFC MAC-address binding with Cisco top of rack switches.

Suggested action

This recommendation applies to HPE Synergy interconnects that are connected to Cisco switches. When deploying servers with HPE OneView using multi-hop FCoE out of the logical enclosure to external Cisco switches, as part of the external switch configuration you need to manually configure the vSAN and vfc interfaces binding to each server’s mac address. While HPE OneView SAN storage configuration automates zoning configuration in the SAN, it does not configure the vfc interfaces which are configured at the edge of the SAN. Those must be configured manually.

Be sure to use a Cisco firmware release after March 2016 to avoid the Cisco defect (CSCug84860) concerning MAC address binding.

Note that when using server profile virtual MAC addresses you’ll have to do this for each server after applying your profile. If you’re using physical MAC addresses, then you can configure the vfc’s once and then apply as many profiles as desired.

Online help Server Hardware screen mentions Adapters as header instead of Ports

On the Server Hardware screen, the section titled **Ports** is documented as **Adapters** in the online help.

Suggested action

Note that the **Adapters** help page refers to the **Ports** UI screen.

Replacing active Frame Link Module (FLM) with FLM running same version of Firmware caused "Refresh" error to be reported in HPE OneView

If an HPE OneView user removes an active **Frame Link Module** and then inserts the replacement before the standby Frame Link Module that is able to take over the Frame, which will display errors in HPE OneView.

Suggested action

Manually refresh the enclosure to clear the errors.

Refresh fails to report a blade that has changed bay when HPE OneView is offline

If servers are moved between bays while HPE OneView is not running, the servers might report errors when HPE OneView is booted back up.

Suggested action

Refresh the enclosure until the errors get cleared and the blades are reported in their proper position.

3PAR Persistent Ports port pair direct attach cabled to different interconnect modules is not supported

The appliance does not support the storage configuration where a pair of ports on a 3PAR StoreServ array are configured for Persistent Ports failover and are cabled for direct attach to two different interconnect modules on an enclosure.

Suggested action

Either disable Persistent Port functionality on the 3PAR StoreServ array (for all ports on the array), or change the direct attach cabling to ensure partnered ports are connected to the same interconnect module.

Changing iSCSI Policy BIOS to non-default value on HPE Synergy Gen10 server results in boot failure

If you change the iSCSI Policy BIOS to non-default value (i.e. Adapter Initiator) on an HPE Synergy Gen10 server, the iSCSI Software boot attempts will not connect to targets and server will not boot.

Suggested action

Boot to RBSU and change the iSCSI Policy setting in the **Network Boot Option to Software Initiator**.

Alert indicating that the deleted networks are still using the connection

After removing networks and updating server profile templates, users may see that some server profiles will have an alert indicating that the deleted networks are still assigned to connections. This is an incorrect alert given the changes made to the profile and are cleared by refreshing the server profile. This can be done through the **Profile Actions** menu.

Suggested action

Refresh the affected server profiles via the **Server Profile Refresh** action in the user interface.

Profile creation fails when selecting internal drives on a Smart Array mezzanine controller

Profile fails with the error, "Unable to apply local storage settings. The Smart Storage Administrator tool failed with the following error message: **ERROR (2829)**, Cannot create array. There are no disks". This is due to 'internal drives' being selected in the profile, but no HPE Premium Backplane Hard Disk Drive Upgrade kit is configured on the mezzanine controller.

Suggested action

Do not select 'internal drives' on the Smart Array mezzanine controller when the HPE Premium Backplane Hard Disk Drive Upgrade kit is not present.

No alerts, incorrect profiles and connections state when deleting network from uplink set

When removing networks from two or more uplink sets in a logical interconnect group and running update from group with server profiles that have active references to the removed networks, some server profiles may continue to show healthy connections even though the network has been removed from the interconnect.

Suggested action

Limit network removals through this technique to a single uplink set in the logical interconnect group. Alternatively, the logical interconnect may be directly edited to remove the networks from one or more uplink sets and then followed up with an edit of the associated logical interconnect group to bring the logical interconnect and the logical interconnect group into compliance. Lastly, if the removal was unintentional, restoring the networks to the logical interconnect group and running a second update from group correctly restores connectivity for all connections.

Remote console window opens but does not connect to the server

When you launch the iLO5 remote console from HPE OneView, the remote console window opens but may not connect to the server.

Suggested action

Log in to the iLO5 web interface and launch the remote console from the iLO5 interface to access the server console.

Removing a frame managed by HPE Synergy Composer 4.0

Removing a frame managed by HPE Synergy Composer 4.0 does not remove the Frame Link Module’s (FLM) self-signed certificate within HPE OneView.

Suggested action

To remove the self-signed certificate manually from the HPE Synergy Composer console, go to **Settings** > **Security** > **Manage Certificates**. Search for the certificate associated with the FLM name.

Not manually removing the self-signed certificate will have no effect on HPE Synergy Composer operation with other frames.

