Hewlett Packard Enterprise

HPE OneView 4.2 Support Matrix

Abstract

This document lists the hardware, firmware, and software requirements for installing and using HPE OneView on a virtual machine host.

Part Number: P01320-003a
Published: April 2019
Edition: 2

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

Google® is a registered trademark of Google Inc.

Microsoft®, Windows®, and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

VMware ESXi® is the 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

Appliance requirements

Appliance VM and host requirements

HPE OneView is a virtual appliance running on the supported hypervisor hosts.

Table 1: Supported hypervisors and versions

Hypervisor	Version
VMware vSphere ESXi	• 5.5 • 5.5 update 1 • 5.5 update 2 • 5.5 update 3 • 6.0 • 6.0 update 1 • 6.0 update 3 • 6.5 • 6.5 update 1 • 6.5 update 2 • 6.7 • 6.7 update 1
Microsoft Hyper-V	Hyper-V is supported on the following Microsoft Windows platforms with the Hyper-V role installed: • Windows Server 2012 (on ProLiant Gen8 and ProLiant Gen9 platforms) • Windows Server 2012 R2 (on ProLiant Gen10 platforms) • Windows Hyper-V Server 2012 • Windows Hyper-V Server 2012 R2 • Windows Server 2016 • Microsoft Hyper-V Server 2016 • Windows Server 2019 Long-Term Servicing Channel (LTSC)
KVM	• RHEL 6.10 • RHEL 7.2 • RHEL 7.3 • RHEL 7.5 • RHEL 7.6 [1]

[1] Support for Second Generation Intel Xeon Scalable Processors only.

The appliance virtual machine (VM) must run on a VM host with ProLiant G7-class CPUs or later. Ensure that you have configured the hypervisor host to reserve the following minimum resource requirements for the HPE OneView virtual appliance:

- Minimum 8 2-GHz or greater virtual CPUs
- Exactly 24GB of memory
- Minimum 275 GB of thick-provisioned disk space

  You can manually grow the virtual disk to increase the size of the firmware repository. The best practice is to grow the virtual disk during appliance installation on a VMware vSphere hypervisor or Microsoft Hyper-V hypervisor.
- Hewlett Packard Enterprise recommends that you have separate networks for management and data.

  It is critical that the virtual appliance have an accurate time source. There are two options for ensuring accurate time on the virtual appliance using Network Time Protocol (NTP):

NTP on the hypervisor	Configure the hypervisor host to use NTP and configure HPE OneView to use the hypervisor host as its time source.
NTP in HPE OneView	Configure HPE OneView to use three or more NTP servers.

- A hypervisor host must reserve the following minimum resource requirements:
  - **Minimum system requirements for installing ESXi/ESX (1003661)** VMware Knowledge Base
  - **Review Prerequisites for Installation** (Hyper-V Server 2012, Hyper-V Server 2012 R2), Microsoft TechNet
  - **Install Hyper-V and Configure a Virtual Machine** (Windows Server 2012), Microsoft Windows Server
- Power management options under BIOS settings:
  - Set Power Regulator to Static High Performance Mode.
  - Set Power Profile to Maximum Performance.
  - Hewlett Packard Enterprise recommends reservations/shares for CPU and memory.

Where to deploy the virtual machine

You can deploy HPE OneView on any ProLiant hardware that meets the requirements in **Appliance VM and host requirements**. Specific restrictions apply to hardware that is managed or monitored by HPE OneView.

You can deploy HPE OneView in a hypervisor in the following hardware environments:

- **Rack-mount ProLiant DL**
- **Blade System**

Restrictions apply to both environments if you want to use HPE OneView to manage the hypervisor host on which it is executing.

IMPORTANT: Hewlett Packard Enterprise recommends that you deploy the HPE OneView virtual appliance on a hypervisor environment that is dedicated to management functions and separate from the production hypervisor environment.

Deploying in a DL-based hypervisor environment

Deploying to a hypervisor cluster configuration for high availability (HA) is the best practice. You can also deploy HPE OneView using a DL-based hypervisor configuration environment.

Add the DL server hypervisor host to HPE OneView in monitored mode. Do not power off the hypervisor host from HPE OneView, because doing so would inadvertently power off the virtual appliance.

NOTE: In a non-HA configuration with a single DL server hypervisor host, adding the DL server hypervisor host into HPE OneView as managed server hardware is not supported.

In an HA configuration, where the HPE OneView virtual appliance can be migrated between hosts, the restriction to add the host as managed still applies, but can be worked around using VM migration. Note that this approach is error prone.

NOTE: The virtual appliance cannot detect the hypervisor host on which it is running, and therefore cannot warn the user regarding an unsupported operation.

The best practice is to use HPE OneView to monitor, not manage, the DL hypervisor hosts in the cluster. In monitored mode, before powering off a host using HPE OneView, make sure that the appliance is not running on that host. If the appliance is running on the host, the HPE OneView appliance needs to be migrated to a different cluster member.

If the DL hypervisor hosts are added into HPE OneView in managed mode, the following additional restrictions apply:

- You cannot apply or edit the server profile for the hypervisor host on which the HPE OneView virtual appliance is currently executing because this requires the server hardware to be powered off.
- You must migrate the appliance to a different host in the cluster before applying the server profile.

Deploying in an HPE BladeSystem hypervisor environment

An HPE BladeSystem configuration has the same **restrictions as DL servers**, along with considerations for managing server profile connections for managed enclosures.

For blade systems, the server profile encapsulates all the network connectivity for the blade servers, and works in conjunction with the interconnect modules in the enclosure.

When deploying HPE OneView on ESXi hosts on a single enclosure, non-HA hypervisor HPE BladeSystem environment, the best practice is to monitor, not manage, the enclosure. The same **restrictions** still apply. Do not power off the VM host where the HPE OneView appliance is currently running.

For a single or multi-enclosure environment where the enclosures are added to HPE OneView in managed mode, the enclosure must include non-VC interconnect modules. The storage and network connectivity for the hypervisor hosts supporting the HPE OneView virtual appliance must be restricted to using these non-VC interconnect modules. When performing server profile operations and power operations, refrain from having the HPE OneView virtual appliance execute on the specific host where these operations are being performed.

Planning for high availability

To use HPE OneView in an HA (high availability) configuration, see your hypervisor documentation for specific requirements.

To maintain appliance availability, HPE OneView provides a backup feature to save your configuration settings and management data to a backup file. Hewlett Packard Enterprise recommends backing up your appliance, preferably daily and after other key configuration changes.

For more information see the *About backing up the appliance* and *Best practices for backing up an appliance* sections in the online help.

Firmware requirements

This section describes the firmware requirements for devices you plan to manage with HPE OneView.

To add a device to the appliance and actively manage, the device must meet the minimum firmware requirements described in the section **Minimum firmware requirements for managed and monitored devices** on page 8.

NOTE: Firmware for monitored devices is managed outside of HPE OneView.

Service Pack for ProLiant (SPP)

Download the latest Service Pack for ProLiant (SPP) from **http://hpe.com/info/SPP** and then upload to the appliance or the external repository added to the appliance.

NOTE: For more information on the current production and post-production versions of SPPs, see the *Important Notes* section from **http://h17007.www1.hpe.com/us/en/enterprise/servers/products/service_pack/spp/index.aspx**.

