



**Hewlett Packard
Enterprise**

HPE OneView 5.0 User Guide

Abstract

The User Guide is intended for administrators who are using the HPE OneView appliance graphical user interface or REST APIs to manage IT hardware in a converged infrastructure environment on virtual machine technology.

Part Number: P01322-004
Published: August 2019
Edition: 1

Notices

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

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

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

Acknowledgments

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

Contents

Learning about HPE OneView.....9

HPE OneView Highlights.....10

HPE OneView for infrastructure management	10
HPE OneView licensing.....	12
Managing, monitoring, or migrating server hardware on enclosures.....	14
Provisioning features.....	14
Resource templates, groups, and sets.....	15
Server profiles and server profile templates.....	17
Streamlined process for bringing hardware under management.....	18
Operating system deployment.....	19
Storage provisioning and management.....	19
About HPE Nimble storage systems.....	20
Firmware and configuration change management features.....	21
Simplified firmware management.....	21
Simplified configuration change management.....	22
Hypervisor cluster import and management.....	22
Networking features.....	22
Monitoring the environment and responding to issues.....	23
Data center environmental management.....	24
Resource utilization monitoring.....	24
Activity and health management	25
Hardware, firmware, and driver inventory information.....	25
Remote Support.....	25
Backup and restore features.....	25
Security features.....	26
High availability features.....	27
Tutorial and Guided setup.....	27
Graphical and programmatic interfaces.....	27
Integration with other management software	28
Other management software warnings.....	28
Open integration.....	29
Smart Update Tools features.....	30

Understanding the resource model.....31

Resource model summary diagram.....	31
Appliance.....	32
Connections.....	33
Connection templates.....	34
Data centers.....	34
Domains.....	35
Enclosures.....	35
Enclosure groups.....	36
Enclosure types.....	36
Hypervisor Manager.....	37
Hypervisor Cluster Profiles.....	37
Hypervisor profile.....	38
Interconnects.....	38

Interconnect types.....	39
Logical enclosures.....	40
Logical interconnects.....	40
Logical interconnect groups.....	41
Logical switches.....	42
Logical switch groups.....	43
Networks.....	43
Network sets.....	44
Power delivery devices.....	44
Rack Managers.....	45
Racks.....	45
SAN Managers.....	46
SANs.....	46
Server hardware.....	47
Server hardware types.....	48
Server profiles.....	48
Server profile templates.....	49
Storage Pools.....	50
Storage Systems.....	51
Switches.....	51
Unmanaged devices.....	51
Uplink sets.....	52
Volumes.....	53
Volume Templates.....	53

Using HPE OneView GUI or REST API scripts..... 54

About accessing HPE OneView message buses.....	54
--	----

How to get started with HPE OneView.....55

Smart Update Tools installation with HPE Insight Control server provisioning.....	55
---	----

Accessing documentation and help.....56

Online help—conceptual and task information as you need it.....	56
This user guide supplements the online help.....	56
Where to find HPE OneView documentation.....	56
Enable off-appliance browsing of UI help	57

Planning tasks..... 58

Planning your data center resources..... 59

How many data centers?.....	59
Managing, monitoring, or migrating server hardware?.....	59
Security planning.....	59
Preparing your data center network switches.....	59
Planning for a dual-stack implementation.....	59
Planning your resource names.....	59
Planning the appliance configuration.....	61
Planning for multiple instances of HPE OneView.....	61
Planning for high availability.....	61
Separate networks for data and management.....	62
Time clocks and NTP.....	62

IP addresses.....	62
Planning for configuration changes.....	63
Configuration changes that require or result in resource outages.....	63
Configuration changes that might require changes to multiple resources.....	64
Adding a network.....	64
Adding an enclosure	65
Planning for enclosure migration from VCM into HPE OneView.....	66
Timing and type of migration.....	66
Understanding the migration process.....	66
Warning issues.....	68
Security in HPE OneView.....	70
Best practices for maintaining a secure appliance	71
Understanding the security features of HPE OneView.....	75
About security settings.....	75
About complex passwords.....	75
About cryptography mode settings.....	76
About directory service authentication.....	78
Enable cross-domain authentication using the global catalog.....	82
About emergency local login.....	83
About permissions.....	83
About scopes.....	83
About trusting certificates	84
About user accounts.....	84
About user roles.....	86
Action privileges for user roles.....	88
Algorithms, cipher suites, and protocols for securing the appliance.....	98
Protocols supported by the appliance.....	100
Algorithms and cipher suites supported in legacy mode.....	100
Algorithms and ciphers suites supported in FIPS 140-2 mode.....	109
Algorithms and ciphers supported in CNSA mode.....	115
Scope-enabled resource categories.....	118
Security-hardened appliance.....	119
Creating a login session.....	120
Authentication for appliance access	120
Two-factor Authentication.....	121
Certificate owner - Subject alternative name attributes.....	123
Certificate owner - Subject attributes.....	124
Directory domain.....	124
Requirements to validate the certificate.....	125
Controlling access for authorized users.....	125
Specifying user accounts and roles.....	125
Mapping of SSO roles for iLO and OA.....	126
Mapping appliance interactions with iLO, OA, and iPDU	126
Secure Shell access.....	127
Protecting credentials.....	128
About audit log.....	128

About audit log forwarding.....	129
Choosing a policy for the audit log.....	130
Appliance access over TLS	130
Managing certificates from a browser.....	130
Use a certificate authority.....	131
Self-signed certificate.....	131
Create an appliance certificate signing request.....	131
Create an appliance self-signed certificate.....	132
Create a CA-signed client certificate for SCMB.....	132
Import an appliance certificate.....	134
Trusting a certificate.....	135
View the Certificate settings.....	135
Download a self-signed certificate.....	135
Verify a certificate.....	137
Nonbrowser clients.....	137
Passwords.....	137
TLS connection.....	137
SSH connection.....	137
Ports required for HPE OneView.....	137
Controlling access to the appliance console.....	140
Switching from one console to another (VMware vSphere and Microsoft Hyper-V)	140
Switching from one console to another (KVM).....	140
Enable or disable authorized services access.....	140
Restricting console access.....	141
Files you can download from the appliance	142
Handling MD5 certificates.....	142

Modeling scope-based access control in HPE OneView.....144

About scope-based access control.....	144
Scope-based access control authorization semantics.....	144
Scope-based access control facts.....	146
Scope-based access control implementation process.....	147
Design the authorization model.....	147
Configure the authorization model.....	149
Scope-based access control example: Scenario overview.....	149
Example: Identify users and groups.....	150
Example: Determine the best fit HPE OneView role.....	150
Example: Define permission scopes	153

Certificate management..... 157

HPE OneView appliance certificate.....	157
Establishing trust between a web browser and HPE OneView.....	157
Establishing trust between HPE OneView and remote devices.....	158
Certificate authority or public key infrastructure-based trust.....	158
Trusting a root CA certificate - “iLO/iLO 3/iLO 4/iLO 5 Default Issuer (do not trust)” certificate.....	159
Using scripts to enable PKI or CA-based trust.....	159
User-verified initial trust.....	159
Automatic initial trust.....	159
Certificates in HPE OneView.....	160
Certificate Revocation Lists.....	161
Certificate status checks.....	162
About certificate validation.....	163
Certificate validation criteria.....	163

Expiry checks for self-signed certificates of devices.....	166
Device-specific certificate handling.....	166
iLO certificates.....	166
Managing servers with iLO configured for two-factor authentication.....	166
Onboard Administrator Certificates.....	167
Enabling and disabling certificate validation.....	167
Appliance Management.....	169
Managing the appliance.....	170
How the appliance handles an unexpected shutdown.....	170
About restoring the appliance.....	171
About the support dump file.....	171
Best practices for restoring an appliance	173
Restore an appliance from a backup file using the HPE OneView GUI.....	174
Scenario: Select a backup file and start the restoration immediately.....	175
Backup and restore the appliance.....	176
Post-restoration tasks.....	177
Appliance maintenance console.....	178
About the appliance maintenance console.....	178
About the appliance maintenance console password.....	180
About the factory reset operation.....	180
Access the appliance maintenance console.....	180
Access the appliance maintenance console through an SSH connection.....	181
Access the appliance maintenance console from the virtual console.....	181
Log in to the appliance maintenance console.....	181
Appliance maintenance console main menu screen details.....	182
Appliance maintenance console details screen details.....	182
Appliance maintenance console appliance states.....	183
Perform a factory reset using the appliance maintenance console	184
Reset the administrator password with the appliance maintenance console.....	185
Reset the appliance maintenance console password.....	186
Restart the appliance using the appliance maintenance console	187
Shut down the appliance using the appliance maintenance console	187
View the appliance details.....	187
Troubleshooting the appliance.....	188
Tasks fail when appliance is in IPv6 mode.....	188
Appliance is offline, unrecoverable error.....	188
Appliance performance is slow.....	188
Appliance rejects your login for HPE OneView.....	189
Cannot log in to HPE OneView after a factory reset action	190
Cannot restart the appliance after a shutdown	191
Browser does not display the HPE OneView user interface.....	191
Login screen is not displayed in HPE OneView.....	192
Reinstall the remote console for proper iLO operation.....	193
Restore action was unsuccessful for HPE OneView	193
Managing and Monitoring in HPE OneView.....	195

HPE OneView Remote Technician	196
Websites.....	197
HPE OneView product feedback.....	198
Support and other resources.....	199
Accessing Hewlett Packard Enterprise Support.....	199
Accessing updates.....	199
Customer self repair.....	200
Remote support.....	200
Warranty information.....	200
Regulatory information.....	201
Documentation feedback.....	201
 Install and configure a web-based external firmware repository on Microsoft	
Windows.....	202
Install IIS Web Server on Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012.....	202
Install IIS Manager on Windows 8 and Windows 10.....	203
Open IIS Manager.....	203
Configure IIS web server on Windows.....	203
Configure Authentication.....	204
Install and enable WebDAV.....	205
Set up HTTPS Binding.....	206
Set up MIME type.....	207
Configure size header.....	207
 Install and configure a web-based external firmware repository on Linux.....	208
Configure Apache web server on Linux.....	208
Configure HTTPS using OpenSSL.....	208
Enable WebDAV and set up Basic Authentication.....	210

Learning about HPE OneView

This part describes HPE OneView and its model for data center resources and introduces you to the terms and concepts used in this document and the appliance online help.

HPE OneView Highlights

Designed for converged infrastructure environments, HPE OneView is a single integrated platform, packaged as an appliance that implements a software-defined approach to managing your physical infrastructure through its entire life cycle. To learn more about HPE OneView, start with the [introduction](#) or select a topic from the following list.

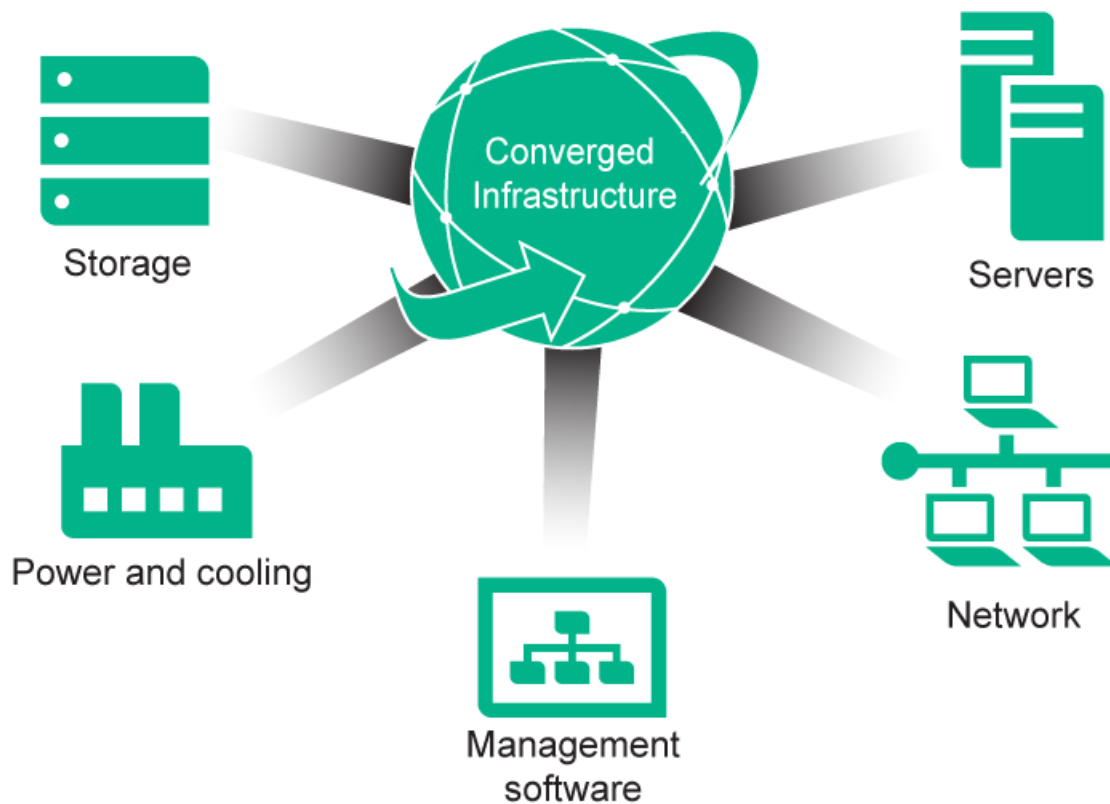
- [HPE OneView licensing](#) on page 12
- [Managing, monitoring, or migrating server hardware on enclosures](#) on page 14
- [Provisioning features](#) on page 14
- [Firmware and configuration change management features](#) on page 21
- [Hypervisor cluster import and management](#)
- [Networking features](#) on page 22
- [Monitoring the environment and responding to issues](#) on page 23
- [Backup and restore features](#) on page 25
- [Security features](#) on page 26
- [High availability features](#) on page 27
- [Graphical and programmatic interfaces](#) on page 27
- [Integration with other management software](#) on page 28
- [Open integration](#) on page 29
- [Smart Update Tools features](#) on page 30

HPE OneView for infrastructure management

Optimized for collaboration, productivity, and reliability, HPE OneView is designed to provide simple, single-pane-of-glass lifecycle management for the complex aspects of enterprise IT—servers, networking, software, power and cooling, and storage.

HPE OneView makes it possible to easily monitor, configure, and manage physical and logical server, network, and storage resources through either a graphical user interface or by using REST (REpresentational State Transfer) APIs.

HPE OneView is designed to manage your converged infrastructure and support key scenarios such as deploying bare-metal servers, deploying hypervisor clusters from bare metal, performing ongoing hardware maintenance, and responding to alerts and outages. It is designed for the physical infrastructure needed to support virtualization, cloud computing, big data, and mixed computing environments.



HPE OneView is delivered as a virtual appliance, a pre-configured virtual machine ready to be deployed on a hypervisor host.

HPE OneView is a scalable, resource-oriented solution focused on the entire life cycle—from initial configuration to on-going monitoring and maintenance—of both physical and logical resources:

- Physical resources are objects you can touch, such as server hardware, interconnects, top-of-rack switches, enclosures, storage systems and racks.
- Logical resources are virtual objects such as templates or groups that when applied to physical resources, provide a common structure across your data center. For example, server profile templates, logical interconnect groups, enclosure groups, server profiles, and volume templates are logical resources.

Software-defined flexibility—your experts design configurations for efficient and consistent deployment

HPE OneView provides several software-defined resources, such as server profile templates, to enable you to capture the best practices of your experts across a variety of disciplines, including networking, storage, hardware configuration, and operating system build and configuration. By having your experts define server profile templates and the networking groups and resources, you can eliminate cross-silo disconnects. By using SBAC (scope-based access control) and the groups, sets, and server profile templates established by your experts, you can enable system administrators to provision and manage hundreds of servers without requiring that your experts be involved with every server deployment.

HPE OneView combines complex and interdependent data center provisioning and management into one simplified and unified interface. You can:

- **Provision the data center**
- **Manage and maintain firmware and configuration changes**
- **Monitor the environment and respond to issues**

The solution also provides core enterprise management capabilities, including:

- **Security features**
- **High availability features**
- **Graphical and programmatic interfaces**
- **Remote support**

HPE OneView manages servers and enclosure networking resources, supports connections from enclosures to storage, and provides information to help you manage data center power and cooling:

- Servers are represented and managed through **server profiles and server profile templates**.
- **Networking** is an essential component to provisioning and managing data center servers.
- **Management software** is integrated with HPE OneView for seamless operation.
- **Environmental management**—such as power, cooling, and space planning—requires that you consider all the equipment in the entire data center, including equipment not managed by HPE OneView. HPE OneView consolidates data center power and cooling information into one interactive view.
- **Storage provisioning and management** with automated zoning is available. Storage devices connect to the enclosures using the following:
 - Fibre Channel fabric attach (SAN switch) connections
 - Fibre Channel over Ethernet (FCoE) fabric attach (SAN switch) connections
 - Fibre Channel direct attach (flat SAN) connections
 - iSCSI connections

HPE OneView licensing

HPE OneView supports the following license types:

- *HPE OneView Standard*

A free license that enables monitoring of supported HPE hardware.

- *HPE OneView Advanced*

A license that enables all HPE OneView management features for supported HPE hardware.

There are two types of *HPE OneView Advanced* licenses:

- *HPE OneView Advanced w/o iLO*

For server hardware that has an existing *iLO Advanced* license, or that does not require the features enabled by *iLO Advanced*.

- *HPE OneView Advanced with iLO Advanced*

Includes an *iLO Advanced* license for the server hardware, which enables advanced management features.

NOTE: For server hardware that is licensed with an *iLO Advanced Premium Security Edition* license, note the following:

- You cannot purchase an HPE OneView license that includes the *iLO Advanced Premium Security Edition* license, you must purchase it separately.
- Use only an *HPE OneView Advanced w/o iLO* license; you cannot apply an *HPE OneView Advanced with iLO Advanced* license to server hardware that has the *iLO Advanced Premium Security Edition* license.
- HPE OneView will not overwrite an *iLO Advanced Premium Security Edition* license with an *iLO Advanced* license.
 - HPE Composable Rack features are licensed separately from the HPE OneView Advanced license. The HPE Composable Cloud for ProLiant DL software license and features are provided with the HPE Composable Cloud for ProLiant DL server license.

HPE OneView Standard licensing delivers monitoring, inventory management, and reporting for HPE BladeSystem and ProLiant BL, DL, XL, and ML servers. HPE OneView Advanced licensing delivers all supported HPE OneView features. The following table provides an overview of the features available for each license type.