Unable to change connection back to iSCSI bootable if connection was one of the two iSCSI boot connections using DHCP and managed volume

When editing a profile that has two iSCSI boot connections, where the first is primary bootable and the second is not bootable, modifying the second connection to be a secondary bootable iSCSI connection using DHCP and a managed volume will result in the validation error "Unable to update profile". The resolution is to ensure all bootable connections using an Ethernet function type and iSCSI boot parameters share the same initiator name.

Suggested action

1. Delete the non-bootable connection
2. Add a new iSCSI bootable connection

Remote FLM certificate is re-accepted by HPE OneView after manual removal

When the user manually deletes a FLM certificate in a remote ring from a HPE OneView UI, HPE OneView re-accepts the certificate automatically when trying to reconnect to the same FLM.

HPE OneView SNMP configurations on iLO5 get corrupted when server is refreshed immediately after the iLO is reset

If a server hardware that is being managed by HPE OneView is refreshed immediately after the iLO5 on the managed server is reset, the SNMP configurations that HPE OneView sets on the iLO5 may get corrupted. This will cause SNMP traps from the iLO5 to no longer be received in HPE OneView. This impacts server monitoring and some aspects of server management such as profile application and power control.

Suggested action

Wait approximately 1 minute after iLO5 has started responding and refresh the server in HPE OneView again. This will restore the SNMP settings on the iLO and ensure that HPE OneView can continue monitoring and managing the server.

Gen10 hardware is not discovered by HPE OneView

When importing enclosures into HPE OneView or adding Gen10 compute modules into an enclosure, the HPE OneView **Hardware Setup** screen or the **Server Hardware** screens do not show any Gen10 hardware listed. This is caused when software or firmware versions are running in HPE Synergy that do not support discovery of Gen10 hardware:

- The HPE Synergy Frame Link Module is running a 1.x firmware version.
- The HPE Synergy Composer is running a 3.00.xx version of HPE OneView.

Suggested action

1. Download the latest release set for HPE Synergy (3.10.Gen10.20170721 or higher).
2. From the release set, extract the HPE Synergy Composer firmware bundle, which includes the update for HPE OneView (3.10.04 or later).
3. Update HPE OneView.
4. From the release set, extract the HPE Synergy Custom SPP Bundle and save it to a firmware repository.
5. Navigate to the **Logical Enclosures** screen, and update the firmware on the Frame Link Module.
6. Once the Frame Link Module is successfully updated to 2.0 (or later), any Gen10 compute modules should be visible in the **Hardware Setup inventory** screen or the **Server hardware overview** screen for verification. If the compute modules are not visible, refresh the enclosure to force discovery.

Create Server Profile online help page does not specify NIC teaming option

On the online help page for **Create Server Profiles**, the **OS deployment screen** does not include information about the NIC teaming option.

Suggested action

The OS deployment screen allows you to team two similar network connections for a teamed NIC attribute. NIC teaming allows you to combine two NIC attributes into a single NIC team attribute, ensuring both connections are to the same network, and allows the deployment plan to indicate if teaming is optional or required for the OS/application to run correctly. The deployment plan is then able to more easily correctly configure a NIC team which prevents the OS from seeing redundant NIC traffic.

Limitations when using Software Administrator role

The Software Administrator role was created to allow the Infrastructure Administrator to delegate rights to manage HPE Synergy Image Streamer resources (e.g., Deployment Plans, Golden Images, OS Build Plans, Plan Scripts, Archive Bundles, etc.) without granting the user the right to manage all HPE OneView resources (e.g., Enclosures, LEs, LIGs, LIs, networks, users, groups, etc). But this limits the Software Administrator role. For example, users with this role are not allowed to view the details of tasks they initiated or alerts associated with their resources.

Suggested action

Grant Infrastructure Administrator rights to the Software Administrator. Refer to the following link to edit the privileges: **Edit a local user account (as Infrastructure administrator)**.

Expired certificate alerts created incorrectly as critical, locked alerts instead of warning alerts

HPE OneView has a new certificate-related security setting: "Check for expiration of self-signed certificates". The setting is disabled by default. When disabled, a warning alert is displayed for any device with an expired certificate on the device's resource page (e.g. server hardware page). Additionally, separate alerts for expired certificates are displayed on the Settings/Activity page. These latter alerts are created incorrectly as critical, locked alerts (red alerts) for self-signed certificates instead of warning alerts.

Suggested action

Communications with devices is not impacted by these specific critical alerts. Both the warning and the critical alerts are cleared automatically when the expired certificates are fixed. The certificate alert can be fixed by either generating a new self-signed certificate for the device and placing that in the HPE OneView certificate trust store or by performing a certificate signing request and using a certificate authority-issued certificate for the device.

Certificate-related alerts not cleared or deleted if associated certificate is deleted

Certificate-related alerts (e.g. for certificate expiration or revocation) do not get cleared or cannot be deleted if the certificate associated with the original alert is deleted.

Suggested action

For devices using self-signed certificates, use the standard device procedures to update the certificate and upload the resulting certificate to HPE OneView. Make sure to use the same alias as the original certificate. Note that the proper alias is displayed in the alert.