Minimum firmware requirements for managed and monitored devices

For HPE OneView to discover a device and determine its type, a **minimum firmware version is required**. This is **not** the **firmware version required for active management or monitoring**. A device with the discovery-only level of firmware can be upgraded to the minimum requirements with an SPP. Firmware components are upgraded when the device is added to HPE OneView as managed. For monitored devices, or for devices below the firmware versions required for HPE OneView discovery, you must manually update the firmware version outside of HPE OneView to the minimum requirements.

NOTE: To ensure that your hardware has the latest and most robust firmware bundle that takes advantage of all the available management features, download the latest firmware bundle to your appliance and add it to the firmware repository.

When you add enclosures and servers as managed, you can specify a firmware baseline for the onboard administrator, interconnects, and iLO modules.

Table 2: Minimum firmware version required for discovery of devices

Device	Firmware version
HPE Superdome Flex Rack Management Controller	2.4.98
HPE Virtual Connect	3.15

Table Continued

Device	Firmware version
HPE BladeSystem Onboard Administrator	3.00[1]
iLO 5 for Gen10 servers	1.10[2]
iLO 4 for Gen9 servers	2.0[3]
iLO 4 for Gen8 servers	1.01[3]
iLO 3	1.20[3]

[1] 6.0.42 for HPE Integrity Superdome X.

[2] HPE OneView 4.1 and later supports iLO 5 when configured to use either the **Production** or **High Security** security states. Refer to the iLO user interface or iLO documentation for additional details on setting iLO security states.

[3] HPE OneView 4.1 and later supports iLO 3 and iLO 4 when configured to use either the standard encryption (default) setting of iLO or the **Enforce AES/3DES Encryption** setting.

Only managed devices will update automatically. Monitored devices must be upgraded manually to match the following minimum firmware.

Table 3: Minimum firmware version required for active management, monitoring, and migration

Device	Firmware version
HPE Superdome Flex Rack Management Controller	2.5.280
HPE Virtual Connect	4.10[1]
HPE BladeSystem Onboard Administrator	4.01[2,3,4]
HPE BladeSystem Onboard Administrator with all non-Virtual Connect interconnects	4.31
HPE BladeSystem Onboard Administrator with a mixture of Virtual Connect and non-Virtual Connect	4.31
iLO 5 for HPE Composable Cloud for Proliant DL	1.40
iLO 5 for Gen10 servers	1.10[5]
iLO 4 for Gen9 servers	2.03[6]
iLO 4 for Gen8 servers	1.30[6]
iLO 3	1.61[6]
iLO 2	2.13

Table Continued

Device	Firmware version
Intelligent Provisioning for Gen8 servers[7]	1.61 for Gen8 AMD systems 1.20 for Gen8 Intel systems
Intelligent Provisioning for Gen9 servers	2.0
SPP	See **Service Pack for ProLiant (SPP)** on page 8
HPE Insight Management Agents (for G6 and G7 server monitoring)	9.20
Emulex Converged Network Adapters	4.2.401.6 or later

[1] Refer to **Firmware considerations for HPE Virtual Connect modules**.

[2] For monitoring support only. For managed support, the minimum firmware version is 4.31.

[3] 6.0.42 for HPE Integrity Superdome X.

[4] Onboard administrator firmware version 4.70 and later support CAC Authentication, which is a form of two-factor authentication using smart cards. HPE OneView will not be able to communicate with the onboard administrator when the CAC Authentication or the **Two-Factor Authentication** is enabled.

[5] HPE OneView 4.1 and later supports iLO 5 when configured to use either the **Production** or **High Security** security states. Refer the iLO user interface or iLO documentation for additional details on setting iLO security states.

[6] HPE OneView 4.1 and later supports iLO 3 and iLO 4 when configured to use either the standard encryption (default) setting of iLO or the **Enforce AES/3DES Encryption** setting.

[7] For Intel based systems:

- When managing firmware baselines through the server profiles, Intelligent Provisioning version 1.20 or later is required.
- When managing BIOS settings through the server profile, servers with iLO version 2.0 or later require Intelligent Provisioning version 1.20 or later.

  To determine the Intelligent Provisioning (IP) version, browse to the iLO on the server, select **System Information** and then click the **Firmware** tab. The latest version of IP firmware is available for **download**.

NOTE: HPE OneView uses the SPP firmware bundle uploaded to the appliance to update the firmware automatically for these devices to the minimum version necessary for full management.

Firmware considerations for HPE Virtual Connect modules

- If an interconnect has an earlier version of HPE Virtual Connect firmware, Hewlett Packard Enterprise recommends using the Virtual Connect Support Utility (VCSU) to update the firmware to version 3.15 before adding the device to the appliance.
- HPE OneView can manage and configure HPE Virtual Connect Fibre Channel modules (using IPv6 addresses) that has a minimum firmware version of 4.10. Any module that has an earlier firmware version when it is added to the appliance is flagged for a firmware update. The flagged modules remain in an unmanaged state until you use **Interconnect** > **Actions** > **Update firmware** in the UI to update the Interconnect firmware.

- HPE OneView does not support migration of Virtual Connect Manager domains that are restricted to CNSA cryptography or that have two factor authentication enabled.
- HPE FlexFabric-20/40 F8 modules require Virtual Connect 4.20 or later.
- HPE Virtual Connect 8Gb 24-Port FC modules require Fibre Channel firmware 3.01 or higher and Virtual Connect 4.40 or higher.
- HPE Virtual Connect 16Gb 24-port Fibre Channel modules require Virtual Connect 4.40 or higher.

Supported Smart Update Tools (SUT)

Smart Update Tools (SUT) and Integrated Smart Update Tools (iSUT) are software utilities used with HPE OneView to stage, install, and activate firmware and driver updates.

Server	Operating System	SUT type	Version
Gen8, Gen9, and Gen10	Windows	iSUT for Windows	SUT 2.0.0 or later SUT 2.3.0 or later (recommended)
Gen8, Gen9, and Gen10	Linux	iSUT for Linux	SUT 2.0.0 or later SUT 2.3.0 or later (recommended)
Gen8 and Gen9	ESXi	SUT for ESXi	SUT 2.0.0 or later SUT 2.3.0 or later (recommended)
Gen10	ESXi	iSUT for ESXi	SUT 2.3.6 or later

Supported Internet Protocol (IP) versions

The HPE OneView appliance supports two distinct IP networking modes:

- IPv4, which is the default
- IPv6

For details about these networking modes, see the *HPE OneView Installation Guide*.

IPv4 mode

IPv4 mode supports all the HPE OneView management features.

HPE OneView appliance or managed devices	IPv4 (mandatory or optional)	IPv6 (mandatory or optional)
HPE OneView appliance	Mandatory	Optional
Managed devices	Mandatory	Optional

IPv6 mode

Some HPE OneView features are not supported in the IPv6 mode. The support restrictions lists the exceptions.

HPE OneView appliance or managed devices	IPv4 (mandatory or optional)	IPv6 (mandatory or optional)
HPE OneView appliance	Disabled	Mandatory
Managed devices	Optional	Mandatory

IMPORTANT: The networking mode of the appliance can be set when configuring the networking parameters while setting up the appliance for the first time. If IPv4 is enabled, the appliance will be in IPv4 mode. If IPv4 is disabled, the appliance will be in IPv6 mode. After the first time setup procedure is complete, the networking mode of the appliance cannot be changed without a full factory reset. This restriction does not permit an appliance running in IPv4 mode to switch to IPv6, even after an appliance upgrade.