Features	HPE OneView Standard	HPE OneView Advanced
Partner integrations		√
Software-defined infrastructure (profiles, groups, sets, and others)		√
Storage provisioning and SAN zoning		√
Virtual Connect advanced management		√
Firmware management		√
Power management (3D visualization)		√
OS provisioning		√
Remote management (HPE iLO Advanced)		√
Map view	√	√
Smart search, Activity view, and Dashboard	√	√
Health monitoring	√	√
Inventory	√	√
Reporting	√	√
REST API access	√	√

Table Continued

Features	HPE OneView Standard	HPE OneView Advanced
Remote Support	√	√
Technical support and software updates	1-year 9x5 support (optional)	3-years 24x7 support (included)

More information

- **Managing, monitoring, or migrating server hardware on enclosures** on page 14
- "About licensing" in the online help

Managing, monitoring, or migrating server hardware on enclosures

Server hardware such as enclosures and rack mount servers, can be added to HPE OneView in one of the following ways, depending on the enclosure type.

An HPE BladeSystem c7000 enclosure is added into HPE OneView as a **Managed**, **Monitored**, or **Migrated** enclosure. An HPE Integrity Superdome X enclosure is added into HPE OneView as a **Monitored** enclosure.

Managed

If you add a managed server to HPE OneView, either in an enclosure or rack server, you can apply configurations, deploy server profiles, monitor operation status, collect statistics, and alert users to specific conditions. For more information, see "About managed c7000 enclosures" in the online help. Managing server hardware requires HPE OneView Advanced licensing.

Monitored

If you add a monitored server to HPE OneView, either in an enclosure or rack server, you can monitor it for inventory and hardware status only. For more information, see "About monitored enclosures" in the online help. Monitoring server hardware uses a free license called HPE OneView Standard.

Migrated

Enclosures from Virtual Connect Manager (VCM) and Virtual Connect Enterprise Manager (VCEM) can be migrated to HPE OneView with the configuration information, so that the enclosure can be managed by HPE OneView. The managed enclosure requires HPE OneView Advanced licensing. For more information about migrating, see "About migrating c7000 enclosures managed by other management systems" in the online help.

Provisioning features

After you install the HPE OneView appliance and perform the initial configuration tasks, you can quickly bring existing hardware under management, and prepare for and deploy hardware to your data center.

Features for provisioning hardware and bringing resources under management include:

- **Resource templates, groups, and sets**
- **Server profiles and server profile templates**
- **Streamlined process for bringing hardware under management**
- **Operating system deployment**
- **Storage provisioning and management**

Resource templates, groups, and sets

With the HPE OneView template-driven approach, you can:

- Use your experts to define server and networking configurations for specific environments.
- Provision hundreds of servers quickly and consistently without requiring that your experts take action for every server you deploy.
- Simplify the distribution of configuration changes across your data center.

Resource templates and groups

The following resources are templates your experts define to meet various workload demands. These templates can then be applied over and over again to the physical resources ensuring quick and consistent configurations.

Template or group	Description
Enclosure group	<p>A template that defines a consistent configuration for an enclosure. An enclosure group specifies the placement of the various interconnects and the logical interconnect groups that apply to those interconnects.</p> <p>When an enclosure group is applied to a physical enclosure, HPE OneView creates a logical enclosure which is then ready to perform work. The same enclosure group can be applied to many physical enclosures to create many identically configured logical enclosures.</p>
Logical interconnect group	<p>A template that defines the desired networking configuration of a physical interconnect or set of interconnects. Logical interconnect groups are used when defining enclosure groups and represent the networking template of that enclosure group.</p> <p>When an enclosure group is applied to a physical enclosure, HPE OneView:</p> <ul style="list-style-type: none">• Creates a logical enclosure• Uses the logical interconnect groups in that enclosure group to configure the physical interconnects in that enclosure into logical interconnects.
Logical switch group	<p>A template that defines how physical switches are combined to form logical switches. Logical switches are an aggregation of up to two physical top-of-rack switches.</p> <p>Once constructed from a logical switch group, a logical switch continues to be associated with its logical switch group. Any change in consistency between the logical switch group and its associated logical switches is monitored and made visible on the associated logical switch screen in HPE OneView.</p>
Server profile templates	<p>A template that defines the characteristics of a server profile. A server profile template can be applied to multiple servers creating identically configured servers. A server profile can be updated to match any server profile template.</p>
Volume templates	<p>A template that defines a standard configuration for storage volumes.</p>

Logical resources

The following logical resources represent the physical, software-defined resources configured to work as needed in your environment. These resources actually run the workloads.

Resource	Description
Logical enclosure	<p>A logical enclosure represents a logical view of a single enclosure with an enclosure group serving as a template. By default, when you add a c7000 enclosure, an enclosure group and logical interconnect group are created. Or, you can create multiple logical interconnect groups and an enclosure group before you add the enclosure.</p> <p>A logical enclosure is automatically created when a c7000 enclosure is added.</p>
Logical interconnect	<p>A logical interconnect is a single administrative entity that consists of the configuration for a set of physical interconnects in a single enclosure. A logical interconnect represents the available networks, uplink sets, internal networks, and stacking links for the physical interconnects.</p>
Logical switch	<p>A logical switch can consist of a maximum of two physical top-of-rack switches (external to a c7000 enclosure) configured in a single stacking domain.</p> <p>A logical switch when part of a Composable Fabric, allows HPE OneView to deploy server profile connections to rack mount servers that are connected to this logical switch.</p> <p>When not part of a Composable Fabric, you can create a logical switch as either monitored or managed:</p> <ul style="list-style-type: none"> • Creating a logical switch as monitored enables HPE OneView to: <ul style="list-style-type: none"> ◦ monitor the operation status ◦ provide physical switch ◦ provide information about the physical port information and port statistics ◦ provides health events and changes in the port state ◦ provides information about network availability between the enclosure edge and upstream ToR switches <p>In monitored mode, deployment of the server profile connections are supported only for Virtual Connect interconnects.</p> <ul style="list-style-type: none"> • Creating a logical switch as managed enables HPE OneView to provide full control of the port state and network provisioning for the ports between the enclosure edge and upstream ToR switches. When adding a logical switch in a managed mode, any existing configuration for ports connected to HPE OneView managed interconnects is replaced with the configuration specified for the HPE OneView interconnect uplinks. Any port that is actively managed by an external management system remains unchanged and is not brought into HPE OneView management.
Server profile	<p>A server profile represents a physical server that has been fully configured to perform its desired function. The server profile specifies all of the storage, networking, firmware, and server settings required by the server workload. A server profile is built on all of the other logical resources in HPE OneView.</p>

Table Continued

Resource	Description
Storage pool	<p>A storage pool is an aggregation of physical storage resources (disks) in a storage system. Storage systems contain information about the storage ports through which they can be accessed. You can provision logical storage spaces, known as volumes, from storage pools.</p> <p>Storage pools are created on a storage system using the management software for that system. You cannot create or delete storage pools from the appliance-you can only add or remove them from management.</p>
Volume	A volume is a logical storage space provisioned from a storage pool on a storage system.

Define configurations for specific environments

Groups and templates enable you to define configurations that are specific to the environment you want to build, such as virtual hosts, Microsoft Exchange environments, external or internal web servers, or corporate database servers.

For example, to build multiple external web servers:

1. Your networking expert can create logical interconnect groups, uplink sets, networks, and network sets to establish all of the connection policies between data center networks and the interconnects managed by the appliance.
2. Your server expert can create enclosure groups, add enclosures, create logical enclosures, and create server profile templates to establish all of the settings required by an external web server.
3. Your server administrators can use the server profile templates whenever they need to deploy this type of server.
4. Your storage expert can add SAN managers and storage systems, and define storage pools and volume templates.

Flexibility in design and deployment

HPE OneView provides flexibility in the creation of groups, templates, and sets. For example, you can create a logical interconnect group in these ways:

- Before you add an enclosure to the appliance to be managed, you can create a logical interconnect group or groups specifying how you want the interconnects to be configured, and an enclosure group that specifies how you want the enclosure to be configured. Then, when you add the enclosure, you can specify the enclosure group you already created.
- You can add an enclosure to the appliance to be managed and, after the appliance discovers and adds the interconnect hardware in the enclosure, you can use or modify the default logical interconnect group that the appliance creates.
- You can migrate a Virtual Connect domain into HPE OneView which creates logical interconnect groups.
- Copy an existing logical interconnect group to create a new logical interconnect group.

Groups, templates, and sets **also simplify the distribution of configuration changes** within the appliance.

Server profiles and server profile templates

Server profiles and server profile templates enable you to provision hardware quickly and consistently according to your best practices. Store your best practice configuration in a server profile template and then use the server profile template to create and deploy server profiles. You can also create a server profile template from an existing server profile.

A server profile captures key aspects of a server configuration in one place, including:

- Firmware update selection and scheduling
- BIOS settings
- iLO settings
- Local RAID configuration
- Network connectivity
- Boot order configuration
- Local storage and SAN storage
- Unique IDs

As long as similar hardware has been discovered, server profiles enable your experts to specify a server configuration before the server arrives. When the server hardware is installed, your administrators can quickly bring the new server under management.

For example, you can create an unassigned server profile from a template that specifies all the configuration aspects—such as BIOS settings, network connections, and boot order—to use for a type of server hardware. Before the server is installed in an enclosure bay, you can do one of the following:

- Assign the server profile at the time of creation to an empty bay in an enclosure where the server will eventually reside.
- Create an unassigned profile and assign it once the hardware arrives.

You can move a server profile from the currently assigned server hardware to another server hardware of the same type. When you move the server profile to another server hardware, the profile configuration is applied to the newly assigned server hardware.

If the server types match, you can copy the server profile to a different server. There are no restrictions on servers being in upper or in lower bays. If the profile is moved to a server in a different enclosure, it will fail.

NOTE: HPE OneView does not support moving a profile with JBODs to a different enclosure.

You can create server profile connections without assigning networks for preprovisioning and migration.

You can control the server profile behavior. For example, you can assign a server profile to an empty bay and when an appropriate server is inserted into that bay, the server profile is automatically applied to the server hardware. The server profile can also be associated with a specific server to ensure that the profile is not applied if the wrong type of server is accidentally inserted into the bay.

Streamlined process for bringing hardware under management

HPE OneView simplifies the process of bringing the enclosures, interconnects, and server hardware under management.

For example:

- When you **add** an enclosure, the appliance automatically detects all of the hardware seated in the enclosure and brings it under management. For example, the appliance:
 - Updates the enclosure Onboard Administrator, Virtual Connect interconnect modules, and server iLO firmware to the minimum version required (if a firmware bundle is uploaded to the appliance).
 - Configures each Virtual Connect interconnect module, removing the existing VC configuration. To keep the existing VC configuration, migrate the enclosure.

- Configures the Onboard Administrator, which includes configuring NTP (Network Time Protocol) and configuring an SSO (single sign-on) certificate for UI access.
- Configures each server iLO, which includes configuring an SSO certificate for UI access.
- Configures the hardware for monitoring, which includes configuring SNMP (Simple Network Management Protocol) traps.
- When you **migrate** a VCM-managed enclosure, the appliance automatically validates the configuration information (including hardware, Virtual Connect domain, networks, and server profiles) before importing the enclosure. During the migration, the configuration information is moved into HPE OneView.
- When you add an HPE Intelligent Power Distribution Unit (iPDU) power device, the appliance automatically detects and presents the connected devices so that you can bring the devices under management.

Operating system deployment

Server profiles and enclosure groups make it easier to prepare a bare-metal server for operating system deployment.

For example, you can use server profiles in conjunction with deployment tools such as:

- HPE Insight Control server provisioning to install an operating system on the server.

NOTE: HPE Insight Control server provisioning supports provisioning on HPE ProLiant G7, Gen8, and Gen9 servers. For Gen10 ProLiant servers, HPE recommends to use tools like VMware AutoDeploy.

- HPE OneView for VMware vCenter Auto Deploy to deploy hypervisors from bare metal and add them to existing clusters automatically.

Storage provisioning and management

HPE OneView provides automated, policy-driven provisioning of supported storage resources. It is fully integrated with server profiles so that you can manage your new or existing storage infrastructure. With HPE OneView, you can view and manage your storage system and storage pools. You can add existing volumes and create volumes, and then you can create volume templates to provision multiple volumes with the same configuration.

Switched fabric, direct attach, vSAN SAN topologies, as well as iSCSI connections are supported. You can also add SAN managers to make their managed SANs available to the appliance.

Storage system and storage pools are added to the appliance followed by volumes, which are associated with networks. The volumes can then be attached to server profiles.

To enable automated zoning and automatic detection of connectivity, the SANs can be associated with any of the following network connection protocols:

- Fibre Channel fabric attach (SAN switch)
- Fibre Channel direct attach (flat SAN)
- Fibre Channel over Ethernet (FCoE)
- Internet Small Computer System Interface (iSCSI)

Supported storage automation features

Automated storage provisioning

When you import supported storage systems and existing storage pools, HPE OneView can quickly create volumes.

Automatic SAN zoning

HPE OneView automatically manages SAN zoning through server profile volume attachments.

Storage integration through server profiles

Create and make new private volumes accessible to the server hardware by adding volume attachments to the server profile.

Make existing private or shared volumes accessible to server hardware by adding volume attachments to the server profile.

HPE OneView tracks the connection status between server profiles and SANs.

A boot from SAN (BFS) configuration, specified in a server profile or server profile template, enables the primary/secondary assignment and storage system target port selection to be load balanced uniformly over SANs and storage system targets.

Volume management

You can use HPE OneView to manage the full life cycle of your volumes. You can add existing volumes, create volumes, grow volumes, and remove or delete volumes using HPE OneView.

You can use volume templates to define a standard configuration for storage volumes. Volume templates also enable you to choose which configuration settings are locked, making them unable to be changed on volumes created from the volume template.

Volume settings can be managed in volume templates, volumes, server profiles, and server profile templates.

With HPE 3PAR StoreServ, you can also create volume snapshots, create a volume from a snapshot, and revert a volume to a snapshot using HPE OneView.

Zoning policies

HPE OneView enables you to set a zoning policy for your managed SANs. You can choose single initiator/all targets, single initiator/single storage system, or single initiator/single target.

Zone naming and aliases

HPE OneView uses rules-based zone naming to give you full control of your zone names. You can use zone naming to incorporate your current naming structure, which HPE OneView uses during the automated zoning process.

HPE OneView enables you to create aliases for initiators, targets, and target groups in place of their WWPNs.

About HPE Nimble storage systems

A Nimble storage system consists of a group of one to four storage arrays. Each array has a pair of controllers -- an active controller and a standby controller.

A storage pool is configured for each array. HPE OneView does not recommend configuring storage ports for multiple arrays. Each controller typically has 4 to 12 ports, and storage volumes are made available to all the active ports. Failover occurs at the controller level and not at the individual port level.

iSCSI discovery and data access IP addresses are not tied to a specific controller or port. For Fibre Channel access, a SAN zone or a network should be configured for at least 1 port on each active controller and standby controller for proper redundancy in case of controller failover.

HPE OneView can only provision a single pair of target ports to boot a server. Therefore, Hewlett Packard Enterprise recommends to use only single-array storage system groups when configuring Fibre channel connectivity. A dual array storage system group that requires 4 target ports for proper failover redundancy cannot properly support boot volumes.

While data volume attachment paths can have many target ports configured, typically a Nimble storage system is configured in HPE OneView with the port groups automatically assigned to the minimal set of target ports (1 port on each controller in the storage system group), instead of making all the targets accessible through the path network.

Firmware and configuration change management features

Simplified firmware management

HPE OneView provides fast, reliable, and simple firmware management across the appliance.

When you add a resource for the appliance to manage, the appliance automatically updates the resource firmware to the minimum version required by the appliance. A firmware bundle must be uploaded to the appliance for the automation to occur.

NOTE:

- Firmware for monitored resources is not managed by HPE OneView.
- To manage firmware for rack managers (HPE Superdome Flex Server), see the “Rack Managers” topics in the online help.

A firmware bundle, also known as an SPP (Service Pack for ProLiant), is a tested update package of firmware, drivers, and utilities. Firmware bundles enable you to update firmware on managed servers and infrastructure (enclosures and interconnects).

An on-appliance firmware repository enables you to upload SPP firmware bundles and deploy them across your environment according to your best practices. For example, you can:

- View the versions and contents of firmware bundles stored in the firmware repository.
- View the version of firmware installed on supported hardware from the **Server Hardware** page.
- Set a firmware baseline—required state for firmware versions—on a managed resource, such as a server profile, or on a group of resources, such as all the interconnects in a logical interconnect.
- Detect when a managed resource does not comply with the firmware baseline.
- Report on firmware compatibility.
- Update firmware for an entire logical enclosure.
- Update firmware for individual resources or for groups of resources, such as logical interconnects.¹
- Update OS drivers and firmware.
- Remove a firmware bundle from the repository.
- Increase the size of the virtual disk for the SPP repository.

An additional externally managed HTTP/HTTPS web server can be added to the appliance as an external repository. It is a user-maintained HTTP/HTTPS web server. You can upload firmware bundles in a specific directory and then register the HTTP/HTTPS server with HPE OneView. This functionality is supported for WEBDAV-enabled web servers such as Apache HTTPD and IIS.

Hypervisor clusters are updated nondisruptively for VMware ESXi systems, when the orchestrated activation option is chosen. If the logical enclosure contains one or more hypervisor profiles, each hypervisor is serially placed into a maintenance mode before updating. It can take up to 90 minutes to place a hypervisor into the maintenance mode, perform the firmware update, and take it back out of the maintenance mode.

Hewlett Packard Enterprise occasionally releases component hotfixes between main SPP releases. Hewlett Packard Enterprise notifies you that a hotfix is available to upload and provides details about the SPP to which the hotfix applies. There are different ways to apply a hotfix in HPE OneView.

¹ Enclosure groups do not include a firmware baseline. Therefore, updates to enclosure firmware are managed through a logical enclosure configuration.

More information

- [Install and configure a web-based external firmware repository on Microsoft Windows](#)
- [Install and configure HTTPS web server on Linux](#)

Simplified configuration change management

Templates and groups simplify the distribution of configuration changes across the appliance. For example:

- Simplify multiple and complex changes by making one change to a group or template. Then, for each member of the group, you can use a single action to update the configuration to match the configuration of the group.
- The appliance notifies you when it detects that a resource does not comply with the current template or group. You control when and if a resource configuration is updated.
- The logical interconnect settings manage the firmware for physical interconnects to ensure that all interconnects within the logical enclosure have compatible firmware.