If the expired self-signed certificate is being replaced by a certificate authority-signed certificate, use any existing, valid self-signed certificate that already exists in the trust store and temporarily upload it using the appropriate alias as described above. After the alert clears, you can delete the temporary self-signed certificate. Note that the presence of this temporary certificate in the trust store does not present a security risk. It does not enable communications with the device.

For both cases above, the trust store certificate alert processing for expiration is performed using a scheduled background task. It can take up to an hour for the alert to clear.

Removing and re-inserting one or both of the stacked interconnect modules may cause an incorrect stacking health alert

When one or both of the stacked interconnect modules are removed and re-inserted, HPE OneView might report a report on the Logical Interconnect page. This alert indicates that the "stacking health is disconnected" although the stacking ports are linked up on the interconnect page. This is an incorrect alert.

Suggested action

Check the link state of Q7 and Q8 on the Logical Interconnect page. If the ports are linked the stacking health alert is false and can be cleared. Go to the **Logical Interconnect** screen and from the actions menu clear the alert.

Error when creating Logical JBODs using HDD drive type with Chinese localization

An error indicating that the drive type is "null" occurs when creating Logical JBODs using HDD drive type with Chinese localization.

Suggested action

When defining Logical JBODs, do not use the **Drive type** option for **Select drives by**, instead use the **Size and technology** option. This requires entering the drive size and drive technology manually in the displayed form.

Communication issue if a device certificate chain has an expired CA roots and intermediates

If the remote server/device presents only a leaf certificate or a partial certificate chain when HPE OneView initiates an HTTPS connection, and if any of the root or intermediate certificates stored in HPE OneView trust store that form the remaining chain are expired, the connection to the device will continue to be trusted using the expired certificate until corrective action is taken by the user.

Suggested action

HPE OneView displays alerts well in advance of expiration for any certificate in the trust store. Daily alerts are displayed starting two months prior to expiration. Follow the corrective action suggested in the alert to avoid this issue.

Subsequent edits of passwords left blank in the Image Streamer OS deployment plan will incorrectly indicate that a password is set

When an Image Streamer OS deployment plan is specified in a server profile template and password values are left blank in the deployment plan's custom attributes, subsequent edits of the server profile template will show a row of dots indicating that a password is set even when it is not.

Suggested action

When editing a server profile template that is intended to have passwords set, it is best to not rely on the visualization, but instead clear the fields and re-enter the passwords.

Server profile created using an Image Streamer deployment plan may not reflect accurate password fields

When creating a server profile from a server profile template using an Image Streamer deployment plan, the contents of custom attribute password fields may not reflect the values entered in the server profile template. This may be seen as either no password where a password should exist or a password where no password should exist.

Suggested action

When creating a server profile from a server profile template with an OS deployment plan, start the process from the server profile template page via the **Create server profile** action. Do not start the process from the server profile or server hardware pages. If the process is started from the server profile or server hardware page, regardless of the contents of the custom attribute password fields in the server profile, always clear the fields and enter the desired passwords.

Server profile may not detect the removal of a network

It is possible, under heavy load, that a server profile may not detect the removal of a network that it is using and may continue to report itself as OK even though there is now connectivity loss. The refresh action on the server profile is typically used to correct the profile's state when it does not match reality. When refresh is used, the state of the connection and server profile is updated correctly, but an explanatory alert is not created to explain the problem.

Suggested action

Either specify a new network for the connection or remove the connection from the server profile.

Erroneous consistency warning alerts raised when a SAN volume attachment is removed from a server profile template

When a SAN volume attachment is removed from a server profile template, erroneous consistency warning alerts will be raised on each server profile associated with the server profile template. In fact, there is no inconsistency because additional volumes (beyond what the server profile template mandates) are acceptable and do not affect consistency.

Suggested action

The alerts can be manually cleared.

Appliance network setting fails if hostname is composed of numbers only

Appliance network setting fails if hostname is composed of numbers only.

Suggested action

Enter a alphanumeric value for hostname.