Support restrictions

- IPv6 addresses are only supported for managed rack-based servers. c7000 enclosures and blades are not supported even though the **Add Enclosure** option is enabled in the appliance.
- You cannot specify a range of IPv6 addresses when adding servers to HPE OneView.
- HPE OneView, when configured for IPv6, cannot send or receive communications to or from devices on an IPv4 network.
- There is no storage system support in IPv6 mode.
- There is no remote support in IPv6 mode.
- A backup can only be restored to an appliance using the same networking mode.

Supported web browsers and versions

The following web browsers have been tested and qualified for use with HPE OneView.

- Microsoft Internet Explorer Version 11
- Microsoft Edge
- Mozilla Firefox Version 64.x
- Mozilla Firefox ESR (Extended Support Release) Version 52.x
- Google Chrome Version 71.x

IMPORTANT: Hewlett Packard Enterprise makes every effort to support newer versions of and updates to supported web browsers. However, newer versions do not always work as expected. There might be issues with the web browsers that preclude support with the current release of HPE OneView, or there might be a gap between the time when the web browsers are released and the time when browser support is available in HPE OneView. In these cases, Hewlett Packard Enterprise will endeavor to support the newer browser versions in the next maintenance release or full release of HPE OneView.

If you encounter a problem with a newer, untested version of a web browser, submit a report to your authorized support representative. In some cases, the short-term solution might be to revert to an earlier, supported web browser version.

Screen resolution

- Minimum resolution: 1024 x 768
- Recommended resolution: 1280 x 1024 or greater

Supported hardware and software

NOTE: HPE OneView 4.1 and later does not support managed device certificates using MD5 digital signatures.

NOTE: For detailed information about supported HPE Storage product configurations, see **http://www.hpe.com/storage/spock**.

IMPORTANT: HPE OneView does not manage or monitor enclosures containing unsupported components and displays a warning message if any unsupported components are detected.

Managed ProLiant BL and WS server blades

The following server blade models can be added as managed:

Table 4: Managed ProLiant BL and WS server blades

Model	G7	Gen8	Gen9	Gen10
BL420c		✓		
BL460c	✓	✓	✓	✓
BL465c	✓	✓		
BL490c	✓			
BL620c	✓			
BL660c		✓	✓	
BL685c	✓			
WS460c (single and double wide blades)		✓	✓	✓

Managed ProLiant DL rack mount servers

The following rack server models can be added as managed:

Table 5: Managed ProLiant DL rack mount servers

Model	Gen8	Gen9	Gen10
DL20		✓	✓
DL60		✓	
DL60e		✓	
DL80		✓	

Table Continued

Model	Gen8	Gen9	Gen10
DL80e		✓	
DL120		✓	✓
DL160	✓	✓	✓
DL180		✓	✓
DL320e	✓		
DL320e v2	✓		
DL320p		✓	
DL325			✓
DL360		✓	✓
DL360e	✓		
DL360p	✓		
DL380		✓	✓
DL380e	✓		
DL380p	✓		
DL380z	✓		
DL385			✓
DL385p	✓		
DL560	✓	✓	✓
DL580	✓	✓	✓

Managed ProLiant ML servers

The following ML server model can be added as managed:

Table 6: Managed ProLiant ML servers

Model	Gen8	Gen9	Gen10
ML110			✓
ML350		✓	✓
ML30			✓

Managed ProLiant XL servers

The following XL server models can be added as managed:

Table 7: Managed ProLiant XL servers

Model	Gen9	Gen10
XL170r	✓	✓
XL190r	✓	✓
XL230a	✓	
XL230b	✓	
XL230k		✓
XL250a	✓	
XL260a	✓	
XL2x260w	✓	✓
XL270d	✓	✓
XL280d	✓	✓
XL420	✓	✓
XL450	✓	✓

Managed Composable Cloud for ProLiant DL

The HPE Composable Cloud for ProLiant DL solution requires 2, 4 or 6 Composable Fabric FM 3180 rack connectivity modules with 5.0 HPE Composable Fabric Manager.

Certain HPE OneView features are only available for use when purchased as part of the HPE Composable Cloud for ProLiant DL solution. This solution includes separate HPE Composable Cloud for ProLiant DL software licenses for each HPE ProLiant DL Gen10 server in the configuration. These licenses grant the rights to use these unique features for the solution such as HPE OneView integration with the HPE Composable Fabric Manager.

Model	Minimum firmware	Gen10
ProLiant DL380	iLO 5 version 1.40	✓
ProLiant DL360	iLO 5 version 1.40	✓
HPE Eth 10/25Gb 2p 631FLR-SFP28 Adapter	214.0.203000 version or later	

For more information about the HPE Composable Cloud for ProLiant DL, see **Hewlett Packard Enterprise Information Library**.

Server hardware management features

The appliance supports the following features on server hardware when added as managed.

Feature	Supported server hardware		
	HPE ProLiant BL G7[1,2]	**HPE ProLiant BL Gen8/Gen9/Gen10 and HPE ProLiant WS Gen8/Gen9/Gen10**	**HPE ProLiant DL Gen8/ Gen9/Gen10, HPE ProLiant ML Gen9, and HPE ProLiant XL Gen9/ Gen10**
Power on or power off the server	✓	✓	✓
View inventory data	✓	✓	✓
Monitor power, cooling, and utilization[3]	✓	✓	✓
Monitor health and alerts	With manual installation and configuration of SNMP Agents **NOTE:** SNMP Agents are not available on ESXi.	✓[4]	✓[4]
Launch iLO remote console[5]	✓	✓	✓
SSO (single sign-on) to iLO web interface	✓	✓	✓
Automatic firmware upgrade (iLO) to minimum supported version when added to the appliance	✓	✓	✓
Rack visualization and editing	✓	✓	✓
Automatic discovery of server hardware type	✓	✓	✓
Remote Support[6]		✓[7]	✓
Server profile features:			
BIOS settings		✓	✓[8]
Firmware		✓	✓

Table Continued

Feature	Supported server hardware		
	HPE ProLiant BL G7[1],[2]	**HPE ProLiant BL Gen8/Gen9/Gen10 and HPE ProLiant WS Gen8/Gen9/Gen10**	**HPE ProLiant DL Gen8/ Gen9/Gen10, HPE ProLiant ML Gen9, and HPE ProLiant XL Gen9/ Gen10**
Connections to networks	✓	✓	✓
Boot order[9]	✓	✓	✓[8], [10]
Local storage[11]		✓	✓[12], [13]
SAN storage	✓	✓	
Insight Control and Insight Control server provisioning	✓	✓[14]	✓[14]

[1] The appliance might report an unsupported status for some double-wide, double-dense ProLiant G7 server blade models, which means that the appliance cannot manage them.

[2] As of the SPP 2017.04.0, all G7 servers will be based-lined ("frozen") and will no longer be supported beginning in Gen10.

[3] Not all servers support monitoring power, cooling, and utilization.

[4] For the best information, install Agentless Management Service (AMS) on the server's OS.

[5] Remote console works up to the point of an OS booting. After the OS boots, the remote console on HPE ProLiant DLs requires iLO Advanced license.

[6] Requires a minimum iLO version of 2.1.

[7] HPE ProLiant WS Gen8 is not supported.

[8] HPE ProLiant DL580 Gen8 is not supported. See **ProLiant DL servers supporting local storage** for a list of models that support local storage.