Hypervisor cluster import and management

HPE OneView provides the ability to import cluster of hypervisors running on the servers that share the workload and manage them. You can manage the hypervisors that are running on the servers, which support HPE Virtual Connect and are managed by HPE OneView. It leverages hypervisor manager software to configure hypervisors, or to query hypervisor configurations. The hypervisor cluster profile enables you to define and maintain consistent configuration from server nodes to hypervisors in the cluster.

Using hypervisor cluster profile, you can import a hypervisor cluster and manage this cluster. You can manage life-cycle operations such as grow or shrink the hypervisor cluster, modify configurations, perform consistency checks, rolling updates, and conduct non-disruptive firmware updates on server nodes.

The hypervisor cluster profile uses a server profile template as a base to define the configuration settings for server nodes and hypervisors in the cluster. You can configure the following settings in the hypervisor cluster profile:

- OS deployment settings
- Hypervisor settings
- Networking
- Storage
- Hypervisors

Hypervisor resources

- [Hypervisor Manager](#)
- [Hypervisor Cluster Profile](#)
- [Hypervisor Profile](#)

Networking features

HPE OneView provides several networking features to streamline the provisioning of networking resources for server hardware and to manage configuration changes, including firmware updates, to Virtual Connect interconnect modules.

Supported networks

The Virtual Connect interconnect modules in enclosures support the following types of data center networks:

- Ethernet for data networks, including tagged, untagged, or tunnel networks.
- Fibre Channel for storage networks, including Fibre Channel fabric attach (SAN switch) connections, and Fibre Channel direct attach (Flat SAN) connections from FlexFabric interconnect modules to supported 3PAR storage systems.
- Fibre Channel over Ethernet (FCoE) for storage networks where storage traffic is carried over a dedicated Ethernet VLAN.

Additional networking resources

- **Logical interconnects** on page 40
- **Logical interconnect groups** on page 41
- **Logical switches** on page 42
- **Logical switch groups** on page 43
- **Network sets** on page 44
- **Switches** on page 51

HPE OneView's networking resources support functionality such as Smart Link, Link Layer Discovery Protocol (LLDP) tagging, Link Aggregation Control Protocol (LACP), loop and pause flood protection, and Simple Network Management Protocol (SNMPv3) trap monitoring.

Monitoring the environment and responding to issues

One user interface

You use the same interface for monitoring that you use to provision resources. There are no additional tools or interfaces to learn.

Isolated management network

The appliance architecture is designed to separate the management traffic from the production network, which increases reliability and security of the overall solution. For example, your data center resources remain operational even in the unlikely event of an appliance outage.

Automatic configuration for monitoring health and utilization

When you add resources to the appliance, they are automatically configured for monitoring health, activity, alerts, and utilization. You can monitor resources immediately without performing additional configuration or discovery steps.

Agentless and out-of-band management

All health and utilization monitoring and management of HPE ProLiant Gen8 (or later) servers is agentless and out-of-band for increased security and reliability. For these servers:

- There are no agents to monitor or update.
- The appliance does not require open SNMP ports on the host operating system.
- The appliance does not interact with the operating system on the host, which frees memory and processor resources on the host for use by server applications, and enables you to monitor servers that have no host operating system installed.

Management from other platforms using the REST APIs and message buses

The REST APIs and the SCMB (State-Change Message Bus) or MSMB (Metric Streaming Message Bus) also enable you to monitor the HPE OneView environment from other management platforms.

Monitoring the environment and responding to issues

Features for monitoring the environment and responding to issues include the following:

- The Dashboard screen details, which displays a summary view of data center capacity and health information.
- The Activity screen, which displays and enables you to filter all system tasks and alerts.
- **Activity and health management**
- **Data center environmental management**
- **Resource utilization monitoring**
- **Hardware and firmware inventory information**

Data center environmental management

HPE OneView integrates these critical areas for environmental management of the data center:

Feature	Description
Thermal data visualization	3D data center thermal mapping provides a view of the thermal status of your entire data center. The appliance collects thermal data from the managed resources in each data center rack and presents the data graphically, enabling easy identification of hot spots in a rack.
Power delivery infrastructure representation	<p>HPE OneView collects and reports processor utilization and power and temperature history for your data center hardware. The appliance monitors power, automatically detects and reports power delivery errors, and provides precise power requirement information for HPE ProLiant Gen8 (or later) servers and enclosures that you can use for planning rack and power usage.</p> <p>Power Discovery Services enable automatic discovery and visualization of the power delivery topology for your data center. HPE iPDUs enable the appliance to map the rack power topology automatically. The appliance detects wiring errors—such as lack of redundancy—and updates electrical inventory automatically when new servers are installed. The appliance also supports per-outlet power control for remote power cycling of each iPDU outlet.</p> <p>You can manually define the power requirements and power topology for devices that do not support Power Discovery Services.</p>
Physical asset location	<p>Location Discovery Services enable the appliance to automatically display the exact 3D location of HPE ProLiant Gen8 and Gen9 servers in Intelligent Series Racks, reducing labor time, lowering operational costs, and eliminating human errors associated with inventory and asset management.</p> <hr/> <p>NOTE: HPE ProLiant Gen10 servers do not support Location Discovery Services.</p> <hr/> <p>You can manually define the positions of racks and devices that do not support Location Discovery Services.</p>

Resource utilization monitoring

HPE OneView periodically collects and maintains CPU utilization information for all of the servers it manages. HPE OneView also collects port-level statistics for networking, including transmit, receive, and error counters. HPE OneView displays all of this data in the UI and makes the data available through the REST APIs.

Activity and health management

HPE OneView provides streamlined activity monitoring and management. The appliance automatically registers alerts and notifications from all managed resources, and resources added to the appliance are immediately available for monitoring and management. When the appliance notifies you of a problem, when possible, it suggests a way to correct the problem.

Using the UI and REST APIs, you can:

- View all activities (alerts and tasks) by description or source, and filter activities using multiple filter criteria.
- Assign alerts to specific users.
- Annotate activities with notes from administrators, enabling the administrators of the data center to collaborate through the appliance instead of through outside tools such as email.
- View alerts for a specific resource from the UI screen for that resource or using the REST API for that resource.
- Automatically forward SNMP traps from managed resources to enterprise monitoring consoles or centralized SNMP trap collectors.

Hardware, firmware, and driver inventory information

HPE OneView provides detailed hardware and firmware inventory information about the resources it manages. You can access the following data through the user interface (UI) and the REST APIs:

- Summary and detailed views of managed hardware, such as servers, enclosures, and interconnects.
- Summary of monitored hardware, such as servers and enclosures.
- Summary and detailed views of firmware bundle contents.
- Firmware inventory for server and enclosure components.
- Driver inventory for Gen8, Gen9, and Gen10 servers.

NOTE: Agentless Management Service (AMS) must be installed to get the complete driver inventory of the server.

You can use the Smart Search feature of the UI to find specific items in the inventory.

Reports are available to help you monitor your inventory as well as help you monitor your environment. The inventory reports provide information about your servers or enclosures such as model, serial number, part number, and so on. Other reports provide a picture of the overall status of your environment.

Remote Support

HPE OneView provides remote support as part of the contract or warranty of a user to allow automatic case creation for hardware failures on servers, enclosures, and interconnects to enable proactive services (for example, Proactive care and Datacenter care). Once enabled, all eligible devices added in future will be automatically enabled for remote support.

HPE will contact you to ship a replacement part or send an engineer to either repair or replace devices that are under warranty or support contract. Remote support includes contract and warranty information, and expiry alerts to help customers keep track of their contacts.

Remote support enables proactive services including proactive scan reports and Firmware/Software Analysis reports with recommendations that are based on collected configuration data.

Backup and restore features

HPE OneView provides services to back up an appliance to a file, and to restore an appliance from a backup file. Backups can be scheduled to occur automatically and stored remotely.

One proprietary backup file for both the appliance and its database

Backup files are proprietary and contain configuration settings and management data—there is no need to create separate backup files for the appliance and its database.

Hewlett Packard Enterprise does not recommend using VM snapshots to protect the appliance. Synchronization errors can occur and result in unpredictable and unwanted behavior.

Flexible scheduling and an open interface for backup operations

You can create or schedule backup files while the appliance is online. Also, you can use REST APIs to:

- Schedule a backup process from outside the appliance.
- Collect backup files according to your site policies.
- Integrate with enterprise backup and restore products.
- Utilize the backup and restore scripts.

A backup file is a snapshot of the appliance configuration and management data at the time the backup file was created. Hewlett Packard Enterprise recommends that you create regular backups, preferably once a day and after you make hardware or software configuration changes in the managed environment.

NOTE: For added security, ensure that you always encrypt your backup files.

Specialized user role for creating backup files


HPE OneView provides a user role, a Backup administrator, specifically for backing up the appliance by permitting access to other resource views without permitting actions on those resources, or other tasks.

Recovery from catastrophic failures

You can recover from a catastrophic failure by restoring your appliance from the backup file.

When you restore an appliance from a backup file, all management data and most configuration settings on the appliance are replaced with the data and settings in the backup file, including things like user names and passwords, audit logs, and available networks.

The state of the managed environment is likely to be different from the state of that environment at the time the backup file was created. During a restore operation, the appliance reconciles the data in the backup file with the current state of the managed environment. After the restore operation, the appliance uses alerts to report any discrepancies that it cannot resolve automatically.

 **IMPORTANT:** During the restore operation from the maintenance console, the appliance might restart and you might lose access to the console. Reconnect to the maintenance console after 5 minutes to monitor the progress of the restore process.

Security features

To ensure a secure platform for data center management, the appliance includes features such as the following:

- HPE OneView offers options to configure management appliances to be compliant with the Federal Information Processing Standard FIPS-140-2 (FIPS 140-2) and Commercial National Security Algorithm (CNSA) standards, or to continue using the legacy cryptography mode. In the FIPS 140-2 and CNSA mode, the appliance restricts protocol versions, cipher suites, and digital certificate strength to FIPS 140-2 and CNSA compliant ones, respectively.
- Customizable TLS versions - REST API to selectively disable TLS1.0 and/or TLS1.1
- Separation of the data and management environments, which is critical to protect against Denial of Service attacks.

- SBAC (scope-based access control) extends role-based access control by restricting a role to operate only on a subset of resources managed by the appliance. For example, a Server Administrator named Sarah can only manage the servers in the "Production" scope.
- Two-factor authentication to provide authentication using smart cards.
- Certificate management to improve the policies and procedures for managing certificate-based trust.
- Single sign-on to iLO and Onboard Administrator without storing user-created iLO or Onboard Administrator credentials.
- Audit logging for all user actions and forwarding to the remote log servers.
- Support for authentication and authorization using an optional directory service such as Microsoft Active Directory.
- Use of certificates for authentication over Transport Layer Security (TLS).
- An automated remote backup feature that allows you to set the day and time a backup will be performed and the ability to specify a remote SSH or SFTP server to store the backup files automatically.

More information

Understanding the security features of HPE OneView

High availability features


HPE OneView is delivered as a preconfigured virtual appliance ready to be deployed on a hypervisor host as a virtual machine. The hypervisor software provides the virtual machine with high-availability and recovery capabilities that allow the virtual machine to be restarted on another host in a cluster and to resume management without disruption to the managed resources.

Tutorial and Guided setup

Tutorial

A tutorial is provided when you first log in to HPE OneView to introduce you to the HPE OneView GUI. This tutorial is also available by clicking **Tutorial** in the Help sidebar. The tutorial shows the location of basic screen functions and briefly describes their purpose.


Guided Setup

A guided setup is available to help you configure your appliance. To open the guided setup introduction, click the **Guided setup** icon . By following the steps in the setup guide, you will be able to configure your appliance. You can get started with the first step or select to view the list of steps involved.

Graphical and programmatic interfaces

HPE OneView was developed to use a single, consistent resource model embodied in a user interface and industry-standard REST APIs for mobile, secure access, and open integration with other management software.

Global views

Feature	Description
Dashboard screen	Provides a graphical representation of the general health and capacity of the resources in your data center. From the Dashboard you can immediately see the areas that need your attention.
Smart Search box	The banner of every screen includes the Smart Search feature, which enables you to find resource-specific information such as specific instances of resource names, serial numbers, WWNs, and IP and MAC addresses.
Activity  sidebar	The Activity sidebar shows tasks initiated during the current session, with the most recent task displayed first. The Activity sidebar and Activity view simplifies the correlation of user activity with system health, allowing for timely resolution of issues.

Resource-specific views

Resource-specific management screens enable you to focus on the resources you are authorized to view and manage. Resource group screens enhance scalability by enabling you to manage multiple resources as one. The following resource-specific views are available from each resource.

Feature	Description
Activity view	The Activity view gives you a unique perspective into the health of your resources by interleaving the tasks, alerts, and administrator notes into a single view for those resources.
Map view	The Map view enables you to examine the configuration and understand the relationships between logical and physical resources in your data center.
Scopes view	The Scopes view enables you to restrict the resources before performing an operation or action. The resources are arranged by categories. All the resources in these categories can be added to or removed from a scope, including enclosures, server hardware, networks, network sets, interconnects, switches, logical switches, logical switch groups, logical interconnects, and logical interconnect groups.
Labels view	The Labels view enables you to organize resources into groups. For example, you might want to identify the servers that are used primarily by the Finance team, or identify the storage systems assigned to the Asia/Pacific division.

Integration with other management software

For a list of management software integrated with HPE OneView, see <https://www.hpe.com/us/en/software/licensing.html>. To use the integrated management software, you must purchase HPE OneView Advanced licenses.

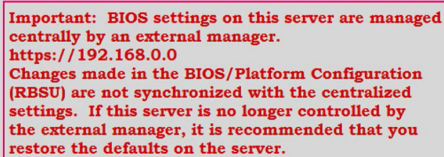
Other management software warnings

Do not use external managers, such as HPE Systems Insight Manager (SIM) or third-party management software, to manage hardware that is under management using HPE OneView. Using another external manager can cause errors and unexpected behavior. For example: iLO has a maximum of three trap destinations, one of which is HPE OneView. If external managers define additional trap destinations, iLO removes one of the existing trap destinations. If HPE OneView is the trap destination iLO removes, HPE OneView will no longer receive SNMP traps and will not display server health or lifecycle alerts.

NOTE: Third-party tools do not provide any warning if they make or require configuration changes to the server. Use caution when using these tools.

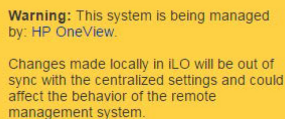
- If you attempt to change a resource managed by HPE OneView with other HPE management tools such as RBSU, a warning message displays.
- If you attempt to make BIOS or iLO changes in Intelligent Provisioning, a warning displays.
- If you attempt to change server firmware using SUM, and the firmware baseline associated with the server profile for that server is not set to Managed manually, SUM displays a warning:

HPE OneView is managing the server and it is configured for Service Pack for ProLiant version x. It cannot be updated to a different version directly using SUM.
- If you attempt to make BIOS changes in RBSU on a server where HPE OneView is managing the BIOS, RBSU displays a warning.



Important: BIOS settings on this server are managed centrally by an external manager.
<https://192.168.0.0>
Changes made in the BIOS/Platform Configuration (RBSU) are not synchronized with the centralized settings. If this server is no longer controlled by the external manager, it is recommended that you restore the defaults on the server.

- If HPE OneView manages the iLO, the iLO login screen displays a warning.



Warning: This system is being managed by: HP OneView.

Changes made locally in iLO will be out of sync with the centralized settings and could affect the behavior of the remote management system.

Open integration

The single, consistent resource model, REST APIs, SCMB (State-Change Message Bus), and MSMB (Metric Streaming Message Bus) enable you to use scripting to integrate HPE OneView with other enterprise applications to address user needs and perform tasks such as:

- Automating standard workflows and troubleshooting steps
- Automating integrations with other software, such as a CMDB (configuration management database)
- Connecting to service desks
- Monitoring resources, collecting data, and mapping and modeling systems
- Exporting data to formats that suit your needs
- Attaching custom databases, data warehouses, or third-party business intelligence tools
- Integrating in-house user customizations

The SCMB is an interface that uses asynchronous messaging to notify subscribers of changes to managed resources—both logical and physical. For example, you can program applications to receive notifications when new server hardware is added to the managed environment or when the health status of physical resources changes—without having to continuously poll the appliance for status using the REST APIs.

Smart Update Tools features

Smart Update Tools (SUT) is an operating system utility used with iLO 4 (Gen8 and Gen9 servers) and iLO 5 (Gen10 servers) for HPE OneView. SUT enables an administrator to perform online firmware and driver updates. SUT polls HPE OneView every five minutes for new requests, processes those requests, and provides HPE OneView with a status. HPE OneView posts the progress in the **Firmware** section of the **Server Profile** page. SUT installs updates in the correct order and ensures that all dependencies are met before starting an update. If there are unmet dependencies, SUT prevents the installation and notifies the HPE OneView administrator that the installation cannot continue due to a dependency.

Smart Update Tools is a generic term used for all variants of SUT. Integrated Smart Update Tools (iSUT) is available for Windows and Linux with Gen8, Gen9, and Gen10 servers. It has to be installed within the managed host OS. Smart Update Tools (SUT) is available for ESXi with Gen8 and Gen9 servers. It is a standalone installation for every instance of HPE OneView.

For more information, see [**HPE OneView Support Matrix**](#).

Key features:

- Combined driver, software, and firmware updates
- Compliance reporting in the HPE OneView dashboard based on the status received from SUT
- An increase in the maximum uptime by minimizing the number of reboot required for activation
- The ability to perform firmware staging and development tasks outside of the actual maintenance window so that one reboot during the maintenance window activates both firmware and driver updates
- Multiple user roles:
 - HPE OneView Software administrator who defines the required state using the firmware options in the server profile
 - SUT administrator who uses SUT to update the firmware and the software on the server
- Manual control and varying levels of automation:
 - On demand or manual updates
 - Semiautomatic when staging is automatic or staging and installation are automatic
 - Scheduled updates
 - Fully automatic update

NOTE: For SUT to function correctly, use iLO 4 firmware version 2.31 or above, or iLO 5 firmware version 1.10 or above. HPE OneView manages the server firmware. HPE OneView automatically updates the iLO firmware, provided an SPP 2016.10.0 or above is available in the HPE OneView repository, and enables SUT to proceed.