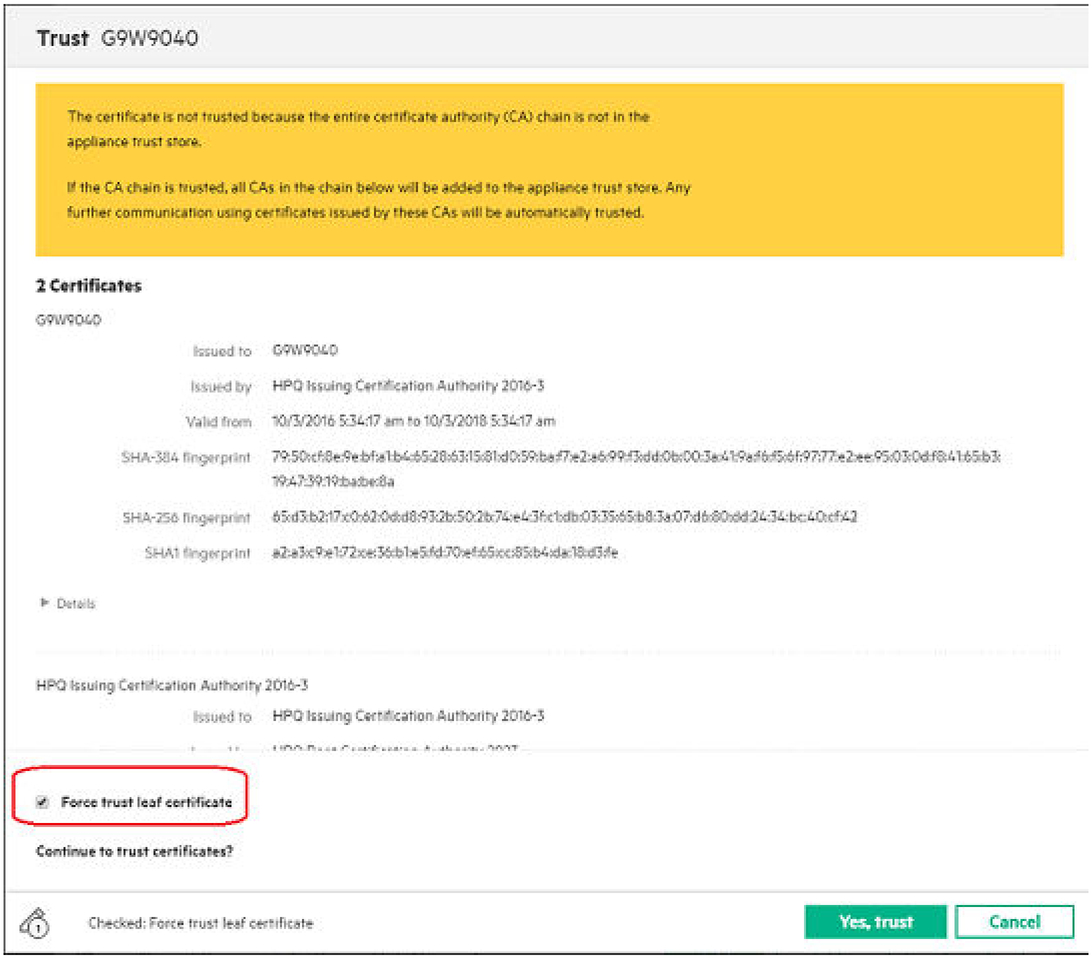
Without one-time additional setup to preserve backward compatibility, REST requests fail for older clients

When integrating HPE OneView 4.0 installations with an enterprise directory, version 4.0 has improved HTTPS certificate checking when using directories with Certificate Authority-issued certificate chains. These improved security checks require one-time additional setup in order to preserve compatibility with scripts or products using older versions of HPE OneView's directory configuration-related REST APIs. Until the additional setup is performed, REST requests such as /rest/logindetails will fail for older clients (e.g. clients using API calls specifying version 500 or earlier).

This issue is specific to new version 4.0 installations. When upgrading from an earlier release, no additional steps are required and backward compatibility is preserved automatically. Directories using self-signed certificates are not impacted.

Suggested action

For a new HPE OneView 4.0 installation using enterprise directory integration and legacy HPE OneView clients, while configuring the directory server, make sure to check the **Force trust leaf certificate** option as shown below:



Trust G9W9040

The certificate is not trusted because the entire certificate authority (CA) chain is not in the appliance trust store.

If the CA chain is trusted, all CAs in the chain below will be added to the appliance trust store. Any further communication using certificates issued by these CAs will be automatically trusted.

2 Certificates

G9W9040

Issued to	G9W9040
Issued by	HPQ Issuing Certification Authority 2016-3
Valid from	10/3/2016 5:34:17 am to 10/3/2018 5:34:17 am
SHA-384 fingerprint	79:50:cf:8e:9e:bf:a1:b4:65:28:63:15:81:d0:59:ba:f7:e2:a6:99:f3:dd:0b:00:3a:41:9a:f6:f5:6f:97:77:e2:ee:95:03:0d:f8:41:65:b3:19:47:39:19:ba:be:8a
SHA-256 fingerprint	65:d3:b2:17:c0:62:0d:d8:93:2b:50:2b:74:e4:3f:c1:db:03:35:65:b8:3a:07:d6:80:dd:24:34:bc:40:cf:42
SHA1 fingerprint	a2:a3:c9:e1:72:ee:36:b1:e5:fd:70:e1:65:cc:85:b4:da:18:d3:fe

▸ Details

HPQ Issuing Certification Authority 2016-3

Issued to	HPQ Issuing Certification Authority 2016-3

☑ **Force trust leaf certificate**

Continue to trust certificates?

Checked: Force trust leaf certificate

This option imports the directory's leaf certificate directly into the HPE OneView trust store. If you have already configured directory integration, you can also manually add directory server leaf certificates using Settings->Security-> Manage Certificates->Add certificates.

Remote support master task incomplete even though subtasks are completed

Initial parent Enable Remote Support task may appear not to complete normally, ending in a timeout error after 6 hours, even though child tasks complete normally. This behavior can be seen with any appliance restart.

Suggested action

No action is required. The timeout error can be ignored.

NOTE:

If a PATCH is being used, the scripting would have to be doing a GET on each subtask to see if it passed or failed. If this approach is taken, then success or failure of each task can be determined by the script.