[9] Due to a limitation in Gen9 BL server ROMs dated 8/27/14 or earlier, it is not possible to set the primary boot device when the boot mode is set to UEFI or UEFI Optimized. If Manage boot order is selected, a warning is displayed in the corresponding profile indicating this condition.

[10] Boot Order is not supported for HPE ProLiant XL260a, which is a UEFI class 3 server (UEFI boot only).

[11] Only supported with the embedded array controller. M.2 drives are supported in specific configurations. See **Supported storage controllers** for details.

[12] Selected models of HPE ProLiant DL Gen8 and Gen9 server hardware support local storage. See **ProLiant DL servers supporting local storage** for a list of models that support local storage.

[13] Local storage is not supported for XL170r, XL190r, and XL260w Gen10 servers. Also, local storage is not supported for XL260w Gen9 servers.

[14] HPE Insight Control and Insight Control server provisioning are not supported on Gen10 platforms.

Monitored Server Hardware

You can add rack mount and blade servers and monitor the hardware. The following hardware are supported as monitored:

- Any half or full height ProLiant BL G6 (with iLO 2)
- ProLiant BL680c G7
- Any ProLiant DL G6 (with iLO 2)

- Any ProLiant DL G7
- Any ProLiant ML Gen8 or Gen9 or Gen10
- Any ProLiant XL server
- HPE BL920s Gen8 or Gen9
- HPE Superdome Flex Server
- Any of the servers listed as managed can be monitored

NOTE: BL220c G7 is not supported.

ML10 is not supported for monitoring.

Server hardware monitoring features

When you monitor server hardware, the appliance supports the following features.

Feature	Monitored Server Hardware				
	ProLiant BL and DL G6 (with iLO 2)	**ProLiant BL and DL G7**	**ProLiant BL, DL, ML, XL Gen8/Gen9/ Gen10**	**ProLiant BL920 Gen8/ Gen9 (HPE BladeSystem Superdome)**	**HPE Superdome Flex server (Rack manager)**
Power on or power off the server	✓	✓	✓	✓	✓
View inventory data	✓	✓	✓	✓	✓
Monitor power, cooling, and utilization[1]		✓	✓	✓ [2]	
Monitor health and alerts	With manual installation and configuration of SNMP Agents[3]	With manual installation and configuration of SNMP Agents[3]	✓	✓	✓
Launch iLO remote console		✓	✓		
Remote support			✓ [4]		✓
SSO (single sign-on)		✓ [5]	✓ [5]	✓ [6]	

[1] Not all servers support monitoring power, cooling, and utilization.

[2] Utilization is not supported.

[3] SNMP Agents are not available on ESXi 5.x and 6.x.

[4] ProLiant ML10 is not supported by remote support.

[5] SSO to the iLO web interface.

[6] SSO to the Onboard Administrator (OA). Requires OA firmware version 8.4.84 and higher.

HPE BladeSystem enclosures

Remote support is available for c7000 enclosures.

The following enclosures can be added as managed or monitored:

- HPE BladeSystem c7000 Enclosure
- HPE BladeSystem c7000 Enclosure (RoHS compliant)
- HPE BladeSystem c7000 Platinum Enclosure (Platinum)

NOTE: HPE BladeSystem c3000 enclosures are not supported.

The following enclosure can be added as monitored only:

HPE BladeSystem Superdome Enclosure

The following rack managers can be added as monitored only:

HPE Superdome Flex Server

More information

- **HPE BladeSystem c7000 Enclosure**
- **HPE BladeSystem Superdome Enclosure**
- **HPE Superdome Flex Rack Manager**

Managed storage arrays

This section documents the storage system versions supported by HPE OneView storage automation capabilities. See **http://www.hpe.com/storage/spock** for additional interoperability and support requirements to follow when configuring storage systems in your environment.

- HPE 3PAR

  The following firmware versions are supported for the listed StoreServ 7000, 8000, 9000, 10000, 20000, and 20000 R2 family platforms.
  - 3PAR OS 3.1.3 MU1, MU2, MU3
  - 3PAR OS 3.2.1 MU1, MU2, MU3, MU4, MU5
  - 3PAR OS 3.2.2 MU1, MU2, MU3, MU4, MU6
  - 3PAR OS 3.3.1 EGA, MU1, MU2, MU3, MU4

- HPE StoreVirtual
  - StoreVirtual 3200 LHOS 13.x
  - StoreVirtual VSA LHOS 12.x
  - StoreVirtual LHOS 13.6

- HPE Nimble

- Nimble OS 4.5
- Nimble OS 5.0
- Nimble OS 5.1

Managed SAN Switches and SAN Managers

This section documents the minimum versions of SAN Manager supported by HPE OneView managed SAN automation capabilities, which include auto-zoning. See **http://www.hpe.com/storage/spock** for additional interoperability and support requirements to follow when configuring SAN switches in your environment.

HPE FlexFabric switches

HPE FlexFabric 5700 products with HPE Comware software versions 7.1.045 Release 2422.x:

- HPE FlexFabric 5700 40XG 2QSFP+ Switch
- HPE FlexFabric 5700 32XGT-8XG 2QSFP+ Switch
- HPE FlexFabric 5700 48G-4XG 2QSFP+ Switch

HPE FlexFabric 5900 products, with HPE Comware software minimum version 7.1.045 Release 2422.x:

- HPE FlexFabric 5900CP 48XG 4QSFP+ Switch
- HPE FlexFabric 5900AF 48XG 4QSFP+ Switch
- HPE FlexFabric 5900AF 48XGT 4QSFP+ Switch

HPE FlexFabric 5930 products, with HPE Comware software minimum version 7.1.045 Release 2422.x:

- HPE FlexFabric 5930 32QSFP+ Switch
- HPE FlexFabric 5930 2-slot 2QSFP+ Switch
- HPE FlexFabric 5930 4-slot Switch

HPE FlexFabric 5940 products, with HPE Comware software minimum version 7.1.070, Release 2609H01:

- HPE FlexFabric 5940 48SFP+ 6QSFP28 Switch
- HPE FlexFabric 5940 48XGT 6QSFP28 Switch
- HPE FlexFabric 5940 48XGT 6QSFP+ Switch
- HPE FlexFabric 5940 48SFP+ 6QSFP+ Switch
- HPE FlexFabric 5940 32QSFP+ Switch
- HPE FlexFabric 5940 2-slot Switch
- HPE FlexFabric 5940 4-slot Switch

HPE FlexFabric 5710 switches, with HPE Comware software minimum version 7.1.070, Release 2612P03

NOTE: Leveraged by FF5940

- HPE FlexFabric 5710 48SFP+ 6QSFP+ or 2QSFP28 Switch
- HPE FlexFabric 5710 48XGT 6QSFP+ or 2QSFP28 Switch
- HPE FlexFabric 5710 24SFP+ 6QSFP+ or 2QSFP28 Switch

HPE FlexFabric 5950 products, with HPE Comware software minimum version 7.1.070, R6205P03H01:

- HPE FlexFabric 5950 48SFP28 8QSFP28 Switch
- HPE FlexFabric 5950 4-slot Switch

HPE FlexFabric 79xx chassis switches, with HPE Comware software minimum version 7.1.070 Release 2138.x:

- HPE FlexFabric 7904 Switch Chassis
- HPE FlexFabric 7910 Switch Chassis

HPE FlexFabric 5980 switch, with HPE Comware software minimum version 7.1.070, Release 2712H03:

HPE FlexFabric 5980 48SFP+ 6QSFP28 Switch

NOTE: Leveraged by 7900.