Understanding the resource model

HPE OneView uses a resource model that reduces complexity and simplifies the management of your data center. This model provides logical resources, including templates, groups, and sets, that when applied to physical resources, provides a common structure across your data center.

The UI distinguishes between physical and virtual resources by using certain actions. For example:

- You can **create**, **delete**, or copy a logical resource, but not a physical resource.
- You can **add** or **remove** a physical resource.

High-level overview

Resource model summary diagram on page 31

Server resources

- **Server profile templates** on page 49
- **Server profiles** on page 48
- **Connections** on page 33
- **Connection templates** on page 34
- **Server hardware** on page 47
- **Server hardware types** on page 48
- **Rack Managers**

Network provisioning resources

- **Enclosure groups** on page 36
- **Enclosure types** on page 36
- **Enclosures** on page 35
- **Interconnect types** on page 39
- **Interconnects** on page 38
- **Logical enclosures** on page 40
- **Logical interconnect groups** on page 41
- **Logical interconnects** on page 40
- **Logical switches** on page 42
- **Logical switch groups** on page 43
- **Switches** on page 51
- **Uplink sets** on page 52

Network resources

- **Networks** on page 43
- **Network sets** on page 44

Storage resources

- **Storage Systems** on page 51
- **Storage Pools** on page 50
- **Volumes** on page 53
- **Volume Templates** on page 53
- **SAN Managers** on page 46
- **SANs** on page 46

Appliance resources

- **Appliance** on page 32
- **Domains** on page 35

Data center power and cooling management resources

- **Data centers** on page 34
- **Racks** on page 45
- **Power delivery devices** on page 44
- **Unmanaged devices** on page 51

Learn more

- For a complete list of resources, see the *HPE OneView REST API Reference* in the online help.
- For information about using HPE OneView, see the other chapters in this guide and the online help.

Resource model summary diagram

The following figure summarizes some of the most frequently used resources and shows the relationships between them.

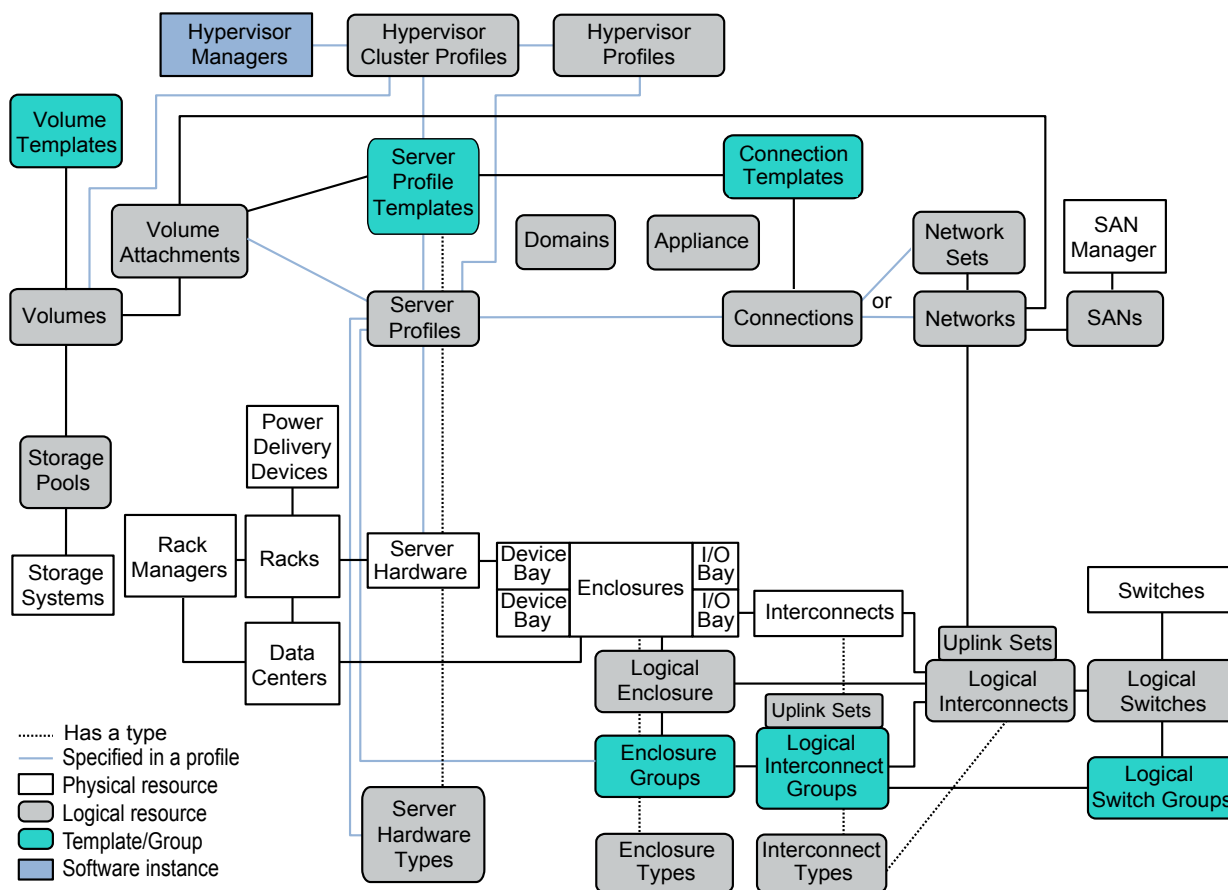


Figure 1: Resource model summary diagram

The UI and REST APIs are organized by resource. The documentation for the UI and REST APIs is also organized by resource.

The complete list of resources are included in the *HPE OneView REST API Reference* in the online help.

The following sections introduce the resources shown in **Resource model summary diagram**.

Appliance

The appliance resource defines configuration details specific to the HPE OneView appliance (as distinct from the resources HPE OneView manages).

Relationship to other resources

An appliance resource is associated with the following resources in the **resource summary diagram**:

- Exactly one **domain**
- Zero or more instances of the other resources in the summary diagram

UI screens and REST API resources

Several REST API resources are related to the appliance and appliance settings. See the resources in the following categories in the *HPE OneView REST API Reference* in the online help:

UI screen	REST API resource
Settings	<ul style="list-style-type: none"> • Appliance time, locale, and timezone settings appliance/configuration/timeconfig/locales appliance/ configuration/time-locale • Appliance device READ community string appliance/device-read-community-string • Reset the appliance to the factory defaults appliance • Upgrade or patch the appliance firmware appliance/firmware • Health of appliance components appliance/health-status • Configure and retrieve network information of the appliance appliance/network-interfaces • Shut down or restart an appliance appliance/shutdown • Generating and downloading support dumps from an appliance appliance/support-dumps • Trap destinations in the management appliance appliance/trap-destinations
OneView License	Status of the End User License Agreement (EULA) and related data appliance/eula

Connections

A connection is the logical representation of a connection between a server and a network or network set. Connections can be configured in server profiles. A connection specifies the following:

- The network or network set to which the server is to be connected
- Configuration overrides (such as a change to the preferred bandwidth) to be made to the default configuration for the specified network or network set
- Boot order

Relationship to other resources

A connection resource is associated with the following resources in the **resource summary diagram**:

- Exactly one **server profile** resource.
- Zero or more **connection template** resources.
- Exactly one **network** or **network set** resource. The resources that are available to the connection depend on the configuration of the logical interconnect of the enclosure that contains the server hardware.

UI screens and REST API resources

UI screen	REST API resources
Server Profiles	connections and server-profiles

Connection templates

A connection template defines default configuration characteristics, such as the preferred bandwidth and maximum bandwidth, for a network or network set. When you create a network or network set, HPE OneView creates a default connection template for the network or network set.

Relationship to other resources

A connection template resource is associated with zero or more **connection** resources. A connection resource is associated with the appropriate connection template for a type of network or network set.

UI screens and REST API resources

UI screen	REST API resource	Notes
None	connection-templates	The UI does not display or refer to connection templates, but connection templates determine the default values displayed for the connection when you select a network or network set.

Data centers

In HPE OneView, a data center represents a physically contiguous area in which racks containing IT equipment—such as servers, enclosures, and devices—are located. You create a data center to describe a portion of a computer room, summarizing your environment and its power and thermal requirements. A data center resource is often a subset of your entire data center and can include equipment that is not managed by HPE OneView. By representing the physical layout of your data center equipment, including unmanaged devices, you can use detailed monitoring information for space planning and determining power and cooling requirements.

In HPE OneView, you can:

- View a 3D model of the data center layout that includes a color-coding scheme to help you identify areas that are too hot or too cold.
- View temperature history data.
- More easily locate specific devices for hands-on servicing.

Relationship to other resources

A data center resource is associated with the following resources in the **resource summary diagram**:

Zero or more **racks**

UI screens and REST API resources

UI screen	REST API resource
Data Centers	datacenters

Domains

The domain resource describes the management domain for the appliance. All physical and logical resources managed by the appliance are part of a single management domain.

Relationship to other resources

A domain resource is associated with the following resources in the **resource summary diagram**:

- Exactly one **appliance**
- Zero or more instances of the other resources in the summary diagram

UI screens and REST API resources

UI screen	REST API resource	Notes
None	domains	The UI does not display or refer to domains, but the domain resource provides information about limits such as the total number of networks that you can add to the appliance. You can use the <code>domains</code> REST API to obtain information about the domain.

Enclosures

An enclosure is a physical structure with device bays supporting server, networking, and storage building blocks. These building blocks share the enclosure's common power, cooling, and management infrastructure.

The enclosure provides the hardware connections between the interconnect downlinks and the installed servers. The enclosure interconnects provide the physical uplinks to the data center networks.

When you add an enclosure to be managed, HPE OneView discovers and adds all of the components within the enclosure, including servers and interconnects installed within the enclosure.

A logical enclosure is associated with an enclosure group which describes how the physical enclosure is connected to the networks and SAN. An enclosure is associated with an enclosure group through the logical enclosure.

Relationship to other resources

An enclosure resource is associated with the following resources in the **resource summary diagram**:

- One **logical enclosure**
- One **enclosure group**
- One or more physical **interconnects**
- One or more **logical interconnects** and one or more **logical interconnect groups** (through the enclosure's association with an enclosure group and interconnects)

- Zero or one **rack** resource
- Zero or more **power delivery devices**

UI screens and REST API resources

UI screen	REST API resource
Enclosures	enclosures

Enclosure groups

An enclosure group is a template that defines a consistent configuration for a logical enclosure. Network connectivity for an enclosure group is defined by the logical interconnect groups associated with the enclosure group.

Using enclosure groups, you can quickly add many enclosures and have them configured into identical logical enclosures.

Relationship to other resources

An enclosure group resource is associated with the following resources in the **resource summary diagram**:

- Zero or more **logical enclosures**
- Zero or more **server profiles**
- Zero or more **server profile templates**
- Exactly one **enclosure**
- Zero or more **logical interconnect groups**

UI screens and REST API resources

UI screen	REST API resource
Enclosure Groups	enclosure-groups

Enclosure types

An enclosure type defines characteristics of a specific Hewlett Packard Enterprise enclosure hardware model, such as an HPE BladeSystem c7000 Enclosure.

Relationship to other resources

An enclosure type resource is associated with zero or more **enclosures**.

UI screens and REST API resources

UI screen	REST API resource	Notes
None	None	The UI does not refer to enclosure type, but the enclosure type is used by HPE OneView when you add an enclosure. The <code>enclosures</code> REST resource includes an <code>enclosureType</code> attribute.

Hypervisor Manager

The hypervisor manager resource is a physical resource that represents hypervisor manager software, such as VMware vCenter server, which manages virtual environments. Hypervisor manager contains the identity and credentials required to communicate with the hypervisor manager software. Hypervisor manager also stores the preferences, which are used as defaults when deploying hypervisor clusters. You must register a hypervisor manager in HPE OneView to be able to create hypervisor cluster profiles. HPE OneView leverages the hypervisor manager software for deploying and managing hypervisor cluster and hypervisors.

Currently you can register a VMware vCenter server as a hypervisor manager in HPE OneView.

Relationship to other resources

A hypervisor manager resource is associated with the following resources in the resource summary diagram:

Zero or more hypervisor cluster profiles.

UI screens and REST API resources

UI screen	REST API resource
Hypervisor Managers	hypervisor-managers

Hypervisor Cluster Profiles

A hypervisor cluster profile is a logical resource that defines consistent compute, network, and storage configuration for a cluster of hypervisors. A hypervisor cluster profile enables you to import and manage a cluster of hypervisors running on servers, which support HPE Virtual Connect and managed by HPE OneView. Hypervisor Cluster profiles ensure consistent configuration across the cluster of server nodes to hypervisors, sharing the same workload.

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

The hypervisor cluster profile uses a server profile template to define the configurations for server nodes and hypervisors, which are a part of the hypervisor cluster. The hypervisor cluster profile orchestrates consistent configurations from the server nodes to hypervisors.

The configurations for the server nodes are derived from the configurations in the associated server profile template. You can specify shared storage volumes in the hypervisor cluster profile, and the storage volumes that are configured in the server profile template.

The network and storage configurations for the hypervisors are derived from the associated server profile template. The hypervisor network configuration defines the virtual switches and port groups. The virtual switch configuration is automatically built based on the connections in the associated server profile template and the hypervisor settings of the hypervisor cluster profile. The hypervisor storage configuration comprises of the hypervisor cluster volumes, and you can be format the volumes with Virtual Machine File System (VMFS).

Hypervisor cluster profile uses only the default TCP/IP stack configurations to create a VMkernel port on VMware vSphere ESXi hosts. To configure the VMkernel port with different TCP/IP stack configurations, use tools external to HPE OneView and retain the same VMkernel port name and VLAN as defined in the hypervisor cluster profile.

While enabling the Multi-NIC vMotion setting in a hypervisor cluster profile, during inconsistency remediation, ensure that the ESXi host has vMotion VMkernel port configured with default TCP/IP stack configuration. For other TCP/IP stack configurations in the vMotion VMkernel port, use tools external to HPE OneView.

While disabling the Multi-NIC vMotion setting in hypervisor cluster profile, provide the vMotion VMkernel port name that has to be retained.

NOTE: You can grow the cluster by creating the server profiles, deploying and adding hypervisors to the cluster using external tools, importing the hypervisors into hypervisor cluster profile, and by remediating inconsistencies.

Relationship to other resources

A hypervisor cluster profile resource is associated with the following resources in the resource summary diagram.

- One hypervisor manager
- One server profile template
- One or more networks
- Zero or one OS deployment plan
- Zero or more storage volumes.
- Zero or more hypervisor profiles

UI screens and REST API resources

UI screen	REST API resource
Hypervisor Cluster Profiles	hypervisor-cluster-profiles

Hypervisor profile

A hypervisor profile contains the configurations intended for a hypervisor running on server hardware managed by HPE OneView. This hypervisor is member of a cluster managed by HPE OneView, and it provides the virtual compute, network and storage resources to the cluster.

A hypervisor profile configuration is inherited from the hypervisor cluster profile; configurations on the hypervisor profile cannot be edited directly.

You can power on or off, reset, place the hypervisors into maintenance mode, and update from hypervisor cluster profile to rectify inconsistencies.

Relationship to other resources

A hypervisor profile resource is associated with the following resources in the resource summary diagram:

- One hypervisor manager
- One hypervisor cluster profile
- One server profile
- One or more networks

UI screens and REST API resources

UI screen	REST API resource
Hypervisor Profiles	hypervisor-host-profiles

Interconnects

An interconnect is a physical resource that enables communication between hardware in the enclosure and the data center Ethernet LANs and Fibre Channel SANs. The HPE Virtual Connect FlexFabric 10Gb/24-port Module is an example of a supported interconnect. For a list of supported interconnects, see the *HPE OneView Support Matrix* at <http://www.hpe.com/info/oneview/docs>.

An interconnect has the following types of ports:

Port type	Description
Uplinks	Uplinks are physical ports that connect the interconnect to the data center networks. For example, the X2 port of an HPE Virtual Connect FlexFabric 10Gb/24-port Module is an uplink.
Downlinks	Downlinks are physical ports that connect the interconnect to the server hardware through the enclosure midplane.
Stacking links	Stacking links are internal or external physical ports that join interconnects to provide redundant paths for Ethernet traffic from servers to the data center networks. Stacking links are based on the configuration of the associated logical interconnect group.

In the resource model:

- Interconnects are a part of enclosures and enclosure groups. The interconnects installed in an enclosure are added automatically when the enclosure is added to HPE OneView.
- Interconnects are defined by a logical interconnect group, which in turn defines the logical interconnect configuration to be used for an enclosure. The physical interconnect configuration in the enclosure must match the logical interconnect group configuration before an interconnect can be managed.
- For an interconnect to be usable, it must be installed in an enclosure and must be defined as part of a logical interconnect. Each physical interconnect can contribute physical uplink ports to an uplink set.
- Firmware baselines and firmware updates for physical interconnects are managed by the logical interconnect.

Relationship to other resources

An interconnect resource is associated with the following resources in the **resource summary diagram**:

- Exactly one **enclosure**
- Zero or one **logical interconnect**, and, through that logical interconnect, one or more **logical interconnect groups**

UI screens and REST API resources

UI screen	REST API resources
Interconnects	interconnects, interconnect-types, and logical-interconnects

Interconnect types

The interconnect type resource defines the characteristics of a model of interconnect, such as the following:

- Downlink capabilities and the number of downlink ports
- Uplink port capabilities and the number of uplink ports
- Supported firmware versions

Relationship to other resources

An interconnect type resource is associated with the following resources in the **resource summary diagram**:

Zero or more **interconnects**

UI screens and REST API resources

UI screen	REST API resource	Notes
Interconnects	interconnect-types	The UI does not display or refer to the interconnect type resource specifically, but the information is used by HPE OneView when you add or manage an interconnect using the Interconnects screen.

Logical enclosures

A logical enclosure represents a logical view of a single enclosure with an enclosure group serving as a template. If the intended configuration in the logical enclosure does not match the actual configuration on the enclosure, the logical enclosure becomes inconsistent.

A logical enclosure is automatically created when a c7000 enclosure is added.

Relationship to other resources

A logical enclosure resource is associated with the following resources in the **resource summary diagram**:

One enclosure, and through the enclosure, one **enclosure group**.