Any script that uses PUT /rest/support/configuration to enable remote support could wait up to 6 hours since this is a synchronous call. A timeout error would result in an HTTP error return code indicating internal server error (not timeout specifically). Information about the exact cause is sent with the server error.

Any script that uses PATCH /rest/support/ to replace the enableRemoteSupport property to do the same function will get a HTTP 202 (normal async response) with a task ID. Ordinarily the script would be written to then poll via GET /rest/tasks/{id} for task completion. In the timeout case, the response to the poll would indicate error termination as described in the API documentation.

Appliance cluster may fail to form and become highly available after move to new enclosure

The HPE OneView appliance cluster may fail to form and become highly available after a Grow Logical Enclosure (LE) operation and related standby appliance move to a new enclosure (Synergy frame) per recommended HA action, and a subsequent Settings > Appliance > Remove Standby, or Upgrade operation, or Restore is performed.

Image Streamer Add deployment server may fail or the Update from group task on the LE may hang when adding Image Streamer to the same LE. Additionally, an alert **The quorum is not configured for the storage system in the Image Streamer deployment appliance** may be shown in HPE OneView after frame link module (FLM) firmware is updated or if the FLM modules have failed.

Suggested action

To address the HPE OneView appliance cluster problem or the Image Streamer quorum alert after it has occurred, contact your local HPE support representative to obtain a fixme.bin or, alternately, execute the following steps:

1. Move the HPE Composer standby appliance to the same frame as the active appliance. After the appliances have synchronized, confirm that the active and standby appliances are noted as **Connected** in the Settings > Appliance page.
2. To resolve the subsequent alert **Two appliances in an appliance cluster should not be in same frame**, move the standby appliance to the new frame. After the appliances have synchronized, confirm that the active and standby appliances are noted as **Connected** in the Settings > Appliance page.

To address the Image Streamer **Add deployment server** failure or **Update from group** hang on the logical enclosure after the problem has occurred, contact your local HPE support representative to obtain a fixme.bin (same version as above). Apply the fixme.bin, and then execute the following steps:

1. Factory reset and reseat the OS deployment server appliance pair.
2. Retry the original failed operation.

Trusting a root CA "iLO/iLO3/iLO4 Default Issuer (do not trust)"

When trusting an iLO's self-signed certificate using the Settings > Security > Manage Certificates > Add Certificate screen and selecting Fetch from IP address or hostname, make sure to always enable the **Force trust leaf certificate** option which ensures that only the iLO's leaf certificate is added to the trust store. If you forget to use this option, the iLO's **Default Issue (do not trust)** is sometimes added to the trust store. In that case, make sure to delete the **Default (do not trust)** certificate. These certificates should never be placed into the trust store and can cause errors when present.

Uploaded CRL takes effect immediately but can take up to 1 hour to appear in the UI

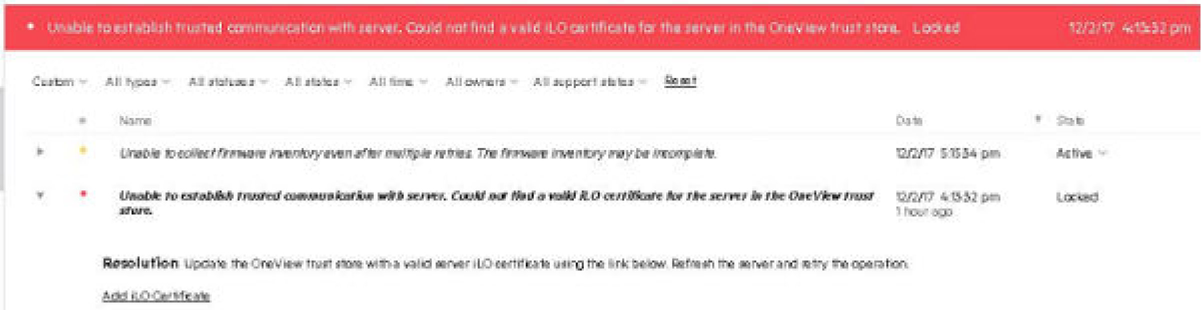
When uploading a certificate authority's certificate revocation list (CRL) the CRL is processed and immediately applied to all subsequent TLS connections from HPE OneView. However, for the uploaded CRL to be displayed as being effective in the Manage Certificates UI it can take up to 1 hour when an hourly certificate status scheduled job runs and updates the status in the UI.

Configure Active Directory server with TLS v1.2

Always configure Active Directory server with TLS v1.2 so that HPE OneView can communicate with Active Directory using TLS v1.2 and not the less secure TLS v1.0 or TLS v1.1 protocols.

Communication with a managed device may fail despite the existence of the certificate in the trust store

Under very rare circumstances communication with a managed device may fail with an **unable to establish trusted communication** alert (shown below) despite the existence of the certificate in the trust store. The resolution to add the certificate will fail.