HPE FlexFabric 129xxx chassis switches, with HPE Comware software minimum version 7.1.070 Release 1138.x:

- HPE FlexFabric 12916 Switch AC Chassis
- HPE FlexFabric 12910 Switch AC Chassis

Brocade switches

Brocade 8 Gb, 16 Gb, and 32 Gb FC SAN switches with HPE Network Advisor or Brocade Network Advisor (BNA) software: 12.1.4, 12.1.5, 12.1.6, 12.3.1, 12.3.3, 12.3.4, 12.4, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 14.0, 14.0.1, 14.0.2, 14.0.3, 14.2.1, 14.2.2, 14.3.1, 14.4.2, and 14.4.3

NOTE: BNA 14.2.0 and 14.4.1 are known not to operate correctly with all HPE OneView releases.

Cisco Nexus switches

Cisco Nexus 5500/5600/6000 models — NX-OS 6.0, 7.0, 7.1, 7.2, 8.3:

- Cisco Nexus 5548UP
- Cisco Nexus 5596UP
- Cisco Nexus 5672UP
- Cisco Nexus 6001P
- Cisco Nexus 6004EF

Cisco MDS switches

Cisco MDS 9xxx model 8, 16, 32 Gb FC SAN switches - NX-OS 6.2, 8.1, 8.2, 8.3

Networking LOM and mezzanine cards

The following adapters are supported. If an adapter is not listed, it belongs to **unmanaged support**. Unmanaged support means that the adapter can exist in the server and function as required, but it is not managed by HPE OneView. The adapter might still be usable depending on the model the adapter is connected to. For example, an interconnect module. The appliance reports the existence of the adapter on the **Server Hardware** or **Server Hardware Types** screens in the appliance UI.

NOTE: When using these components with external storage, see **http://www.hpe.com/storage/spock** for more information on using the following components with external storage and for information on additional interoperability and support requirements.

NOTE: Unmanaged adapters within a server that are managed by the server profile can be updated, if a firmware bundle contains an update for the unmanaged adapters.

Supported LOM and mezzanine cards

FlexFabric adapters

- HPE FlexFabric 10Gb 2-port 534M Adapter[1]
- HPE FlexFabric 10Gb 2-port 554M Adapter
- HPE FlexFabric 20Gb 2-port 630M Adapter [1]
- HPE FlexFabric 20Gb 2-port 650M Adapter
- HPE FlexFabric 10Gb 2-port 534FLB Adapter [1]
- HPE FlexFabric 10Gb 2-port 536FLB Adapter [1]
- HPE FlexFabric 10Gb 2-port 554FLB Adapter
- HPE FlexFabric 20Gb 2 port 630FLB Adapter [1]
- HPE FlexFabric 20Gb 2-port 650FLB Adapter
- HPE FlexFabric 10Gb Dual Port NC551i Converged Network Adapter
- HPE FlexFabric 10Gb Dual Port NC553i Converged Network Adapter

[1] iSCSI CHAP names are limited to 128 characters.

Ethernet and Flex-10 Ethernet adapters

- HPE Flex-10 10Gb 2-port 530M Adapter
- HPE Flex-10 10Gb 2-port 530FLB Adapter
- HPE Flex-10 10Gb 2-port 552M Adapter

Fibre Channel adapters

- HPE QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HPE QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- QLogic QMH2562 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HPE LPe1205A 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

- HPE LPe1605 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- Emulex LPe1205-HPE 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

Interconnect modules

NOTE: When using the components with external storage, see **http://www.hpe.com/storage/spock** for additional interoperability and support requirements when configuring these in your environment.

Table 8: Supported interconnect modules

Device	Full support	Monitored support c7000[1]	Unmanaged support c7000[2]	Unmanaged support Superdome[7]
HPE Virtual Connect FlexFabric-20/40 F8 Module[3]	✓			
HPE Virtual Connect FlexFabric-20/40 F8 TAA Module[3]	✓			
HPE Virtual Connect FlexFabric 10Gb/24-Port Module	✓			
HPE Virtual Connect Flex-10 10Gb Ethernet Module	✓			
HPE Virtual Connect Flex-10/10D Module	✓			
HPE Virtual Connect 8Gb 20-port Fibre Channel Module	✓			
HPE Virtual Connect 8Gb 24-port Fibre Channel Module[4]	✓			
HPE Virtual Connect 16Gb 24-port Fibre Channel Module[4, 8]	✓			
HPE Virtual Connect 16Gb 24-port Fibre Channel TAA Module[4, 9]	✓			
Cisco Fabric Extender for HPE BladeSystem[5]	✓[6]	✓		
HPE 1/10 Gb Ethernet Switch Pass-thru Module			✓	✓
HPE 6127XLG Blade Switch			✓	✓
HPE 6125XLG Blade Switch			✓	✓
HPE 6120G/XG Blade Switch			✓	✓
Brocade 16Gb SAN Switch for HPE BladeSystem c-Class			✓	✓

Table Continued

Device	Full support	Monitored support c7000[1]	Unmanaged support c7000[2]	Unmanaged support Superdome[7]
HPE 4X FDR InfiniBand Switch for BladeSystem c-Class			✓	✓
All other HPE and non-HPE interconnect modules			✓	

[1] Available for basic power and health monitoring.

[2] Unmanaged support means that the device can exist in the enclosure and function as-is, but it is not managed by HPE OneView.

[3] Minimum Virtual Connect firmware version supported is 4.20.

[4] Fibre Channel firmware version 3.01 or higher is required for HPE OneView to manage the module. Minimum Virtual Connect firmware version supported is 4.40.

[5] Also known as the Cisco Nexus B22 Blade Fabric Extender for HPE.

[6] A separate HPE OneView B22HP FEX Management License is required.

[7] These interconnects are supported in an HPE BladeSystem Superdome Enclosure. The HPE BladeSystem Superdome Enclosure can be added as monitored only.

[8] Supports part numbers 751465-B21 and P08475-B21 for this module.

[9] Supports part numbers 778720-B21 and P08476-B21 for this module.

Interconnect requirements

For all the interconnect modules

- For the limits on the maximum number of 10GBase-T SFP+ transceivers for each VC Enet module, see *Virtual Connect Release Notes*.
- Interconnect modules in horizontal pairs (for example, Bay 1 and Bay 2 of an enclosure) must be the same model. The peer bay can also be unpopulated, but you lose horizontal redundancy.

For HPE Virtual Connect FlexFabric-20/40 F8 Module for c-Class BladeSystem, HPE Virtual Connect 16Gb 24-port Fibre Channel Module for c-Class BladeSystem, and Virtual Connect 16Gb 24-port Fibre Channel TAA Module for c-Class BladeSystem

- Customers can now manage, monitor, and provide remote support for c-Class Interconnect devices such as Virtual Connect and Fibre Channel.

  The interconnects supported with OneView Remote Support:

  - HPE Virtual Connect FlexFabric-20/40 F8 Module for c-Class BladeSystem
  - HPE Virtual Connect 16Gb 24-port Fibre Channel Module for c-Class BladeSystem

For HPE Virtual Connect 8Gb 20-port Fibre Channel, HPE Virtual Connect 16Gb 24-port Fibre Channel, and HPE Virtual Connect 8Gb 24-port Fibre Channel modules

- Interconnect modules are for fabric-attach only.
- Interconnect firmware version must be at or higher than the firmware versions listed in **Minimum firmware requirements for managed and monitored devices** on page 8.
- Interconnect modules cannot be placed in bays 1 or 2.