UI screens and REST API resources

UI screen	REST API resource
Logical Enclosures	logical-enclosures

Logical interconnects

A logical interconnect is a single entity for multiple physical interconnects

A logical interconnect is a single administrative entity that consists of the configuration for a set of interconnects in an enclosure. This configuration includes:

- Interconnects, which are required for the enclosure to connect to data center networks.
- Uplink sets, which map data center networks to physical uplink ports. If no uplink sets are defined, the logical interconnect cannot connect to data center networks, and the servers attached to the downlinks of the logical interconnect cannot connect to data center networks.
- Downlink ports, which connect through the enclosure midplane to the servers in the enclosure. A logical interconnect includes all of the physical downlinks of all of the member interconnects. The downlinks connect the interconnects to physical servers. The set of downlinks that share access to a common set of networks is called logical downlinks.
- Internal networks, which are used for server-to-server communications without traffic egressing any uplinks.

- Stacking links, if used, join interconnects either through connections inside the enclosure or external cables between the face plate ports of the interconnects.
- The firmware baseline, which specifies the firmware version to be used by all of the member interconnects. The firmware baseline for physical interconnects is managed by the logical interconnect.

The Network administrator configures multiple paths from server bays to networks

The Network administrator can ensure that every server bay of an enclosure has two independent paths to an Ethernet data center network by creating a logical interconnect for which the following conditions are true:

- The logical interconnect has at least two interconnects that are joined by stacking links, or two interconnects are defined in separate logical interconnect groups.
- The logical interconnect has at least one uplink set that includes uplinks to the network from at least two physical interconnects.

HPE OneView detects and reports a configuration or state in which there is only one path (no redundant paths) to a network or in which there are no paths to a network.

The Server administrator is not required to know the details about interconnect configurations

Because a logical interconnect is managed as a single entity, the server administrator is isolated from the details of interconnect configurations. For example, if the network administrator configures the logical interconnect to ensure redundant access from each server bay in the enclosure to each Ethernet data center network, the server administrator must only ensure that a server profile includes two connections to a network or to a network set that includes that network.

Relationship to other resources

A logical interconnect resource is associated with the following resources in the **Resource model summary diagram**:

- Zero or more **interconnects**. For a logical interconnect to be usable, it must include at least one interconnect. If there are zero interconnects, the enclosure and its contents do not have any uplinks to the data center networks.
- One or more **logical interconnect groups** associated with an enclosure group, which define the initial configuration of the logical interconnects.
- Zero or more **uplink sets**, which associate zero or more uplink ports and zero or more **networks**.
- Zero or one **logical enclosure**.

UI screens and REST API resources

UI screen	REST API resource	Notes
Logical Interconnects	logical-interconnects and logical-downlinks	You use the logical-downlinks REST API to obtain information about the common set of networks and capabilities available to a downlink.

Logical interconnect groups

The logical interconnect group is a template that defines the physical and logical configuration of the interconnects that are configured together to form a logical interconnect. This configuration includes the following:

- The interconnect types, interconnect configurations, and interconnect downlink capabilities
- The interconnect ports used for stacking links
- The uplink sets, which map uplink ports to Ethernet or Fibre Channel networks
- The available networks based on the uplink sets and internal networks

In the resource model:

- A logical interconnect group or groups is associated with an enclosure group instead of an individual enclosure.
- You can create a logical interconnect group either automatically during an enclosure add operation, or independently of enclosure add operations.

If you add an enclosure without specifying an existing enclosure group, HPE OneView creates both an enclosure group and a single logical interconnect group based on the physical interconnects in that enclosure. You can then edit that enclosure group and that logical interconnect group.

If you want multiple logical interconnect groups per enclosure, create the logical interconnect groups before you add the enclosure, or edit the logical interconnect groups to remove interconnects from one logical interconnect group and add them to another.

- The uplink sets defined by the logical interconnect group establish the initial configuration for uplink sets for each logical interconnect in the enclosure group. If you change uplink sets for an existing logical interconnect group:
 - Only enclosures that you add after the configuration change are configured with the new uplink set configuration.
 - Existing logical interconnects are reported as not being consistent with the logical interconnect group. You can then request that those existing logical interconnects be updated with the new configuration.

After a logical interconnect has been created and associated with a logical interconnect group, it continues to be associated with that group and reports if its configuration differs from the group. You can then change the configuration of the logical interconnect to match the group.

Relationship to other resources

A logical interconnect group resource is associated with the following resources in the **resource summary diagram**:

- Zero or more **logical interconnects**
- Zero or more **enclosure groups**

The uplink sets defined by a logical interconnect group specify the initial configuration of the **uplink sets** of each logical interconnect in the group.

UI screens and REST API resources

UI screen	REST API resource
Logical Interconnect Groups	<code>logical-interconnect-groups</code>

Logical switches

A logical switch is added into HPE OneView as a managed or monitored logical switch. The logical switch can consist of a maximum of two physical top-of-rack (ToR) switches (external to the c7000 enclosure) configured in a single stacking domain. The logical switch can also consist of Composable Fabric rack connectivity modules. For more information, see documentation on HPE Composable Cloud.

Connectivity limits one logical switch per one logical interconnect. Interconnects within a logical interconnect cannot be connected to more than one logical switch.

A logical switch is based on a logical switch group configuration. If the logical switch transitions to an `Inconsistent with group` state (because of changes in either the logical switch or the logical switch group), update the logical switch configuration based on the logical switch group to return to a consistent state.

A logical switch when part of a Composable Fabric, allows HPE OneView to deploy server profile connections to rack mount servers that are connected to this logical switch.

When not part of a Composable Fabric, you can create a logical switch as either monitored or managed:

- Creating a logical switch as monitored enables HPE OneView to:
 - Monitor the operation status.
 - Provide physical port information and port statistics.
 - Provide health events and changes in the port state.
 - Provide information about network availability between the enclosure edge and upstream ToR switches.
- Creating a logical switch as managed enables HPE OneView to provide full control of the port state and network provisioning for the ports between the enclosure edge and upstream ToR switches. When adding a logical switch in a managed mode, any existing configuration for ports connected to HPE OneView managed interconnects is replaced with the configuration specified for the HPE OneView interconnect uplinks. Any port that is actively managed by an external management system remains unchanged and is not brought into HPE OneView management. Deployment of the server profile connections supported only for Virtual Connect interconnects.

UI screens and REST API resources

UI screen	REST API resource
Logical Switches	logical-switches

Logical switch groups

The logical switch group is a template for creating logical switches. Logical switches are an aggregation of up to two physical top-of-rack switches.

Once constructed from a logical switch group, a logical switch continues to be associated with its logical switch group. Any change in consistency between the logical switch group and its associated logical switches is monitored and made visible on the associated logical switch screen in HPE OneView.

UI screens and REST API resources

UI screen	REST API resource
Logical Switch Groups	logical-switch-groups

Networks

A network represents a Fibre Channel, Ethernet, or Fibre Channel over Ethernet (FCoE) network in the data center.

Relationship to other resources

A network resource is associated with the following resources in the [resource summary diagram](#):

- Zero or more **connections**
- Zero or one **uplink set** per **logical interconnect**
- For tagged, Ethernet networks, zero or more **network sets**

UI screens and REST API resources

UI screen	REST API resource
Networks	fc-networks or ethernet-networks or fcoe-networks

Network sets

A network set represents a group of tagged, Ethernet networks identified by a single name. Network sets are used to simplify server profile configurations and server profile templates. When a connection in a server profile specifies a network set, it can access any of the member networks. Adding or deleting networks from a network set affects profiles that use the network set. One common use for network sets is as a trunk for multiple VLANs to a vSwitch.

In the resource model:

- A network set can contain zero or more tagged, Ethernet networks.
- A tagged, Ethernet network can be a member of zero or more network sets.
- A connection in a server profile can specify either a network or a network set.
- A network set can be member of an uplink set, if only the contained networks are not a duplicate of networks in other network sets associated to the same logical interconnect.

Other configuration rules apply.

Relationship to other resources

A network set resource is associated with the following resources in the **resource summary diagram**:

- Zero or more **connections**, and, through those connections, zero or more **server profiles**.
- Zero or more Ethernet **networks**.
- Zero or more uplink sets.

UI screens and REST API resources

UI screen	REST API resource
Network Sets	network-sets

Power delivery devices

A power delivery device is a physical resource that delivers power from the data center service entrance to the rack components. You create the power distribution device objects to describe the power source for one or more components

in the rack. Power delivery devices can include power feeds, breaker panels, branch circuits, PDUs, outlet bars, outlets, and UPS devices.

For a complete list of power delivery devices, see the screen details online help for the **Power Delivery Devices** screen.

Relationship to other resources

A power delivery device resource is associated with the following resources in the **resource summary diagram**:

- Zero or more **racks**
- Zero or more **unmanaged devices**

UI screens and REST API resources

UI screen	REST API resource
Power Delivery Devices	<code>power-devices</code>

Rack Managers

A rack manager platform is a multinode system. The nodes are housed within a rack or across racks, and are centrally managed by a management controller. A rack manager platform consists of one or more chassis, systems or nPartitions, and managers.

Relationship to other resources

A rack manager resource is associated with the following resources in the **resource summary diagram**:

- Zero or one **rack resource**
- One or more chassis
- One or more managers (Rack Management Controller)

UI screens and REST API resources

UI screen	REST API resource
Rack Managers	<code>rack-managers</code>

Racks

A rack is a physical structure that contains IT equipment such as enclosures, servers, power delivery devices, and unmanaged devices in a data center. By describing the physical location, size, and thermal limit of equipment in the racks, you enable space, power planning, and power analysis features for your data center.

Relationship to other resources

A rack resource is associated with the following resources in the **resource summary diagram**:

- Zero or one **data centers**
- Zero or more **enclosures**
- Zero or one **Rack Managers**
- Zero or more instances of **server hardware** (for HPE ProLiant DL servers)

- Zero or more **unmanaged devices**
- Zero or more **power delivery devices**

UI screens and REST API resources

UI screen	REST API resource
Racks	racks

SAN Managers

SAN Managers enables you to bring systems that manage SANs under management of HPE OneView. When you add a SAN manager to HPE OneView, the SANs that it manages become available to associate with HPE OneView networks that you can attach to server profiles.

In the resource model:

SAN managers are not associated with HPE OneView resources directly. The SANs they manage (known as managed SANs) can be associated with HPE OneView networks, which can then be configured in server profiles.

Relationship to other resources

The SAN managers resource is associated with the following resources in the **resource model summary diagram**:

A managed SAN on a SAN manager can be associated with one HPE OneView **network**, which can be associated with one **server profile**.

UI screens and REST API resources

UI screen	REST API resource
SAN Managers	fc-device-managers

SANs

SANs are discovered by SAN Managers and become managed when they are associated with HPE OneView networks. Server profile attachments to volumes over SANs auto configure the server, SAN zoning, and storage system enabling the server to access the volume.

SANs are made available to HPE OneView when the SAN manager to which they belong is added.

In the resource model:

- SANs are associated with the SAN Manager on which they reside.
- SANs can be associated with one or more Fibre Channel (FC) or Fibre Channel over Ethernet (FCoE) networks.

Relationship to other resources

The SANs resource is associated with the following resources in the **resource model summary diagram**:

A managed SAN on a SAN manager can be associated with one or more Fibre Channel (FC) and/or one or more Fibre Channel over Ethernet (FCoE) **network**.

UI screens and REST API resources

UI screen	REST API resource
SANs	fc-sans

Server hardware

Server hardware represents an instance of server hardware, such as a physical HPE ProLiant BL460c Gen8 Server Blade installed in an enclosure, or a physical HPE ProLiant DL380p rack server.

For information about the supported server hardware, see the *HPE OneView Support Matrix* at <http://www.hpe.com/info/oneview/docs>.

Relationship to other resources

A server hardware resource is associated with the following resources in the **resource summary diagram**:

- Zero or one **server profile**

If a server does not have a server profile assigned, you cannot perform actions that require the server profile resource, such as managing firmware or connecting to data center networks. However, you can:

- Add the managed server hardware to HPE OneView, including automatically updating the server firmware to the minimum version required for management by HPE OneView.

NOTE: Attempts to add monitored servers with less than the minimum firmware version required by HPE OneView will be unsuccessful. Update firmware outside of HPE OneView, for example, with Smart Update Manager (SUM).

- View inventory data.
 - Power on or off the server.
 - Launch the iLO remote console.
 - Monitor power, cooling, and utilization.
 - Monitor health and alerts.
- Exactly one **server hardware type**
 - If the server hardware is a server blade, exactly one device bay of an **enclosure**.
This association also applies to full-height servers, which occupy two device bays but are associated with the top bay only.
 - If the server hardware is a rack mount server, zero or one **rack** resource, and zero or more **power delivery devices**.
 - If the server hardware is a rack manager server, one or more chassis.

UI screens and REST API resources

UI screen	REST API resource	Notes
Server Hardware	server-hardware	Use the server hardware resource, not the server profile resource, to perform actions such as powering on or off the server, resetting the server, and launching the iLO remote console. You can launch the iLO remote console through the UI. The REST APIs do not include an API to launch the iLO remote console.

Server hardware types

A server hardware type captures details about the physical configuration of server hardware, and defines which settings are available to the server profiles assigned to that type of server hardware. For example, the server hardware type for the HPE ProLiant BL460c Gen8 Server Blade includes a complete set of default BIOS settings for that server hardware configuration.

When you add an enclosure to HPE OneView, HPE OneView detects the servers installed in the enclosure and creates a server hardware type for each unique server configuration it discovers. When you add a unique rack mount server model, HPE OneView creates a new server hardware type for that server configuration.

Relationship to other resources

A server hardware type resource is associated with the following resources in the **resource summary diagram**:

- Zero or more **server profiles**
- Zero or more **server profile templates**
- Zero or more servers of the type defined by that server hardware type

UI screens and REST API resources

UI screen	REST API resource
Server Hardware Types	server-hardware-types

Server profiles

Server profiles capture key aspects of the server configuration in one place, enabling you to provision converged infrastructure hardware quickly and consistently according to your best practices.

A server profile can contain the following configuration information about the server hardware:

- Basic server identification information
- Firmware versions
- Connections to Ethernet networks, Ethernet network sets, FCoE networks, Fibre Channel networks, and iSCSI
- Local storage
- SAN storage
- Boot settings

- BIOS settings
- iLO settings
- Physical or virtual UUIDs (universally unique identifiers), MAC (media access control) addresses and WWN (World Wide Name) addresses

Relationship to other resources

A server profile is associated with the following resources in the **resource summary diagram**:

- Zero or one **server profile template**
- Zero or more **connection** resources. You use a connection resource to specify connection from the server to a network or network set. If you do not specify at least one connection, servers using Virtual Connect cannot connect to data center networks. The networks and network sets that are available to a server profile connection depend on the configuration of the logical interconnect of the enclosure that contains the server hardware.

NOTE: Servers not using Virtual Connect do not need connection resources, as connectivity is controlled by programming the switches.

- Zero or one **server hardware** resource.
Exactly one **server hardware type** resource.
- Zero or more **volumes** through volume attachments.

NOTE: A volume attachment is a logical resource within a server profile that defines a volume attached to a network.

- Exactly one **enclosure group** resource.
To enable portability of server profiles, a server profile is associated with an enclosure group resource instead of an enclosure resource. Because enclosures in the enclosure group are configured identically, you can assign a server profile to any appropriate server hardware, regardless of which enclosure and bay in the enclosure group contains that server hardware.

UI screens and REST API resources

UI screen	REST API resource
Server Profiles	server-profiles

Server profile templates

Server profile templates help to monitor, flag, and update server profiles in HPE OneView.

A server profile template defines the source for the configuration of:

- Firmware versions
- Connections to Ethernet networks, Ethernet network sets, Fibre Channel networks, and iSCSI
- Local storage
- SAN storage
- Boot settings
- BIOS settings

- iLO settings
- Profile affinity

Relationship to other resources

A server profile template is associated with the following resource in the **resource summary diagram**:

- Zero or more **server profile** resources.
- Zero or more **connection** resources.
- Exactly one **server hardware type** resource.
- Zero or more **volumes** through volume attachments.
- Zero or more **storage pools** through volume templates.
- Exactly one **enclosure group** resource.

To enable portability of server profiles, a server profile is associated with an enclosure group resource instead of an enclosure resource. Because enclosures in the enclosure group are configured identically, you can assign a server profile to any appropriate server hardware, regardless of which enclosure and bay in the enclosure group contains that server hardware.

UI screens and REST API resources

UI screen	REST API resource
Server Profile Templates	server-profile-templates

Storage Pools

A storage pool exists on a storage system and contains volumes. Storage pools are created on a storage system using the management software for that system. After you add a storage pool to HPE OneView, you can add existing volumes or create new volumes.

In the resource model:

- A storage pool exists on only one storage system.
- A storage pool can contain zero or more volumes.
- A storage pool can be associated with zero or more volume templates.

Relationship to other resources

A storage pool resource is associated with the following resources in the **resource model summary diagram**:

One **storage system**, and through it, zero or more **volumes**, which can be connected to zero or more **server profiles**.

UI screens and REST API resources

UI screen	REST API resource
Storage Pools	storage-pools

Storage Systems

You can connect supported storage systems to HPE OneView to manage storage pools and volumes.

In the resource model:

- A storage system can have zero or more storage pools.
- A storage system can have zero or more volumes in each storage pool.

Relationship to other resources

A storage system resource is associated with the following resources in the [resource model summary diagram](#):

- Zero or more **storage pools**, and through those storage pools, zero or more **volumes**.
- Zero or more **server profiles**, through zero or more volumes.

UI screens and REST API resources

UI screen	REST API resource
Storage Systems	storage-systems

Switches

Switches provide a unified, converged fabric over Ethernet for LAN and SAN traffic. This unification enables network consolidation and greater use of infrastructure and cabling, reducing the number of adapters and cables required and eliminating redundant switches.

A configuration of enclosures, servers, and third-party devices—such as the Cisco Fabric Extender for HPE Blade System modules and Cisco Nexus top of rack switches—provides scalability to manage server blades and a higher demand for bandwidth from each server with access-layer redundancy.

HPE OneView provides minimal monitoring (power and state only) of switches and their associated interconnects. See the [HPE OneView Support Matrix](#) for the complete list of supported devices.

Relationship to other resources

A Cisco Nexus top of rack switch is associated with interconnects, specifically the Cisco Fabric Extender for Blade System modules within an enclosure, as shown in the [resource summary diagram](#).

UI screens and REST API resources

UI screen	REST API resource
Switches	switches

Unmanaged devices

An unmanaged device is a physical resource that is located in a rack or consumes power but is not currently managed by HPE OneView. Some unmanaged devices are unsupported devices that cannot be managed by HPE OneView.

All devices connected to an Intelligent Power Distribution Unit (IPDU) using an Intelligent Power Discovery (IPD) connection are added to HPE OneView as unmanaged devices.