● Unable to establish trusted communication with server. Could not find a valid iLO certificate for the server in the OneView trust store. Locked 12/2/17 4:13:52 pm

	●	Name	Date	State
▸	●	*Unable to collect firmware inventory even after multiple retries. The firmware inventory may be incomplete.*	12/2/17 5:15:34 pm	Active
▾	●	***Unable to establish trusted communication with server. Could not find a valid iLO certificate for the server in the OneView trust store.***	12/2/17 4:13:52 pm 1 hour ago	Locked

Resolution Update the OneView trust store with a valid server iLO certificate using the link below. Refresh the server and retry the operation.

Add iLO Certificate

Suggested action

From the Settings > Security > Manage Certificate page:

- Delete the device certificate for which the communication failed
- Add the device certificate back with the same alias name

Add Deployment Server fails when changing the network subnet mask setting does not reflect in the UI

If the HPE OneView Appliance network subnet mask setting is changed, the HPE OneView Appliance UI does not reflect the change and the Add Deployment Server fails.

Suggested action

Restart the HPE OneView Appliance from the Settings >Appliance page.

NOTE:

The Add Deployment Server will not fail if the HPE OneView Appliance restart is issued before adding the Deployment Server.

Synergy compute modules may experience a read-only file system following firmware update

Synergy compute modules with server profiles attached to FCoE networks may experience a read-only file system following firmware update of Virtual Connect SE 40Gb F8 Modules. This issue only pertains to servers attached to FCoE networks and does not apply to servers which utilize Ethernet, iSCSI, or FC network connections in any combination.

Suggested action

When performing a firmware update of Virtual Connect SE 40Gb F8 modules with servers connected to FCoE networks a maintenance window will be required. After the firmware update has completed, it is important to visit each of the FCoE connected servers to verify the current state of the servers' filesystem. If the filesystem has been marked as read only, the server must be restarted to recover the filesystem to read/write mode. Once all FCoE servers have been verified, the maintenance window may be exited. This verification process only applies to servers with FCoE connections. Servers without FCoE connections do not need to be verified.

Scanning tool reports a weak SSH cipher issue

Vulnerability Scanning tool (Nessus) reports that HPE OneView supports a weak SSH cipher, aes-256-cbc.

Suggested action

No action is required at this time.

This issue has been assessed as low severity and mitigations have been applied to SSH to deal with it. Use of this cipher is limited to the management network. This issue will be addressed in a future release.

HPE OneView uses OpenSSH 5.3, which includes mitigations to reduce the possibility of a successful plain text recovery, as described in CVE-2008-5161, caused by use of CBC ciphers.

For additional details regarding CVE-2008-5161 see:

http://community.arubanetworks.com/t5/Wireless-Access/SSH-and-AES-CBC/td-p/248919

Notes for HPE OneView 4.0 for HPE Synergy

Supported iSCSI boot configurations

The following parameters are supported:

- IPv4 (no support for IPv6)
- Static IP address and DHCP allocated IP addresses
- SW-iSCSI (software initiator) and HW-iSCSI (iSCSI offload, hardware assisted initiator)
- Bootable Ethernet connection using iSCSI can only be on the first virtual function of the physical port (i.e. port "a") and HW-iSCSI connections can only be on the second function of the physical port (port "b", which is the storage function)

Fibre Channel direct attach connections

HPE OneView 4.0 for HPE Synergy supports Fibre Channel fabric attach and Fibre Channel over Ethernet (FCoE) network connections. DirectAttach with 3PAR Storage (FlatSAN) is supported in HPE OneView 4.0.

Port Mirroring

Bi-directional mirroring is supported for VC SE 16 Gb FC module with firmware version 4.00.33 or higher.

System board replacement

When a profile is assigned to a server in bay and that server is removed for maintenance reasons, HPE OneView (like VC) places a power hold on that bay to ensure it doesn't just power on without some validation for network security, etc. Once a blade is inserted, HPE OneView will detect it and check the blade/OA to see if it is the same server (using the UUID) and has the same configuration as the blade before, and if it does, the power hold is released. If it does not, the profile was marked in error at which point you can remove the profile from that server/bay (or edit and re-apply if it is still the same hardware type).

In the case of a system board replacement, most likely the UUID needs to be manually reprogrammed via RBSU, so it appears to be the same server to a profile. In this case, to release the power hold, edit the profile and mark it un-assigned, and save. This releases a power hold and allows a power on of the server so it can then be reprogrammed accordingly. Once changes are made, let the server complete a POST cycle and then re-assign that profile to that server/bay.

Documentation addendum

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

Security

Refer to “Understanding the security features of the appliance” in the *HPE OneView 4.0 User Guide for HPE Synergy* for the most up-to-date information regarding security.

HPE OneView API Reference

NOTE:

Minimum supported API versions are subject to change in future releases, therefore it is recommended to migrate to the latest API version at the earliest possible convenience in order to avoid compatibility issues when upgrading to newer versions of HPE OneView.

FC Direct Attach to 3PAR storage arrays

FC Direct Attach to 3PAR storage arrays for the HPE Virtual Connect SE 40Gb F8 Module for HPE Synergy delivers a simplified and automated storage provisioning experience to Virtual Connect customers by eliminating the need to use ToR/EoR SAN switches.