For HPE Virtual Connect FlexFabric-20/40 F8 modules

- Interconnect module requires 10 fans in an enclosure.
- Do not insert more than 6 HPE Virtual Connect FlexFabric–20/40 F8 modules in one enclosure.
- If configured for 4x10G operation, a pluggable module with an attached splitter cable must be installed to multiplex the QSFP+ port into four SFP+ ports on the remote end.
- HPE Virtual Connect FlexFabric-20/40 F8 modules are supported on c7000 enclosures with the following SKUs: 5*XXXXX*-B21, 6*XXXXX*-B21, and 7*XXXXX*-B21.

FCoE is supported on these interconnects and corresponding ports

- HPE Virtual Connect FlexFabric 10Gb/24-port ports X1-X4 only
- HPE Virtual Connect Flex-10/10D Ethernet Module ports X1-X10
- HPE Virtual Connect FlexFabric-20/40 F8 module ports Q1-Q4, X1-X8

More information

Minimum firmware requirements for managed and monitored devices

Ethernet switches

The following Ethernet switches are supported for monitoring and basic configuration when attached to HPE Virtual Connect Flex-10 and FlexFabric interconnects, as well as Cisco Fabric Extender modules. Monitoring is provided for the physical switch information, physical port information, port statistics, health events, and port state changes, as well as for the network availability between enclosure edge and upstream switches. Optionally, a control of the port state and network provisioning between enclosure edge and upstream switch ports can be enabled as part of the basic configuration.

Switch Type	Minimum Supported Version
Cisco Nexus 5548UP Switch Cisco Nexus 5596UP Switch	NX-OS 6.0(2)N2(7)
	NX-OS 7.0(8)N1(1)
	NX-OS 7.1
	NX-OS 7.2
	NX-OS 7.3[1]
Cisco Nexus 5672UP Switch Cisco Nexus 5612UP Switch	NX-OS 6.0(2)N2(7)
	NX-OS 7.0(8)N1(1)

Table Continued

Switch Type	Minimum Supported Version
	NX-OS 7.1
	NX-OS 7.2
	NX-OS 7.3[1]
Cisco Nexus 6001P Switch	NX-OS 7.0(8)N1(1)
Cisco Nexus 6004EF Switch	NX-OS 7.1
	NX-OS 7.2
	NX-OS 7.3[1]

[1] The NX-OS 7.3(2)N1(1) variant is not supported due to Cisco support limitations. For more information, see Cisco defect: SR 683379290.

Adapter and HPE Virtual Connect configurations

HPE OneView supports network connectivity through the following adapter and HPE Virtual Connect module configurations.

Table 9: Supported FLB/LOM/mezzanine adapter configurations

Configuration	FlexFabric Adapters	Flex-10 Adapters	Ethernet Adapters
HPE Virtual Connect FlexFabric 20/40 F8 Module with VC f/w 4.50 or higher, and either HPE FlexFabric 20Gb 2-port 650FLB/M Adapter or HPE FlexFabric 10GB 2-port 556FLB Adapter	8 FlexNICs or 7 FlexNICs and 1 FlexHBA per physical port[1]	4 FlexNICs per physical port (Ethernet only)	No connectivity
HPE Virtual Connect FlexFabric 10Gb/24-port Module	4 FlexNICs or 3 FlexNICs and 1 FlexHBA per physical port	4 FlexNICs per physical port (Ethernet only)	

Table Continued

Configuration	FlexFabric Adapters	Flex-10 Adapters	Ethernet Adapters
HPE Virtual Connect Flex-10/10D Module HPE Virtual Connect Flex-10 10Gb Module	4 FlexNICs per physical port (Ethernet only)		
Ethernet Interconnect (external manager)	2x physical ports[2]		

[1] One of the four FlexNICs can be configured for storage functionality using FCoE (Fibre Channel over Ethernet). Ethernet is available on all four FlexNICs. HPE OneView configures FlexNIC network connectivity using server profile connections, such as device type, network or VLAN settings, and bandwidth settings.

[2] Not managed by HPE OneView. HPE OneView retains the physical ports in their unconfigured, default state. You can obtain network connectivity using a standard ethernet interconnect or ethernet passthrough module in the adjacent IO bays of the enclosure.

Racks and power

- HPE Intelligent Power Distribution Units (Firmware version 1.4 and later)
- HPE Intelligent Series Racks
- HPE Location Discovery Services for Software and Firmware (ProLiant DL Gen8 rack mount servers and HPE BladeSystem c7000 enclosures with the following SKU: 5*XXXXX*-B21, 6*XXXXX*-B21, and 7*XXXXX*-B21

Supported storage controllers

The following embedded controllers are supported when configuring a local storage in the server profile.

- HPE Smart Array P220i
- HPE Smart Array P230i
- HPE Smart Array P244br
- HPE Smart Array P246br
- HPE Smart Array P420i
- HPE Smart Array P440ar
- HPE Smart Array P830i
- HPE Smart Array P840ar
- HPE Dynamic Smart Array B140i
- HPE Dynamic Smart Array B320i
- HPE Dynamic Smart Array S100i

- HPE Smart HBA H244br
- HPE Smart HBA H240ar
- HPE Smart HBA H450ar
- HPE Smart Array E208i-a SR Gen10
- HPE Smart Array P408i-a SR Gen10
- HPE Smart Array P204i-b SR Gen10

Table 10: Supported M.2 drive configurations

Storage controller	M.2 drives AND front drives installed	ONLY M.2 drives installed
B140i	All local storage must be managed by HPE OneView	M.2 drives are managed by HPE OneView, no profile mobility
P244br H244br P246br	Front drives are managed by HPE OneView M.2 drives must be managed manually outside of HPE OneView	M.2 drives are not managed by HPE OneView, they must be managed manually outside of HPE OneView

ProLiant DL servers supporting local storage

NOTE: All supported Gen10 servers support local storage.

Table 11: ProLiant DL servers supporting local storage

Model	Gen8	Gen9	Gen 10
DL360		✓	✓ [1]
DL360p	✓		
DL380		✓	✓ [1]
DL380p	✓		
DL560	✓	✓	✓
DL580	✓	✓	✓

[1] The model supports HPE Composable Cloud for ProLiant DL.

Hypervisor managers

You can register VMware vCenter server as a hypervisor manager in HPE OneView. This hypervisor manager is used by the hypervisor cluster profile for managing the hypervisors and clusters.

VMware vCenter server	• 6.0 • 6.0 update 1 • 6.0 update 2 • 6.0 update 3 • 6.5 • 6.5 update 1 • 6.5 update 2 • 6.7 update 1

Hypervisors in a managed hypervisor cluster

Using hypervisor cluster profiles, you can manage cluster of hypervisors that are running on servers which support HPE Virtual Connect and managed by HPE OneView. These are HPE ProLiant BL blade servers — Gen8, Gen9, and Gen10. Additionally, within the HPE Composable Cloud for ProLiant DL solution, using hypervisor cluster profiles you can manage a cluster of hypervisors that are running on the selected DL Gen10 servers purchased with the solution that are connected to the HPE Composable Fabric and are managed by HPE OneView.