Other devices that do not support IPD—such as KVM switches, routers, in-rack monitors and keyboards—are not added to the list of unmanaged devices automatically. To include these devices in HPE OneView, you can add them manually and describe their names, rack positions, and power requirements.

Relationship to other resources

An unmanaged device resource is associated with the following resources in the [resource summary diagram](#):

- Zero or more [racks](#)
- Zero or more [power delivery devices](#)

UI screens and REST API resources

UI screen	REST API resource	Notes
Unmanaged Devices	unmanaged-devices	You can view, add, or edit the properties of unmanaged devices using either the UI or the REST APIs. To delete an unmanaged device, you must use the REST APIs.

Uplink sets

An uplink set assigns data center networks to uplink ports of interconnects. The uplinks must be from physical interconnects that are members of the logical interconnect to which the uplink set belongs. An uplink set is part of a logical interconnect. For each logical interconnect:

- An uplink set can include a network set, if only the contained networks are not a duplicate of networks in other network sets associated to the same logical interconnect.
- A network can be a member of one uplink set per logical interconnect group.
- An uplink set can contain one Fibre Channel network.
- An uplink set can contain multiple Ethernet networks.
- An uplink set can contain one or more FCoE networks, but the uplinks must be contained within a single FCoE-capable interconnect.
- Internal networks allow server-to-server connectivity within the logical interconnect. Internal networks are created by adding existing networks to internal networks and not associating them with an uplink set. If you add an internal network to an uplink set, the network is automatically removed from the internal networks.

Relationship to other resources

An uplink set is part of a [logical interconnect](#) or a [logical interconnect group](#).

The uplink sets defined by a [logical interconnect group](#) specify the configuration for uplink sets used by logical interconnects that are members of the group. If the uplink sets of a logical interconnect do not match the uplink sets of the logical interconnect group, HPE OneView notifies you that the logical interconnect is not consistent with its group.

UI screens and REST API resources

UI screen	REST API resource
Logical Interconnects	uplink-sets
or	
Logical Interconnect Groups	

Volumes

A volume is a virtual disk allocated from a storage pool. A server profile can define the attachment of a server to a volume.

In the resource model:

- A volume exists in only one storage pool, which exists on only one storage system.
- A volume can be attached to zero, one, or many server profiles.

Relationship to other resources

A volume resource is associated with the following resources in the resource model summary diagram:

- One storage pool, and through it, one storage system
- Zero, one, or many server profiles through volume attachments
- Zero, one, or many server profile templates through volume attachments
- Zero or one volume template

UI screens and REST API resources

UI screen	REST API resource
Storage Volumes	storage-volumes

Volume Templates

A volume template defines the settings for the volumes created from it. Use a volume templates to create multiple volumes with the same configuration.

In the resource model:

A volume template can be associated with one storage pool.

Relationship to other resources

A volume template resource is associated with the following resources in the resource model summary diagram:

One storage pool, which can have zero, one, or many volume templates associated with it

UI screens and REST API resources

UI screen	REST API resource
Storage Volume Templates	storage-volume-templates

Using HPE OneView GUI or REST API scripts

HPE OneView makes it possible to easily monitor, configure, and manage physical and logical server, network, and storage resources through either a GUI (graphical user interface) or by using REST (REpresentational State Transfer) APIs.

HPE OneView GUI

The HPE OneView GUI is user-friendly, visually intuitive, and menu-driven to guide you through daily tasks. The HPE OneView GUI provides:

- A tutorial to introduce you to the HPE OneView GUI.
- A guided setup to help you configure your appliance.
- Alerts and activities to provide progress and status.
- **Online help** to provide more information.

The GUI provides on-screen hints and tips to help you avoid and correct errors, and provides links to learn more about the tasks. At the top of each screen, the help icon gives you access to the entire help system.

HPE OneView REST API

HPE OneView has a resource-oriented architecture that provides a uniform REST interface. REST is a web service that uses basic CRUD (Create, Read, Update, and Delete) operations performed on resources using HTTP `POST`, `GET`, `PUT`, and `DELETE`.

The REST APIs:

- Provide an industry-standard interface for open integration with other management platforms.
- Are designed to be ubiquitous—every resource has one URI (Uniform Resource Identifier) and represents a physical device or logical construct.
- Enable you to automate anything you can do from the UI using your favorite scripting or programming language.
- Are designed to be highly scalable.

About accessing HPE OneView message buses

HPE OneView supports asynchronous messaging to notify subscribers of changes to managed resources (both logical and physical) and changes to metrics on managed resources. For example, you can program applications to receive notifications when new server hardware is added to the managed environment or when the health status of physical resources changes, and you can stream power, thermal and CPU metrics for managed resources.

Using HPE OneView REST APIs, you can obtain certificates to access the two message buses: the State-Change Message Bus or the Metric Streaming Message Bus.

The message content is sent in JSON (JavaScript Object Notation) format and includes the resource model.

Before you can set up subscription to messages, you must create and download an AMQP (Advanced Message Queuing Protocol) certificate from the appliance using REST APIs. Next, you connect to the message bus using the `EXTERNAL` authentication mechanism with or without specifying a user name and password. This ensures that you use certificate-based authentication between the message bus and your client. After connecting to the message bus, you set up a queue with the queue name empty, and AMQP generates a unique queue name. You use this queue name to bind your client to exchanges and receive messages.

To connect to the message and set up a queue, you must use a client that supports the AMQP.

How to get started with HPE OneView

The **Quick Start** topics in the online help provide steps to configure the appliance and resources. To learn more about the configuration details, select one of the following topics:

- **Quick Start: Initial configuration of HPE OneView**
- **Quick Start: Add a network and associate it with an existing server**
- **Quick Start: Configuring SAN storage**

The *HPE OneView Installation Guide* at <http://www.hpe.com/info/oneview/docs> contains instructions on how to install HPE OneView.

Smart Update Tools installation with HPE Insight Control server provisioning

Smart Update Tools (SUT) can be installed along with HPE Insight Control server provisioning on ProLiant servers. When run in AutoStage mode, SUT only stages the firmware and drivers to the operating system. The firmware and driver installation can be executed during a planned maintenance window to activate the firmware.

NOTE: HPE Insight Control server provisioning supports provisioning on HPE ProLiant G7, Gen8, and Gen9 servers. For Gen10 ProLiant servers, HPE recommends to use tools like VMware AutoDeploy.

More information

- *HPE Insight Control Server Provisioning Administrator Guide* at <http://www.hpe.com/info/insightcontrol/docs>
- *Smart Update Tools for iLO Amplifier Pack User Guide* at **Smart Update Tools Information Library**.

Accessing documentation and help

This chapter describes how to access help from the appliance, how to access the publicly available online information library.

Online help—conceptual and task information as you need it

The online help documents both the UI and the REST APIs, and includes:

- Descriptions of resources and UI screens
- Quick-start instructions for bringing your data center under management
- Step-by-step instructions for using the UI to perform tasks
- Information about using the SCMB (State-Change Message Bus) to subscribe to state change messages

UI help design

The online help for the UI is designed so that each resource is documented in its own chapter. At the top of each help chapter is a navigation box that directs you to:

- Tasks that you can perform using the UI
- An **About** section that provides conceptual information about the resource
- A screen details section for every screen, which provides definitions of screen components to assist you in data entry and decision making
- Troubleshooting information in case you encounter a problem

This user guide supplements the online help

This user guide provides:


- Overviews of the appliance and its features
- Descriptions of resources and UI screens
- Tasks you can perform outside of the appliance when the appliance is unavailable
- Planning information, including configuration decisions to make and tasks that you might need to perform before you install an appliance, add managed devices, or make configuration changes
- Security information

Where to find HPE OneView documentation

User guides and other manuals


HPE OneView user guides and other manuals are available on the [Enterprise Information Library](#).

Online help

To view help on the appliance, click .

Help sidebar

Links in the sidebar open help in a new browser window or tab:

- **Help on this page** opens help for the current screen
- **Browse help** opens the top of the help system where you decide which help topics you want to read
- Clicking  on a screen or dialog box opens context-sensitive help for that dialog box.

NOTE: To submit feedback about HPE OneView documentation, send email to docsfeedback@hpe.com.

Enable off-appliance browsing of UI help

The off-appliance versions of the HPE OneView help systems are useful for developers who are writing API scripts or other users who prefer the convenience of accessing help locally without logging in to the appliance.

Procedure

1. Go to the [Enterprise Information Library](#).
2. Select the *HPE OneView Online Help* ZIP and save it to your computer or to a local directory on a web server.
3. Use the utility of your choice to extract the contents of the .zip file.
4. Navigate to the content directory.
5. To open the HPE OneView help system, double-click the `index.html` file.

Planning tasks

The chapters in this part describe data center configuration planning tasks that you might want to complete before you install the appliance or before you make configuration changes. By completing these planning tasks, you can create a data center configuration that takes full advantage of the appliance features and is easier for your administrators to monitor and manage.

Planning your data center resources

In addition to ensuring that your environment meets the prerequisites for installation of the appliance, there are other planning tasks you might want to complete before adding data center resources. By completing these planning tasks, you can create a data center configuration that takes full advantage of the appliance features and is easier for your administrators to monitor and manage.

How many data centers?

An appliance data center resource represents a physically contiguous area in which racks containing IT equipment are located. You create data centers in the appliance to describe a lab floor or a portion of a computer room, which provides a useful grouping to summarize your environment and its power and thermal requirements.

Using data centers to describe the physical topology and power systems of your environment is optional. If you choose to create multiple data centers, consider including data center information in your other resource names to enable you to use the appliance search capabilities to filter results by data center.

Managing, monitoring, or migrating server hardware?

Determine whether you want to add enclosures into HPE OneView to manage or monitor them, or if you want to migrate a Virtual Connect enclosure. See [Managing, monitoring, or migrating server hardware on enclosures](#).

Security planning

To learn about the security features of the appliance, and for general information about protecting the appliance, see [Understanding the security features of HPE OneView](#).

Preparing your data center network switches

The switch ports for data center network switches that connect to the Virtual Connect interconnect modules must be configured as described in "Data center switch port requirements" in the online help. Network traffic should also be considered as described in "About active/active and active/standby configurations" in the online help.

Planning for a dual-stack implementation

Network management systems can use IPv4 or IPv4/IPv6 communication protocols on the same network infrastructure. The default protocol is IPv4. Managing interconnects with IPv4 and IPv6 protocols provides network address redundancy if the IPv4 primary address fails to connect.

IPv4/IPv6 dual communication stack configuration is required for the appliance to communicate with the interconnects on the IPv6 management network

To set up a dual-stack protocol for an enclosure, use the Onboard Administrator to enable IPv6 and IPv6 address types.

NOTE: SNMP access and SNMP trap destinations support IPv4 and IPv6 addresses.

Planning your resource names

The banner of every screen includes the **Smart Search** feature, which enables you to find resource-specific information such as instances of resource names, serial numbers, WWNs, and IP and MAC addresses. In general, anything that appears in a resource master pane is searchable.

Defining a standard naming convention for your networks, network sets, enclosures, enclosure groups, logical interconnect groups, and uplink sets makes it easy for you to identify them and enables efficient searching or filtering in the UI.

Consider the following information when choosing resource names:

- To minimize the need for name changes and to make network-related resources easier to identify, consider choosing names that include the following information:
 - The purpose of the resource. For example:
 - `prod` for production network resources
 - `dev` for development network resources
 - For tagged networks, the VLAN ID

NOTE: If you are creating multiple tagged networks at the same time (creating networks in bulk), the network name is automatically appended with an underscore (`_`) and the VLAN ID. For example, `Dev_101`.

 - An identifier to help you distinguish between resources that use the left side or the right side of an enclosure. For example:
 - `left` and `right`
 - `A` and `B`
 - `1` and `2`
 - Examples of network names that follow the recommended naming conventions include the following:
 - `dev_1105_A`
 - `prod_1102_1`
 - `test_1111_left`
 - If you plan to use multinet connections in server profiles, create network sets that contain all the networks to be used by a single profile connection. Choose names such as the following:
 - `dev_nset_A`
 - `prodnset_1`
 - `testns_left`
 - Changing the names of uplinks sets can result in resources being taken offline temporarily.
To minimize the need for name changes, and make the uplink sets easier to identify, choose names such as the following:
 - `devUS_A`
 - `prodUS_1`
 - `testUS_left`
- The appliance does not support the filtering of resources, such as server hardware, based on physical location (data center name). To enable filtering by data center name, choose a naming convention that includes the data center name in the resource name.
- The appliance supports the filtering of resources by model, so you can search for server hardware without having to include the model number in the name.
- The appliance provides default names for many resources. For example:
 - Enclosures are assigned the name `Encln`, where `n` is a number that is incremented by 1 when each enclosure is added.
 - `enclosure_name-LI` is the default name of a logical interconnect, where `enclosure_name` is the name of the enclosure.

- Datacenter 1 is the name assigned to the data center when you initialize the appliance.
- Server hardware types are assigned names based on the server model, such as BL460c Gen8 1. If you select a server hardware type as a standard, you can choose to rename that server hardware type to include the word Standard or some other identifier to help administrators quickly determine the correct server hardware type to choose.
- You can create shorter names by using abbreviations for resources. For example:

Resource name	Typical abbreviations
Enclosure	Encl
Enclosure group	EG, Group
Logical interconnect	LI
Logical interconnect group	LIG
Uplink set	US

For more information about the search capabilities of the appliance, see "Search resources" in the online help.

Planning the appliance configuration

These topics cover appliance configuration.

For supported hypervisors and versions, see the *HPE OneView Support Matrix* at <http://www.hpe.com/info/oneview/docs>.

Planning for multiple instances of HPE OneView

If you are planning to deploy multiple HPE OneView appliances or also have HPE Synergy in your environment, you can use HPE OneView Global Dashboard. Global Dashboard provides a unified view of health, alerting, and key resources managed by HPE OneView across multiple appliances and data center sites. As information about resources changes, those changes are updated in real time in Global Dashboard.

More information

HPE OneView Global Dashboard User Guide at [Hewlett Packard Enterprise Information Library](#)

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.

Separate networks for data and management

HPE recommends having separate networks for management and data. See [**Best practices for maintaining a secure appliance**](#) for more information.

Time clocks and NTP

HPE recommends using NTP on the host on which you install the virtual appliance. If you are not using NTP on the host, HPE recommends configuring NTP directly on the virtual appliance. Do not configure NTP on both the host and the virtual appliance. In addition, the clock on the VM host must be set to the correct time.

IP addresses

You must specify what type of IP addresses are in use and how they are assigned to the appliance, either manually by you or assigned by a DHCP (Dynamic Host Configuration Protocol) server.

The appliance supports configuring IPv4-only or IPv6-only or a dual mode (both IPv4 and IPv6) for appliance IP address.

VM appliance

On a VM appliance, IP addresses can be assigned in two ways: manually by the user (static IP) or assigned by DHCP (Dynamic Host Configuration Protocol). DHCP is not supported for assigning appliance IP addresses unless DHCP reservations are used.

More information

[**Planning for a dual-stack implementation**](#) on page 59

Planning for configuration changes

This chapter identifies configuration changes that might result in a resource being taken offline temporarily or that might require that you make changes to multiple resources.

Configuration changes that require or result in resource outages

Appliance

Taking an appliance offline does not affect the managed resources—they continue to operate while the appliance is offline.

When you install an appliance update, the appliance restarts and goes offline.

Enclosures

The Onboard Administrator (OA) is taken offline automatically during an enclosure firmware update.

Interconnects and logical interconnects

- Server profile connections to networks in an uplink set are taken offline when you delete the uplink set.
- Server profile connections to networks in an uplink set can be interrupted for a few seconds when you change the name of an uplink set using either of these methods:
 - Change the name of the uplink set in the logical interconnect.
 - Change the name of the uplink set in the logical interconnect group, and then update the logical interconnect from the logical interconnect group.
- An interconnect is taken offline when you:
 - Update or activate firmware for a logical interconnect. Staging firmware does not require interconnects be taken offline.
 - Update firmware for an enclosure and select the option to update the enclosure, logical interconnect, and server profiles.
- If an interconnect has firmware that has been staged but not activated, any subsequent reboot of that interconnect activates the firmware, which takes the interconnect offline.
- You can prevent the loss of network connectivity for servers connected to a logical interconnect that has a stacking mode of `Enclosure` and a stacking health of `Redundantly Connected` by updating firmware using the following method:
 1. Staging the firmware on the logical interconnect.
 2. Activating the firmware for the interconnects in even-numbered enclosure bays.
 3. Waiting until the firmware update completes and the interconnects are in the `Configured` state.
 4. Activating the firmware for the interconnects in the odd-numbered enclosure bays.

Networks

- If you attempt to delete a network that is in use by one or more server profiles, the appliance warns you that the network is in use. If you delete the network while it is in use, server profile connections that specify the network explicitly (instead of as part of a network set) are taken offline.

If you add a network with the same name as the network you deleted, connections that specify the network explicitly (instead of as part of a network set) are not updated—you must edit each server profile connection to reconfigure it to

specify the network you added. Because you must edit the server profile to edit the connection, you must power off the server.

- If you attempt to delete a network that is a member of a network set, the appliance warns you that the network is assigned to at least one network set. If you delete that network and there are other networks in that network set, server profile connectivity to the deleted network is taken offline, but connectivity to other networks in the network set is unaffected.

You can add a network to a network set, including a network that has the same name as a network you deleted, while server profile connections to that network set remain online.

Network sets

- If you attempt to delete a network set that is in use by one or more server profiles, the appliance warns you that the network set is in use. If you delete the network set while it is in use, server profile connections to that network set are taken offline.
- If you add a network set with the same name as the network you deleted, connections that specify the network set are not updated—you must edit each server profile connection to reconfigure it to specify the network set you added. Because you must edit the server profile to edit the connection, you must power off the server.
- Server profiles with connections to a network set can be affected when a network in the network set is deleted.

Server profiles and server hardware

- Before you edit a server profile, you might need to power down the server hardware to which the server profile is assigned. See "About editing a server profile" in the online help for a list of edits that can be performed without powering down the server hardware.
- Firmware updates require that you edit the server profile to change the firmware baseline.
- Server profiles and server hardware can be affected by changes to networks and network sets. For example, if a new network is added, you might need to add a new connection.
- Server profiles and server hardware network connectivity can be affected by changes to the names of uplink sets.

Configuration changes that might require changes to multiple resources

- **Adding a network** on page 64
- **Adding an enclosure** on page 65

Adding a network

When you add a network to the appliance, you might need to make configuration changes to the following resources:

- **Networks**

Add the network.