Viewing of Remote Support events that are received from HPE Synergy Composer

You can now view events coming from the HPE Synergy Composer that are appropriate for automatic routing to Remote Support, once remote support is enabled in HPE OneView.

Removed support for API versions

API versions that are no longer being supported are detailed in **one or more of the following** documents:

- HPE OneView 4.0 Release Notes
- HPE OneView 4.0 Support Matrix
- HPE OneView 4.0 API Scripting Help

Firmware and drivers update for ESXi OS for Gen10 servers

For Gen10 servers, the support for ESXi WBEM inventory providers is no longer available.

Securing remote login when using REST API

To log into an appliance remotely using /rest/login-sessions/smartcards , you must use a client library that supports client certificate authentication with a private key, in addition to the server certificate authentication done normally. When evaluating the client library, make sure that the client private key is not passed to the server.

One possible way to secure remote login with this REST API is to use Curl version 7.54.1-1 or later, which in turn uses libssh2 (see **curl man page**).

Documentation errata

- The HPE OneView online help mentions that the **OS volumes** > **General** section displays the state of the OS volume. This is incorrect. The state of the OS volume is displayed in **Deployment Appliances** > **Storage** section of the HPE Synergy Image Streamer user interface.
- In the following note in the **Valid configurations for enclosure groups with multiple logical interconnect groups** section of the HPE OneView online help, the sentence "HPE Synergy Image Streamer deployment is not supported when Virtual Connect SE 40Gb F8 Modules are configured for redundancy in multiple frames" does not apply to HPE OneView 4.0:

  NOTE:

  To use HPE Synergy Image Streamer for operating system deployment in a highly available environment, a pair of Synergy Image Streamer appliances is required for each Virtual Connect SE 40Gb F8 Module for Synergy and Interconnect Link Module set of Synergy frames. A logical enclosure can have at most one pair of Image Streamer appliances.

  HPE Synergy Image Streamer deployment is not supported when Virtual Connect SE 40Gb F8 Modules are configured for redundancy in multiple frames.

Documentation and troubleshooting resources for HPE Synergy

HPE Synergy documentation

The Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**) is a task-based repository. It includes installation instructions, user guides, maintenance and service guides, best practices, and links to additional resources. Use this website to obtain the latest documentation, including:

- Learning about HPE Synergy technology
- Installing and cabling HPE Synergy
- Updating the HPE Synergy components
- Using and managing HPE Synergy
- Troubleshooting HPE Synergy

HPE Synergy Configuration and Compatibility Guide

The *HPE Synergy Configuration and Compatibility Guide* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It provides an overview of HPE Synergy management and fabric architecture, detailed hardware component identification and configuration, and cabling examples.

HPE Synergy Frame Link Module User Guide

The *HPE Synergy Frame Link Module User Guide* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It outlines frame link module management, configuration, and security.

HPE OneView User Guide for HPE Synergy

The *HPE OneView User Guide for HPE Synergy* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It describes resource features, planning tasks, configuration quick start tasks, navigational tools for the graphical user interface, and more support and reference information for HPE OneView.

HPE OneView Global Dashboard

The HPE OneView Global Dashboard provides a unified view of health, alerting, and key resources managed by HPE OneView across multiple platforms and data center sites. The *HPE OneView Global Dashboard User Guide* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It provides instructions for installing, configuring, navigating, and troubleshooting the HPE OneView Global Dashboard.

HPE Synergy Image Streamer User Guide

The *HPE Synergy Image Streamer User Guide* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It describes the OS deployment process using Image Streamer, features of Image Streamer, and purpose and life cycle of Image Streamer artifacts. It also includes authentication, authorization, and troubleshooting information for Image Streamer.

HPE Synergy Image Streamer GitHub

The HPE Synergy Image Streamer GitHub repository (**github.com/HewlettPackard**) contains sample artifacts and documentation on how to use the sample artifacts. It also contains technical white papers explaining deployment steps that can be performed using Image Streamer.

HPE Synergy Software Overview Guide

The *HPE Synergy Software Overview Guide* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It provides detailed references and overviews of the various software and configuration utilities to support HPE Synergy. The guide is task-based and covers the documentation and resources for all supported software and configuration utilities available for:

- HPE Synergy setup and configuration
- OS deployment
- Firmware updates
- Troubleshooting
- Remote support

HPE Synergy Firmware Update Overview

The *HPE Synergy Firmware Update Overview* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It provides information on how to update the firmware for HPE Synergy.

Best Practices for HPE Synergy Firmware and Driver Updates

The *Best Practices for HPE Synergy Firmware and Driver Updates* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It provides information on recommended best practices to update firmware and drivers through HPE Synergy Composer, which is powered by HPE OneView.

HPE OneView Support Matrix for HPE Synergy

The *HPE OneView Support Matrix for HPE Synergy* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It maintains the latest software and firmware requirements, supported hardware, and configuration maximums for HPE OneView.

HPE Synergy Image Streamer Support Matrix

The *HPE Synergy Image Streamer Support Matrix* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It maintains the latest software and firmware requirements, supported hardware, and configuration maximums for HPE Synergy Image Streamer.