The following are the supported hypervisors that can be managed as a cluster.

VMware vSphere ESXi	• 6.0 • 6.0 update 1 • 6.0 update 2 • 6.0 update 3 • 6.5 • 6.5 update 1 • 6.5 update 2 • 6.7 update 1

You can specify the OS deployment plan as **None** in the hypervisor cluster profiles and use the external tools of your choice to deploy hypervisors on the server. The hypervisors that are deployed using external tools can be imported into a hypervisor cluster profile to manage them.

Using the hypervisor cluster profiles, you can manage life cycle operations such as grow or shrink the hypervisor cluster, modify configurations, perform consistency checks, and rolling updates. You can also conduct nondisruptive firmware updates on the server nodes.

If you use **HPE OneView for VMware vCenter** software for managing the hypervisor clusters and **HPE Insight Control server provisioning** for deploying hypervisors, you will see the hypervisor cluster profiles configured with an **HPE Insight Control server provisioning** deployment plan in HPE OneView. You cannot edit these hypervisor cluster profiles using HPE OneView user interface. However, you can manage other life cycle operations such as view and resolve inconsistencies with rolling updates, nondisruptive firmware updates on the server nodes.

HPE OneView does not currently support managing the life cycle of VMware vSAN cluster using the hypervisor cluster profiles.

Device support for HPE OneView virtual appliances in FIPS and CNSA mode

The following tables provide information on the capability of devices that are managed by HPE OneView virtual appliances when switched to Federal Information Processing Standard (FIPS) or Commercial National Security Algorithm (CNSA) mode.

IMPORTANT: FIPS/CNSA cryptography applies only to a VM appliance managing non-c7000 hardware.

FIPS mode information

Device/External server	Supported in HPE OneView FIPS mode	Customer action required	If not supported in FIPS mode, expected behavior of the device/feature when switched to FIPS mode	Description
Intelligent Modular PDU (iPDU)	No	iPDU does not support TLSv1.1+. The maximum keysize is 1024 and does not support SNMPv3, so essentially is not FIPS compliant.		Will be moved to **`Unmanaged`** state. Warning message (static) will be provided for all iPDUs during the mode switch Compatibility report.
Server hardware firmware and driver updates	Yes	Yes, for the online updates, the customer has to provide the iLO 5 credentials through SUT CLI.	A generic warning will be issued in the Compatibility report informing the user that updates will not work for iLO 5/ Gen10 servers in the offline mode. For the online mode, the alert will be modified to inform the user to install SUT and provide credentials using CLI. Updates will continue to work for iLO 4 in FIPS mode.	

Table Continued

Device/External server	Supported in HPE OneView FIPS mode	Customer action required	If not supported in FIPS mode, expected behavior of the device/feature when switched to FIPS mode	Description
External repositories	No	No	A generic warning will be issued in the Compatibility report.	External repositories are not yet supported in the FIPS/CNSA modes. Internal repositories will continue to work in all modes.
External repositories such as enterprise directory servers	Yes	No action required if the enterprise directory server is already configured to be FIPS compliant. Otherwise, customers need to configure the TLS protocols cipher-suites and certificate configured on the enterprise directory server to be FIPS compliant.	A generic warning will be issued in the Compatibility report.	Communication with enterprise directory servers uses TLS connection and will go through seamlessly if the protocols and cipher-suites of the server matches to that of HPE OneView.
External repositories such as Email servers	Yes with TLS option	No action required if the SMTP server is already configured to be FIPS compliant. Otherwise, customers need to configure the TLS protocols cipher-suites and certificate configured on the SMTP server to be FIPS compliant.	A generic warning will be issued in the Compatibility report.	

Table Continued

Device/External server	Supported in HPE OneView FIPS mode	Customer action required	If not supported in FIPS mode, expected behavior of the device/feature when switched to FIPS mode	Description
External repositories such as remote backup servers	Yes	Yes. Customers need to change the SSH algorithms to match the supported algorithms listed in the compatibility report.	A generic warning will be issued in the Compatibility report.	Remote backup servers have SMTP and SSH outbound connections that will auto negotiate to the restricted ciphers.
External repositories such as Proxy servers	Yes	No.	A generic warning will be issued in the Compatibility report.	Communication with proxy servers uses TLS connection and will go through seamlessly if the protocols and cipher-suites of the server matches to that of HPE OneView.
iLO 5 (Gen10 or higher) with firmware 1.11 or later	Yes	Yes. May need to add a FIPS strength certificate to iLO, if iLO not already in FIPS mode, or, need to manually place iLO in FIPS mode. FIPS mode initiates a factory reset. User must refresh the server at that point.		Firmware 1.11 revision is submitted for FIPS validation.

Table Continued

Device/External server	Supported in HPE OneView FIPS mode	Customer action required	If not supported in FIPS mode, expected behavior of the device/feature when switched to FIPS mode	Description
iLO 4 (Gen8/Gen9) with firmware 1.11 or later	No	Yes. May need to add a FIPS strength certificate to iLO, if iLO not already in FIPS mode, or, need to manually place iLO in FIPS mode. FIPS mode initiates a factory reset. User must refresh the server at that point.		
iLO 4 (Gen8/Gen9) with firmware version prior to 2.11	No	Upgrade firmware before using.	A generic warning will be issued in the Compatibility report.	

CNSA mode information

Device/External server	Supported in HPE OneView CNSA mode	Customer action required	If not supported in CNSA mode, expected behavior of the device/feature when switched to CNSA mode	Description
Intelligent Modular PDU (iPDU)	No	iPDU does not support TLSv1.1+. The maximum keysize is 1024 and does not support SNMPv3, so essentially is not FIPS compliant.		Will be moved to **`Unmanaged`** state. Warning message (static) will be provided for all iPDUs during the mode switch Compatibility report.
Server hardware firmware and driver updates (offline firmware update)	Yes	No action is required. The firmware update is supported in the CSNA mode for the **Firmware Only** option.	A generic warning will be issued in the Compatibility report.	

Table Continued

Device/External server	Supported in HPE OneView CNSA mode	Customer action required	If not supported in CNSA mode, expected behavior of the device/feature when switched to CNSA mode	Description
Server hardware firmware and driver updates (online firmware update)	No	Yes, for the online updates, the customer has to provide the iLO 5 credentials through SUT CLI.	A generic warning will be issued in the Compatibility report informing the user that updates will not work for iLO 5/ Gen10 servers in the offline mode. For the online mode, the alert will be modified to inform the user to install SUT and provide credentials using CLI. Updates will continue to work for iLO 4 in FIPS mode.	
External repositories	No	Needs to enable FIPS/CNSA mode settings in the web server hosting the external repository.	A generic warning will be issued in the Compatibility report.	External repositories are not yet supported in the FIPS/CNSA modes. Internal repositories will continue to work in all modes.
External repositories such as enterprise directory servers	Yes	No action required if the enterprise directory server is already configured to be CNSA compliant. Otherwise, customers need to configure the TLS protocols cipher-suites and certificate configured on the enterprise directory server to be CNSA compliant.	A generic warning will be issued in the Compatibility report.	Communication with enterprise directory servers uses TLS connection and will go through seamlessly if the protocols and cipher-suites of the server matches to that of HPE OneView.