If the network is not added to a network set, you must add a connection to the network in the server profiles that you want to connect to that network. Power off the server hardware before adding the connection to a server profile.

- **Network Sets**

(Optional) If the network you are adding is an Ethernet network you might want to add it to a network set or create a network set that includes the network.

If you add the network to a network set, server profiles that have connections to the network set automatically have access to the added network. You do not have to edit these server profiles.

- **Logical Interconnects and Logical Interconnect Groups**

For a server connected to a logical interconnect to access a network, the logical interconnect must have an uplink set that includes a connection to that network:

- You might need to update multiple logical interconnects.
- You can make configuration changes to the logical interconnect group, and then update each logical interconnect from the group.
- If your configuration changes include deleting an uplink set or changing the name of an uplink set, server profile network connectivity can be affected.

- **Server Profiles**

For a server to connect to the network, the server profile for the server hardware must include a connection to either the network or a network set that includes the network.

If the server profile does not have a connection to a network set that includes this network, you must add connections to the network.

For a summary of the tasks you complete when adding a network, see "Quick Start: Add a network and associate it with an existing server" in the online help.

Adding an enclosure

When you add an enclosure to be managed by the appliance, you might need to make configuration changes to the following resources:

- **Enclosures**

Add the enclosure to be managed.

- **Enclosure Groups**

Every managed enclosure must be a member of an enclosure group. If you do not choose an existing enclosure group, you must create one when you add the enclosure.

- **Logical Enclosures**

Logical enclosures maintain configurations of enclosures that are linked together. Use logical enclosures for firmware updates, OA scripting, and making the enclosures consistent with changes made from the enclosure group.

- **Logical Interconnects and Logical Interconnect Groups**

Logical interconnects and logical interconnect groups define the network connectivity for the managed enclosure. Enclosure groups must specify a logical interconnect group. When you create an enclosure group, if you do not specify an existing logical interconnect group, you must create one. For a server connected to a logical interconnect to access a network, the logical interconnect group you create must have an uplink set that includes a connection to that network.

- **Server Profiles**

Adding and assigning server profiles to the server blades in the managed enclosure is not required at the time you add the enclosure, but to use the server blades in a managed enclosure, you must assign server profiles to them. To access a network, the server profile must include a connection to that network or a network set that includes that network.

For a summary of the tasks you complete when adding a managed enclosure and connect its server blades to data center networks, see "Quick Start: Add a c7000 enclosure with a single logical interconnect group" in the online help.

Planning for enclosure migration from VCM into HPE OneView

Planning for a migration from VCM-managed enclosures to HPE OneView-managed enclosures is an important part of the migration process. Understanding what will be migrated from Virtual Connect Manager (VCM) and the requirements of HPE OneView can help ensure a smooth and easy migration. This chapter will help explain the requirements and what to expect with migration. For example, a partial list of what will not be migrated is shown in "About blocking issues during migration" in the online help.

The automated migration process imports the configuration information for the enclosures including hardware, Virtual Connect (VC) domain, networks, and server profiles with some exceptions. MAC and WWN settings on server profile connections are retained and specified as user-defined in HPE OneView. Any new addresses allocated after the migration are assigned from the HPE OneView ID pool. See "About ID pools" in the online help for more information.

In planning your migration, keep in mind that Virtual Connect is case sensitive but HPE OneView is case insensitive. For example, in Virtual Connect, "Profile1" is different than "profile1" is different than "PROFILE1". In HPE OneView, "Profile1" is the same as "profile1" is the same as "PROFILE1". You may need to change the name of some components before migrating to avoid name conflicts.

Timing and type of migration

In determining when to perform a migration, decide if you want to perform an in-service or offline migration. For offline, consider the required down time needed to perform the migration. For in-service, consider the hardware and software infrastructure needed to perform the migration.

The size of the configuration that you want to migrate affects process time. Large, complex configurations take more time to process than smaller ones.

Understanding the migration process

An enclosure managed by VCM can be migrated into HPE OneView so that it can be managed by HPE OneView. The migration can occur through the HPE OneView UI or using REST API. The basic process consists of the following steps. Review this process to see the types of issues you might encounter so you can determine what changes you need to make in your environment to perform a successful migration. See "Before migrating enclosures" in the online help for more information.

! **IMPORTANT:** Execute `show config -includepoolinfo` from the VCM command line. Back up the VCM configuration: the Virtual Connect (VC) domain as well as the output from `show config -includepoolinfo`. The backup is used if you need to revert to VCM for management. If a restoration is needed, you will need the factory default credentials for the VC interconnect found on the label.

The `show config -includepoolinfo` output enables you to check specific details of the VC domain after the enclosure has been migrated to HPE OneView. See the Virtual Connect User Guide at <http://www.hpe.com/info/virtualconnect/docs> for more information.

Prerequisites for performing a migration

- Minimum required privileges: HPE OneView Infrastructure administrator, Onboard Administrator (OA), and VCM Domain Administrator.
- OA and VCM credentials as well as the OA IP address for the enclosure.
- For VCEM-managed enclosures: VCEM credentials to remove the Virtual Connect domain from the domain group using the VCEM web interface, or the HPE PowerShell module.
- Backup and secure the VCM configuration (including the output from `show config -includepoolinfo`).

- Review the **HPE OneView Support Matrix** and verify that the enclosure contains supported servers, interconnect modules, and mezzanine cards.
- Review *Prerequisites for bringing an enclosure into HPE OneView* in the online help for prerequisites and preparation that must be in place.
- Assign server profiles before the migration, or recreate server profiles after the migration, if applicable.
- Ensure network connectivity with OA and iLOs in the Virtual Connect domain.
- Ensure all interconnect modules are present and powered on within the enclosure.

Migration task

Start compatibility and migration process

1. Determine if you want to perform an offline or in-service migration.
2. Determine whether to migrate your enclosure using the HPE OneView GUI or HPE OneView REST API.
3. Provide OA and VCM credentials and the enclosure OA IP address.

HPE OneView checks the compatibility of the VCM-managed enclosure with HPE OneView and produces a migration compatibility report of the issues. The report shows warnings and blocking issues.

Resolve issues in the compatibility report

1. Review and resolve issues from the top down in the compatibility report. By resolving issues that are listed first, you might resolve issues listed later in the report.
 - Resolve all **blocking** migration errors listed on the compatibility report by modifying the configuration in VCM or HPE OneView. See the online help for a list of some of the blocking issues you might encounter.
 - Evaluate **warnings** on the compatibility report to determine if action needs to be taken.

Unless specified otherwise, warnings indicate a capability that will not be migrated into HPE OneView. Make sure the detected capability is not critical to operations before proceeding. For a list of some of the warnings you might encounter, see **Warning issues** on page 68.

2. Resolving an issue may require disabling a feature within VCM, changing a configuration in VCM, or in some cases, changing the HPE OneView logical interconnect group.

For more information on VCM, see the *HPE Virtual Connect for c-Class BladeSystem User Guide* or the *HPE Virtual Connect Manager Command Line Interface for c-Class BladeSystem User Guide* at <https://www.hpe.com/info/virtualconnect/docs>.

Table Continued

Migration task

Migrate

1. For in-service migration, after resolving all blocking issues and warnings you want to resolve, run a final compatibility test.

For offline migration, after resolving all blocking issues (except server power-on) and warnings you want to resolve, power off the servers and run a final compatibility test.

2. If the final report shows that all blocking issues are resolved:
 - a. Read each acknowledgment in full (including any learn more links).
 - b. Understand and accept the implications of each acknowledgment by clicking each one.
 - c. Proceed with the migration.

NOTE: You have the option to migrate up to four single enclosure domains from VCM into HPE OneView simultaneously.

Post migration tasks

1. Upon successfully completing an offline migration, power on the servers.
2. Optional: Recreate server profiles in HPE OneView, if server profiles were not assigned to server hardware before migration.
3. Perform the following best practices:
 - a. Back up the new configuration in HPE OneView.
 - b. Test network and storage connectivity.
 - c. Plan a reboot if one of the acknowledgments, such as an SR-IOV virtual function configuration, indicated a change which would impact your operation.

NOTE: During an in-service migration, some changes do not take effect until the servers are rebooted for the first time following a migration.

After migration, the enclosure is no longer available in VCM.

Warning issues

The following partial list of Virtual Connect features are not supported in HPE OneView. These features are considered **warning** issues and are listed in the compatibility report. Migration can continue with these warnings, but you should review them to determine if the features are important to your environment. If a feature is required in your environment and your enclosure contains ProLiant G6 or later server blades, you might want to consider monitoring your enclosure. See "About monitored enclosures" in the online help for more information.

NOTE: Unassigned profiles will not be migrated. The profiles will be deleted from VCM during the migration. Either assign profiles before the migration or use the `show config -includepoolinfo` output to recreate the profiles once the enclosure is in HP OneView.

Potential warnings

- | | | |
|---|----------------------------|--|
| • Custom module hostname | • Network Access Group | • Unassigned server profiles |
| • Mixed USE-BIOS connections in a profile | • RADIUS/TACACS+ | • User role configuration |
| • Module-specific DNS name | • sFlow traffic monitoring | • VCM SNMP traps and Ethernet and FC SNMP access settings inconsistent |
| | • SMIS not enabled | |
-

NOTE: In general, if a feature is listed as a warning which is not required for the environment, continuing will mean the functionality will not be migrated to HPE OneView.

Security in HPE OneView

The chapters in this part describe the security features found in HPE OneView, best practices, and troubleshooting.

Best practices for maintaining a secure appliance

The following table comprises a partial list of security best practices that Hewlett Packard Enterprise recommends in both physical and virtual environments. Security best practices differ by customer and their specific or unique requirements. No one set of best practices is applicable for all customers.

Topic	Best Practice
Access	<ul style="list-style-type: none">Control <u>access to the appliance</u><ul style="list-style-type: none">Allow HPE Services access
Accounts	<ul style="list-style-type: none">Limit or disable the number of local accounts. Integrate the appliance with an Enterprise directory solution such as Microsoft Active Directory or OpenLDAP. Use the enterprise directory features for password expiration, complexity, history, and to disable local users and groups.If local accounts are used, protect the built-in administrator account with a strong password.Do not use the built-in Administrator account. All users must log in using their own credentials to facilitate auditing.
Audit logs	Download the appliance audit logs at regular intervals.

Table Continued

Topic	Best Practice
Certificates	<ul style="list-style-type: none"> Use certificates signed by a trusted certificate authority (CA). <p>HPE OneView uses certificates to authenticate and establish trust relationships. One of the most common uses of certificates is when a connection from a web browser to a web server is established. The machine level authentication is carried out as part of the HTTPS protocol, using SSL. Certificates can also be used to authenticate devices when setting up a communication channel.</p> <p>The appliance supports self-signed certificates and certificates signed by a CA.</p> <p>The appliance is initially configured with self-signed certificates for the web server and the State Change Message Bus (SCMB).</p> <p>The same CA signed appliance certificate used to secure access to HPE OneView is also used for the SCMB server certificate. A client certificate is not available for SCMB by default, but can be generated from the internal HPE OneView CA, <u>or through another trusted CA.</u></p> <p>Hewlett Packard Enterprise advises customers to examine their security needs (that is, to perform a risk assessment) and consider the use of certificates signed by a trusted CA.</p> <ul style="list-style-type: none"> You should use your company's existing custom CA and import their trusted certificates. The trusted root CA certificate must be deployed to both HPE OneView and to the hardware devices that HPE OneView manages. HPE OneView performs the CA-based certificate validation. All the devices that you are connecting to must have certificates that are trusted by that root CA. If your company does not have its own certificate authority, consider using a commercial CA. There are numerous third-party companies that provide trusted certificates. You will need to work with the external CA to have certificates generated for specific devices and systems and then import these trusted certificates into the components that use them. <p>As the Infrastructure administrator, you can generate a certificate signing request (CSR) and, upon receipt, upload the certificate to the appliance web server. This ensures the integrity and authenticity of your HTTPS connection to the appliance. Certificates can also be uploaded for the SCMB.</p> <p>See <u>Use a certificate authority</u> on page 131.</p> <p>The following considerations apply when you are looking to replace a self-signed certificate with a commercial CA-signed certificate:</p> <ul style="list-style-type: none"> Determine if you want to use commercial CA certificates for all of the devices in your environment, or just the appliance web server certificate. Determine if you want to use a public key infrastructure (PKI) to generate your own CA-signed certificates, or purchase commercial CA-signed certificates for all your managed devices. For the appliance web server certificate, you must request the CA to include the following: <ul style="list-style-type: none"> Key usage with digital signature. Key encipherment values. Extended key usage with Server Authentication or Client Authentication as values. Basic Constraints for Subject Type with End Entity as the value.

Table Continued

Topic	Best Practice
	<ul style="list-style-type: none"> ◦ Expiration or validity of the certificates: Frequently expiring commercial certificates are difficult to manage. Therefore, Hewlett Packard Enterprise recommends a minimum validity period of one to two years. ◦ The Enterprise Directory Server administrator must ensure that the Subject Alternative Name and the Subject of the Certificate Signing Request (CSR) that was used to obtain the CA-signed certificate for the managed device contains either the host (fully qualified domain name), resolved IP Address or the wildcard entry for the domain name. Anytime the IP address or hostname of the appliance changes, any CA-signed appliance certificate associated with the appliance is erased, and a new self-signed appliance certificate is generated. In this case, you must generate a new CSR, have it signed by a CA, and import it into the appliance. ◦ If a commercial CA has a chain, such as, root CA and other intermediate CAs, you must load all the certificates in the chain to HPE OneView as the appliance expects all those certificates to be trusted. ◦ The maximum number of certificates that can be present in the certificate chain is nine. The appliance fails to connect to any device or server if it has a certificate chain depth higher than the maximum limit. The maximum certificate chain depth is set by default on the appliance, and cannot be customized by the user. ◦ If you want to perform certificate revocation checks, you must set up Certificate Revocation Lists (CRL) from the CAs, and refresh them periodically.
Network	<ul style="list-style-type: none"> • Hewlett Packard Enterprise recommends creating a private management LAN and keeping that separate, known as air-gapped, from production LANs, using VLAN or firewall technology (or both). <ul style="list-style-type: none"> ◦ Management LAN Connect all management processor devices, including Onboard Administrators, iLOs, and iPDUs to the HPE OneView appliance by using the management LAN. Grant management LAN access to authorized personnel only. For example, Infrastructure administrators, Network administrators, and Server administrators. ◦ Production LAN Connect all NICs for managed devices to the production LAN. • Hewlett Packard Enterprise recommends to not connect management systems such as, the appliance, the iLO, and the Onboard Administrator directly to the Internet. If you require inbound Internet access, use a corporate VPN (virtual private network) that provides firewall protection. For outbound Internet access (for example, for Remote Support), use a secured web proxy. To set the web proxy, see "Preparing for remote support registration" or "Configure the proxy settings" in the online help for more information.

Table Continued

Topic	Best Practice
Passwords	<ul style="list-style-type: none"> Hewlett Packard Enterprise recommends that you integrate HPE OneView with an enterprise directory such as Microsoft Active Directory or OpenLDAP and disable local HPE OneView accounts, except for the Maintenance Console. Your enterprise directory can then enforce common password management policies such as password lifetime, password complexity, and minimum password length. The appliance maintenance console uses a local administrator account. Hewlett Packard Enterprise recommends that you set a password for appliance maintenance console access.
Permissions	<p>Permissions are used to control user access to the appliance and the resources managed by the appliance. The Infrastructure administrator grants rights to users and directory groups by assigning permissions. A permission consists of a role and an optional scope. The role grants access to resource categories. For more information about permissions, see <i>HPE OneView Online help</i>.</p> <ul style="list-style-type: none"> Role: HPE OneView defines a set of roles that describe the actions a user can perform on resource categories. When assigned to a user or directory group, a role grants the right to perform actions on categories of resources managed by the appliance. The Infrastructure administrator role should be reserved for the highest access. See "About user roles" in the online help. Scope: Define a scope and assign a subset of resources representing the management domain of one or more users. A scope in a permission further restricts the rights granted by the role to particular resource instances. Thus, it is appropriate to use a common scope in permissions for users with differing roles.
Two-factor authentication	HPE OneView supports two-factor authentication. Deploy two-factor authentication for increased security.
Updates	<ul style="list-style-type: none"> Sign up for HPE OneView bulletins at: http://www.hpe.com/support/e-updates Install updates for all components in your environment on a regular basis.
Virtual Environment	<ul style="list-style-type: none"> Restrict access to the appliance console to authorized users so that only authorized personnel can initiate HPE service requests, which can grant privileged access to the appliance. If you use an Intrusion Detection System (IDS) solution in your environment, ensure that the solution has visibility into network traffic in the virtual switches. Follow your hypervisor software best practices.

Understanding the security features of HPE OneView

Most security policies and practices used in a traditional environment are applicable in a virtualized environment.

High-level overview

Security-hardened appliance on page 119

- **Best practices for maintaining a secure appliance** on page 71
- **Nonbrowser clients** on page 137

User access and authentication

- **About complex passwords** on page 75
- **About directory service authentication** on page 78
- **Authentication for appliance access** on page 120
- **Controlling access for authorized users** on page 125
- **Creating a login session** on page 120
- **Specifying user accounts and roles** on page 125
- **Protecting credentials** on page 128

Console access

Controlling access to the appliance console on page 140

Certificates

- **Two-factor Authentication** on page 121
- **Managing certificates from a browser** on page 130
- **Certificate management** on page 157

Learn more

- **Algorithms, cipher suites, and protocols for securing the appliance** on page 98
- **Ports required for HPE OneView** on page 137
- **Files you can download from the appliance** on page 142
- **About audit log** on page 128

About security settings

The **Security** settings enable you to:

- Edit the cryptography mode to configure the appliance to be compliant with Federal Information Processing Standards (FIPS) or Commercial National Security Algorithm (CNSA) standards. In these modes, the appliance uses only stronger communication protocol versions and ciphers, stronger encryption for data at rest, and stronger digital certificates. **About cryptography mode settings** provides details.
- Configure two-factor authentication.
- Generate a self-signed certificate when authentication by a certificate authority is not required or available.
- Generate a certificate signing request (CSR) for a certificate that establishes the authenticity of your public keys and verifies them through a certificate authority. **Use a certificate authority** on page 131 provides details.
- View certificate settings.
- Install an HPE public key to validate the authenticity and integrity of files delivered as part of the HPE OneView update process. If the key ever expires or is revoked, you can download the current key from **<http://www.hpe.com>** and upload it into the appliance.