HPE Synergy Glossary

The *HPE Synergy Glossary*, in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**), defines common terminology associated with HPE Synergy.

HPE Synergy troubleshooting resources

HPE Synergy troubleshooting resources are available within HPE OneView and in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**).

Troubleshooting within HPE OneView

HPE OneView graphical user interface includes alert notifications and options for troubleshooting within HPE OneView. The UI provides multiple views of HPE Synergy components, including colored icons to indicate resource status and potential problem resolution in messages.

You can also use the Enclosure view and Map view to quickly see the status of all discovered HPE Synergy hardware.

HPE Synergy Troubleshooting Guide

The *HPE Synergy Troubleshooting Guide* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It provides information for resolving common problems and courses of action for fault isolation and identification, issue resolution, and maintenance for both HPE Synergy hardware and software components.

Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy

The *Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy* is in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**). It provides information for resolving common problems associated with specific error messages received for both HPE Synergy hardware and software components.

HPE OneView Help, HPE OneView REST API Scripting Help, and HPE OneView API Reference

The *HPE OneView Help*, the *HPE OneView REST API Scripting Help*, and the *HPE OneView API Reference* are readily accessible, embedded online help available within the HPE OneView user interface. These help files include “Learn more” links to common issues, as well as procedures and examples to troubleshoot issues within HPE Synergy.

The help files are also available in the Hewlett Packard Enterprise Information Library (**www.hpe.com/info/synergy-docs**).

HPE Synergy QuickSpecs

HPE Synergy has system specifications as well as individual product and component specifications. For complete specification information, see the HPE Synergy and individual HPE Synergy product QuickSpecs on the Hewlett Packard Enterprise website (**www.hpe.com/info/qs**).

HPE Synergy document overview (documentation map)

www.hpe.com/info/synergy-docs

Planning

- *HPE Synergy 12000 Frame Site Planning Guide*
- *HPE Synergy Configuration and Compatibility Guide*
- *HPE OneView Support Matrix for HPE Synergy*
- *HPE Synergy Image Streamer Support Matrix*
- *Setup Overview for HPE Synergy*
- *HPE Synergy Software Overview Guide*

Installing hardware

- *HPE Synergy Start Here Poster* (included with frame)
- *HPE Synergy 12000 Frame Setup and Installation Guide*
- *Rack Rails Installation Instructions for the HPE Synergy 12000 Frame* (included with frame)
- *HPE Synergy 12000 Frame Rack Template* (included with frame)
- Hood labels
- User guides
- *HPE Synergy Cabling Interactive Guide*
- *HPE OneView Help for HPE Synergy — Hardware setup*

Configuring for managing and monitoring

- *HPE OneView Help for HPE Synergy*
- *HPE OneView User Guide for HPE Synergy*
- *HPE OneView API Reference for HPE Synergy*
- *HPE OneView REST API Scripting Help for HPE Synergy*
- User Guides

Managing

- *HPE OneView User Guide for HPE Synergy*
- *HPE Synergy Image Streamer Help*
- *HPE Synergy Image Streamer User Guide*
- *HPE Synergy Image Streamer API Reference*
- *HPE Synergy Image Streamer deployment workflow*
- *HPE Synergy Frame Link Module User Guide*

Monitoring

- *HPE OneView User Guide for HPE Synergy*
- *HPE OneView Global Dashboard User Guide*

Maintaining

- Product maintenance and service guides
- *Best Practices for HPE Synergy Firmware and Driver Updates*
- *HPE OneView Help for HPE Synergy*
- *HPE OneView User Guide for HPE Synergy*
- *HPE Synergy Appliances Maintenance and Service Guide for HPE Synergy Composer and HPE Synergy Image Streamer*

Troubleshooting

- HPE OneView alert details
- *HPE Synergy Troubleshooting Guide*
- *Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy*
- *Integrated Management Log Messages and Troubleshooting Guide for HPE ProLiant Gen10 and HPE Synergy*
- *HPE OneView API Reference for HPE Synergy*
- *HPE Synergy Image Streamer API Reference*

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website: **www.hpe.com/assistance**
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website: **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, go to the **Software Depot for Synergy**.
- 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 HP Passport set up with relevant entitlements.

Websites

Website	Link
Hewlett Packard Enterprise Information Library	**www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**

Table Continued

Website	Link
Contact Hewlett Packard Enterprise Worldwide	**www.hpe.com/assistance**
HPE OneView Docs	**www.hpe.com/info/oneview/docs**
Subscription Service/Support Alerts	**www.hpe.com/support/e-updates**
Customer Self Repair	**www.hpe.com/support/selfrepair**
Remote Support for HPE OneView FAQ document	**Remote support doc**
Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix	**www.hpe.com/storage/spock**
HPE 3PAR StoreServ Storage	**www.hpe.com/info/storage**
HPE Integrated Lights-Out	**www.hpe.com/info/ilo**
Storage white papers and analyst reports	**www.hpe.com/storage/whitepapers**

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

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:

www.hpe.com/support/selfrepair

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.