Table Continued

Device/External server	Supported in HPE OneView CNSA mode	Customer action required	If not supported in CNSA mode, expected behavior of the device/feature when switched to CNSA mode	Description
External repositories such as Email servers	Yes with TLS option	No action required if the SMTP server is already configured to be CNSA compliant. Otherwise, customers need to configure the TLS protocols cipher-suites and certificate configured on the SMTP server to be CNSA compliant.	A generic warning will be issued in the Compatibility report.	
External repositories such as remote backup servers	Yes	Yes. Customers need to change the SSH algorithms to match the supported algorithms listed in the compatibility report.	A generic warning will be issued in the Compatibility report.	Remote backup servers have SMTP and SSH outbound connections that will auto negotiate to the restricted ciphers.
External repositories such as Proxy servers	Yes	No.	A generic warning will be issued in the Compatibility report.	Communication with proxy servers uses TLS connection and will go through seamlessly if the protocols and cipher-suites of the server matches to that of HPE OneView.

Table Continued

Device/External server	Supported in HPE OneView CNSA mode	Customer action required	If not supported in CNSA mode, expected behavior of the device/feature when switched to CNSA mode	Description
iLO 5 (Gen10 or later)	Yes	The iLO must be placed in SuiteB mode, which is really CNSA mode. This action requires an iLO Advance High Security license. Also, SuiteB mode is only available when the iLO is in FIPS mode.	A generic warning will be issued in the Compatibility report.	
iLO 4 (Gen9)	No		A generic warning will be issued in the Compatibility report.	

Configuration maximums

Allocated IDs

Table 12: Allocated ID configuration maximums

Resource	Maximum
MAC ranges	66,240
WWN ranges	15,360
Virtual SN (serial number) ranges	1,280

Appliance

Table 13: Appliance configuration maximums

Resource	Maximum
Maximum disk space for firmware bundles	100 GB
Concurrent users	5

NOTE: Users can add more SPPs by using an external repository.

Connections

Table 14: Connection configuration maximums

Resource	Maximum
Connections per physical port (maximum FlexNICs)	8[1]
Physical ports per server:	
Half-height server blades	6 ports (dual-port LOM card and 2 mezzanine cards)
Full-height server blades	10 ports (2 dual-port LOM cards and 3 mezzanine cards)
Connections per server (on average)	24
Reserved connections[2]	4,800

Table Continued

Resource	Maximum
Deployed connections[3]	61,440
Total number of connections	66,240

[1] See **Adapter and HPE Virtual Connect configurations** for configuration information.

[2] Connections that have been created, but are not yet associated with any specific interconnect downlink.

[3] Connections that have been assigned to a physical interconnect port and possibly a sub-port (FlexNIC on the server).

SAN Storage

Table 15: Enclosure configuration maximums

Resource	Maximum
Volumes	10,000
Storage Systems	40

Enclosures

Table 16: Enclosure configuration maximums

Resource	Maximum
Enclosures	54
Enclosure groups	54
Logical enclosures	54
Interconnects in all enclosures	240

Networking limits

Table 17: Networking limits configuration maximums

Resource	Maximum
Total number of network sets	1,000
Ethernet tagged networks per regular network set (Blade System and rack mount)	162
Ethernet tagged networks per large network set (rack mount)	4000

Table Continued

Resource	Maximum
Logical interconnect groups	240
Logical interconnects	240
Uplink sets per logical interconnect	144

Networks

Table 18: Network configuration maximums

Resource	Maximum
Tagged, untagged, tunneled, and FCoE networks defined	8,192
Provisioned Ethernet networks per logical interconnect	1,000
Native FC networks (including FCoE/FC bridged networks), which can be defined	255
Fibre Channel networks per interconnect	8
Fibre Channel networks per logical interconnect or enclosure	48
Total SNMP trap destinations per logical interconnect of which up to 5 can be designated as Fibre Channel.	25
Networks per logical interconnect or enclosure	1,048
Networks per physical downlink (Blade System)	162
Networks per physical downlink (rack mount)	4000
Networks per uplink set	1,000
FCoE networks per uplink set or per interconnect	32
Maximum number of private networks per logical interconnect	128

Power and facilities

Table 19: Power and facility configuration maximums

Resource	Maximum
Data centers	640
Racks	640
PDDs (power delivery devices)	82,016
Unmanaged devices	26,880
iPDUs	2,560
iPDU components (load segments and outlets)	76,800
Branch circuits	2,560
Breaker panels	64
Power feeds	32

Server hardware

Table 20: Server configuration maximums

Resource	Maximum
Enclosures	54
Total number of servers[1]	1024
Managed servers	740
Monitored servers	1024
Rack managers	20
Total number of servers[2]	160
Interconnect modules	240

[1] You can add servers as managed or monitored. Out of the total number of servers you can add, HPE OneView allows you to have any combination of managed and monitored servers up to the maximum number supported of each type.

[2] You can add rack manager servers as monitored. Number of supported servers vary from 20 to 160.

- 20 servers: 1 partition of 8 chassis in a single rack manager
- 160 servers: 8 partition of 1 chassis each in a single rack manager

Server profiles

Table 21: Server profile configuration maximums

Resource	Maximum
Total number of assigned server profiles	740
Total number of unassigned server profiles	100

Certificate chain depth

Table 22: Certificate chain depth configuration maximums

Resource	Maximum
Number of CA certificates present in the certificate chain	9

Hypervisor cluster profiles

Table 23: Hypervisor cluster profiles configuration maximums

Resource	Maximum
Number of hypervisors managed by a hypervisor cluster profile configured with 100 networks	32
Number of hypervisors managed by a hypervisor cluster profile configured with 200 networks	24

Websites

Website	Link
Hewlett Packard Enterprise Information Library	**www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**
Contact Hewlett Packard Enterprise Worldwide	**www.hpe.com/assistance**
HPE OneView Documents	**www.hpe.com/info/oneview/docs**
Subscription Service/Support Alerts	**www.hpe.com/support/e-updates**
Software Depot	**www.hpe.com/support/softwaredepot**
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 Virtual Connect user guides HPE Virtual Connect command line references	**http://www.hpe.com/info/vc/manuals**
HPE 3PAR StorServ Storage	**http://www.hpe.com/info/storage**
iLO	**http://www.hpe.com/info/ilo**
HPE BladeSystem enclosures	**http://www.hpe.com/servers/bladesystem**
HPE ProLiant server hardware websites	• General information: **www.hpe.com/info/servers** • BL series server blades: **http://www.hpe.com/info/blades** • DL series rack mount servers: **http://www.hpe.com/servers/dl**
HPE Composable Cloud for ProLiant DL	**Hewlett Packard Enterprise Information Library**
Storage white papers and analyst reports	**www.hpe.com/storage/whitepapers**

HPE OneView Remote Technician

Speed issue resolution with HPE OneView Remote Technician. With HPE OneView Remote Technician, troubleshooting and resolving support issues is faster and easier. At your invitation, authenticated HPE support technicians access your HPE OneView appliance through a secure TLS connection to troubleshoot and diagnose issues.

- You do not have to be present when a trusted HPE support technician diagnoses the issue, including downloading logs directly without the need for an FTP site.
- HPE OneView Remote Technician is built into HPE OneView 4.1 and later with no additional applications.
- To access HPE OneView Remote Technician, open the **Diagnostics** menu within the **HPE OneView Settings** page.
- Does not require HPE OneView Remote Support.

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/info/assistance

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

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

Information to collect

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

Accessing updates

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

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

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

  www.hpe.com/support/AccessToSupportMaterials

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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