About complex passwords

An Administrator can use the **Enforce complex password** option to require complex passwords for all users. When emergency local login is enabled, an Administrator is required to have a complex password. See "Enable complex passwords" in the online help.

Complex password requirements are enforced when users change their password or create user accounts.

Complex password rules apply only for the local users configured in HPE OneView. For authentication directory service users, the authentication directory configuration determines the password complexity rules.

Complex passwords must contain the following:

- Minimum of 14 characters
- Minimum of one uppercase character
- Minimum of one lowercase character
- Minimum one number
- Minimum of one special character. For example, !@#\$%^&* _-=+.,?
- No whitespace

About cryptography mode settings

You can use the **Cryptography Settings** option to configure the cryptography mode for your appliance. Available cryptography modes include:

- **Legacy:** This is the default cryptography mode. In the legacy mode all TLS protocol versions (1.0, 1.1, and 1.2) and associated cipher suites for those versions are supported. TLS certificates are not required to have FIPS or CNSA minimum key lengths nor strong digital signatures.
- **FIPS:** Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard for products performing cryptography. The FIPS 140-2 Cryptographic Module Validation Program has validated the cryptography libraries of HPE OneView. When in the FIPS mode:
 - The cryptographic modules of the appliance are configured to operate in accordance with the FIPS 140-2 level 1 specification. This setting ensures that the required FIPS self-tests are run while loading these cryptographic modules.
 - The ciphers and algorithms used for cryptographic operations by the appliance are restricted to only those approved by FIPS.
 - The appliance allows only TLS1.1 and TLS 1.2 protocols for all TLS communications.
 - All SSH and SNMPv3 communication use only cipher suites and algorithms approved by FIPS.

For additional information, see the **FIPS-140** site.

- **CNSA:** The Commercial National Security Algorithm (CNSA) cryptography mode restricts HPE OneView to use only those algorithms included in the CNSA suite. The CNSA suite is a subset of the general FIPS support and includes a set of algorithms used to protect national security systems, including information classified as 'top secret.' In the CNSA mode, the appliance uses only TLS 1.2 protocol and a CNSA-strength subset of the TLS 1.2 ciphers. Similarly, SSH and SNMP communication uses CNSA-compliant ciphers and algorithms.

For additional information, see the **CNSA standards** site. This website uses a US Government Certificate Authority-signed certificate which is not present, by default, in most browser trust stores. See **Establishing Site Trust** for more information on establishing trust with this website.

NOTE:

- In HPE OneView releases prior to version 4.0, local user passwords are hashed using SHA256. Starting with release version 4.0, the first time the user logs in, irrespective of the appliance cryptography mode, the password gets rehashed and stored as SHA384.
- When the iLO of a managed server is in the CNSA mode, the iLO user interface or console is not accessible from HPE OneView console user interface.

For a complete list of ciphers and algorithms supported in the legacy, FIPS and CNSA modes, see *Algorithm and ciphers for securing the appliance* in the *HPE OneView User Guide* available on the [Hewlett Packard Enterprise Information Library](#).

The installation scenarios and the default behavior during a mode switch are:

Fresh installation

The appliance defaults to the legacy mode.

Upgrade

Cryptography mode of the appliance prior to upgrade is retained after the upgrade. For an appliance upgraded from a release that did not support cryptography modes, the appliance is configured to be in legacy mode after the upgrade.

Factory reset

A factory reset or the Preserve network settings option does not change the cryptography mode. The cryptography mode of the appliance prior to the reset is retained. Verify that the Cryptography setting is set to required mode in the **Security** settings panel in the online help.

Backup and restore

A restore operation restores the appliance to the same cryptography mode as the backed-up appliance.

For HPE OneView to operate in FIPS or CNSA mode, it is not required that all systems or devices that are managed or monitored by HPE OneView (for example, blade iLO) or the external servers that communicate with HPE OneView (for example, Microsoft Active Directory Server) also operate in FIPS or CNSA-approved mode only. However, HPE OneView must be able to communicate with these managed or monitored devices and external servers with the protocols and cipher suites supported by the chosen mode. For example, as long as a device supports FIPS-compliant TLS protocols, ciphers and certificates, HPE OneView in FIPS or CNSA modes can manage that device.

For information on the support for various devices and supported cryptography modes, see the *HPE OneView Support Matrix* on the [Hewlett Packard Enterprise Information Library](#).

Additionally, using a higher mode of cryptography requires that you use stronger certificates for all TLS communications. For example, in the CNSA mode, managed devices using RSA certificates need a minimum key length of 3072 bits and a digital signature using SHA-384 or greater.

Not all devices that HPE OneView manages or monitors support these stronger cryptography modes. Some examples are:

- ProLiant Gen 6 systems have iLO versions that only support TLS 1.0. These servers are not supported when the appliance is in the FIPS or CNSA modes.
- ProLiant Gen7 systems have iLO versions that only support TLS 1.0 and 1.1. These servers are not supported when the appliance is in the CNSA mode.
- ProLiant Gen8 systems have iLO versions that support TLS 1.1 and 1.2, and are compatible with both FIPS and CNSA modes.

When opting for a higher security mode, use the **Compatibility report** option to get a complete report of any currently managed or monitored devices that are not compatible with the target mode.

NOTE: Changing the cryptography mode might regenerate the web server or RabbitMQ certificates. The newly generated RabbitMQ client certificate, along with the CA and key pair, must be applied to the RabbitMQ client. When using CA-signed certificates you might need to issue a new certificate signing request (CSR), obtain a stronger certificate and reimport the certificate into your appliance. Check the compatibility report for details. The appliance automatically reboots as part of configuring the appliance in a different cryptographic mode.

About directory service authentication

You can configure HPE OneView to use an external enterprise directory service for user authentication. HPE OneView supports the following enterprise directory services:

- Active Directory
- OpenLDAP

When you use a directory service, directory users are granted HPE OneView permissions using their group membership in the directory. After defining a directory service, use the **User and Groups** screen to define permissions for directory groups.

Directory groups are assigned one or more HPE OneView permissions. A directory user is assigned the HPE OneView permissions that represent the union of the permissions for all the directory groups that the user is a member of. Only after permissions are defined for directory groups, directory users are authenticated into the appliance.

Any user in the group can log into the appliance using the following steps:

1. Select the enterprise directory service in the login page.
2. Enter a *user name*. The format for the user name depends on the Directory type. Consult your HPE OneView administrator and directory administrator for the proper user name format. Valid formats include:
 - Email address. For example: `jane.larry@example.com`.
 - The down-level logon name or domain name\user logon name. For example: `example\janeL` where `example.com` is the directory domain.
 - The common name of the user (CN attribute in the directory). For example: `janeL`


NOTE:

A best practice is to set the HPE OneView display name for the directory service to match the leading part of the fully qualified domain name (*example* if there is *example.com*) directory. The format for the *user name* depends on the Directory type.

3. Enter the *password*.

Enterprise directory user in the appliance

There is no explicit user created in the appliance corresponding to the directory user. However, when a directory user is logged into the appliance, the user is identified by the user name preceded by the enterprise directory name.

In the Session control, () the user is identified by the name preceded by the enterprise directory service. For example:

```
CorpDir\pat
```



IMPORTANT: Unlike local users, if a user is deleted from an authentication directory, their active sessions remain active until that user logs out. Similarly if there is any modification of the user group in the authentication directory, that does not reflect in the currently active session for the user.

If there is a change in the group-to-role assignment (including a deletion) for an authentication directory group while a user from that group is logged in, their current active session is not affected until they log out. Local user sessions are ended when such modifications are made.

Directory server

When a directory is configured on the appliance, you can specify one or more directory servers that can be accessed for the directory service. If more than one directory server is added for a directory, they are assumed to be replicated servers for high availability or disaster tolerance. If one directory server is not reachable, the other configured servers are accessed for authenticating the user.

NOTE:

- If you use a cluster for your directory server configuration, the cluster hostname can be specified as the directory server. Hewlett Packard Enterprise recommends using a cluster for your directory server configuration instead of configuring replicated directory servers in the appliance.
- Directory search operations can be time consuming depending on your directory configuration and network latency affecting login time. When using Active Directory with many domains, for optimal login performance, configure a global catalog for your directory server.

Binding to the directory server

The appliance must bind to the directory server for performing search and authentication operations. You can choose to bind using any one of the following options:

- **Service Account:** A directory service account that has read-access permission to your directory server can be configured in the appliance. The service account takes user name and password as inputs. HPE OneView stores the credentials you provide for future use. The **Service Account** option is mandatory when **two-factor authentication** is enabled in HPE OneView.
- **User Account:** The user account uses the credentials supplied by the user while connecting HPE OneView to the directory service. The user account helps in querying the directory during the authentication process. **User Account** is the default option for directory binding. The user credentials for the directory service are not stored in HPE OneView.

User login formats used for authentication

To support user login with only the user name specified, the following formats are tried to authenticate with the directory service:

If the *user name* is not an email address (denoted by the presence of an @ character) or a \ character (to denote the *domain\user name* format), logins are attempted in the following order:

1. The *user name* is treated as the logon name, and directory-name gets prepended as *directory-name\user-name*, for example: *example\jane*.
2. The *user name* is treated as a *UID*.
3. The *user name* is treated as *Common Name (CN)*.

NOTE: If the Active Directory Server Service configured in HPE OneView has a user lock-out policy (defined, for example, on *n* number of successive failed login attempts), Hewlett Packard Enterprise recommends that you use the email or the domain\user name format to log into HPE OneView. If email or *domain\user name* format is not used (instead, just the user name is used), HPE OneView internally tries different login formats as described previously. This may result in locking out the user from the GUI on a single failed login attempt (wrong password). To minimize login attempts, configure the directory display name to be the same as the first component of the directories fully qualified domain name. For example, assign the HPE OneView name *example* for the directory *example.com*.

Trusting the directory server

Hewlett Packard Enterprise recommends that you use CA-signed certificates on your directory servers. The entire certificate chain (including the CA root and any intermediate certificates) for the directory certificate must be placed in the HPE OneView trust store before configuring the directory service. This action ensures that the appliance automatically trusts the directory server when it is configured on the appliance.

After adding an enterprise directory service and server

You can:

- Designate it as the default directory service to be used at login time.
- Disable local logins so that only users whose accounts are authenticated by the directory service can log in. Local accounts are prevented from logging in.

Configuring an enterprise directory server in HPE OneView

Consider the following points when configuring an enterprise directory server in HPE OneView:

- When HPE OneView tries to connect to a directory server, trust verification is performed using the certificates that are trusted by the appliance. Hence, import the root certificate of the directory server certificate chain into the appliance before adding the directory server.

Otherwise, you will be prompted to either add the issuing certificate or trust the self-signed certificate of the directory server.

- It is possible that the directory server might present a certificate chain that includes the server certificate, one or more Issuers, and optionally a root certificate.

If the server does not present the root certificate in the certificate chain, obtain the root certificate from the directory server administrator and import it into the appliance before adding the directory.

- If there are multiple directory servers configured under the same directory service, import all the issuer certificates (roots and intermediate CA certificates of each directory server) into the appliance before adding the directory.
- If the directory service in HPE OneView is configured with a domain name and there are multiple domain controllers in the domain that are load balanced in a round-robin fashion, import all the issuer certificates (roots and intermediate CA certificates of each domain controller) into the appliance before adding the directory.

Hostname verification when configuring and communicating to an enterprise directory server

If the directory server is set up with a CA signed certificate, HPE OneView performs hostname verification while establishing a connection. This hostname verification succeeds only when one of the following is specified in the Subject CN or the SAN field of the directory server certificate:

- A wildcard domain name. For example, *.example.com.
- Fully Qualified Domain Name (FQDN) of the directory server. For example, ad01.americas.example.com.

NOTE: If FQDN is used in the Subject CN or the SAN field, set up the DNS name resolution to resolve the FQDN to the IP address of the directory server.

- IP address of the directory server.

If these details are not mentioned correctly, an error is displayed along with the resolution.

When any of these details are mentioned, HPE OneView verifies if the details of the directory server to which the connection is being established is the same as the details specified in the Subject Common Name (Subject CN) field or the Subject Alternative Name (SAN) field of the certificate that is associated with and presented by the server.

HPE OneView does not perform hostname verification while establishing a connection if the directory server is trusted in HPE OneView using any one of the following:

- A self-signed certificate
- The **Force trust leaf certificate** option. This option can be accessed using **Settings > Security > Managed Certificates > Add Certificate**.

NOTE: Force trusting a leaf certificate is not recommended. If you use the **Force trust leaf certificate** option, only the leaf level certificate is trusted in the appliance. The leaf certificate is not subjected to revocation checks or hostname verification. Also, every time the directory server certificate is regenerated, you are required to import the new certificate into the appliance for successful communication with the directory server.

In an environment where multiple domain controllers are load balanced in a round-robin fashion, it is possible that the certificates of different domain controllers may have been signed by different intermediate CA certificates. In this case, either force trust the leaf certificates of all the domain controllers or trust all the root and intermediate CA certificates in the appliance using the **Settings > Security > Managed Certificates > Add Certificate** option.

Considerations for configuring a Microsoft Active Directory service

- For the strongest security, Hewlett Packard Enterprise recommends to configure your directory server using TLS 1.2 protocol only.
- The following maps the Active Directory attribute to the corresponding LDAP property:

LDAP property	Active Directory attribute
cn	Common-Name
uid	UID
userPrincipalName	User-Principal-Name
sAMAccountName	SAM-Account-Name

- If a user object is created in the **Active Directory Users and Computers** Microsoft Management Console, the names default as follows.

Specify the following components of the user name, displayed here with the corresponding attribute:

User name component	Attribute
First Name	givenName
Initials	initial
Last Name	sn

The field labeled `Full Name` defaults to this format. This string is assigned to the `cn` attribute (**Common Name**).

```
givenName.initials.givenName.initial.sn
```

In the **New Object – user** dialog box, you are also required to specify a **User logon name**. **User logon name**, in combination with the DNS domain name, becomes the `userPrincipalName`. The `userPrincipalName` is an alternative name that the user can use for logging in. It is in the form:

```
LogonName@DNSDomain
```

For example:

```
joeuser@example.com
```

- Finally, as you enter the **User logon name**, the first 20 characters are automatically filled in the **pre-Windows 2000 logon name** field, which becomes the `sAMAccountName` attribute.
- CN-logins for built-in Active Directory user accounts, like `Administrator`, are not accepted. Other login formats are acceptable if their respective attributes (`sAMAccountName`, `userPrincipalName`, and `UID`) are set properly.

Enable cross-domain authentication using the global catalog

If your enterprise directory environment has multiple trusted domains where user accounts or directory groups are defined in different domains, connecting to the local domain does not locate the membership of the user in groups outside the domain.

When configuring multidomain directories in HPE OneView, use the Active Directory Global Catalog to allow HPE OneView to perform group membership lookup across domains.

Use the following steps to enable cross-domain authentication in HPE OneView using the Global Catalog:

NOTE: This scenario assumes that there are two trusted domains, **region1** and **region2**. If the user in **region1** belongs to a group in **region2**, Active Directory is configured as described in this procedure to enable user authentication.

Prerequisites

Privileges: Infrastructure administrator.

Procedure

1. From the main menu, select **Settings**.
2. Either click the **Edit** icon in the **Security** panel, or select **Actions > Edit**.
3. On the **Edit Security** screen, under **Directories**, click **Add Directory**.
4. Enter the data requested on the **Add/Edit Directory** screen.

Define the directory configuration specifying the parent domain as the value for **Base Distinguished Name (Base DN)**. For example, for trusted domains, **region1.example.com** and **region2.example.com**, specify the directory name as **example**, and the **Base DN** value as **DC=example** or **DC=com**.

5. Click **Add directory server**. For **Directory server port**, enter the Global Catalog SSL port. The default port is 3269.
6. When adding directory groups on the **Users and Groups** screen, specify the directory groups from either **region1.example.com**, or **region2.example.com** in the **Add group** screen.
7. To verify cross-domain authentication, log in as **user@domain** or **domain\user**. For example, **admin@example.com**, **region1\admin**, or **admin**.

About emergency local login

When configured to use a directory service, administrators can choose to disable local logins for improved security. If the local logins are disabled and directory service is unavailable, users cannot log in to the appliance. Under these circumstances, if permitted by your security policies and HPE OneView configuration, the emergency local login option allows an Administrator to log in to the appliance.

To enable emergency local login, see "Enable emergency local login" in the online help.

NOTE: If local login is disabled when upgrading to the HPE OneView, emergency local login is automatically enabled.

By default, emergency local login is restricted to the appliance console, but can be configured to allow web-based login.

The Administrator account must have a complex password when emergency local login is enabled for security purposes. You can enable **Enforce complex passwords** to ensure that all local accounts have strong passwords, including the Administrator account. The password complexity is enforced the next time that the account password is changed.

Hewlett Packard Enterprise recommends that you change the Administrator password immediately after enabling emergency local login. See **About complex passwords** on page 75.

About permissions

Permissions are used to control a user's access to the appliance and the resources managed by the appliance. Permissions consist of a role and an optional scope. The permission role grants the user access to resource categories. For example, the Server administrator role grants read, create, delete, update and use rights to the server hardware category. Specifying a permission scope further restricts the rights granted by the role to a subset of instances within a resource category. For example, scope can be used to restrict the server hardware rights granted by the Server administrator role to only the servers in the Test scope.

A user or group may be assigned multiple permissions. Use the screen to manage the permissions assigned to a user or group. See "Users and Groups" in the online help for information about managing the permissions assigned to a user or a group.

You create a login session when you log in to the appliance through the browser. On login, the session grants the user all permissions assigned by the Infrastructure Administrator.

A user granted multiple permissions can disable certain permissions. When operating with reduced permissions, the user is only allowed to perform actions authorized for the selected permission.

Allowing a user to operate in a least privilege mode is a security best practice. It allows the user to reduce the risk of making an unintended change.

Use the **Change permission dialog** to enable or disable session permissions. For information about the Change permission dialog, see the online help.

About scopes

A scope is a grouping of resources that can be used to restrict the range of an operation or action. For example, you can create scopes based on:

- Organization or department (Marketing, Research and Development, Finance)
- Usage (Production, Development, Testing)
- Skills (Linux, Windows)

For example, a data center could be organized so that all servers running Linux are monitored using one scope and all servers running MS Windows are monitored using another scope. Email notifications can be configured such that Windows technicians are notified for issues on the servers running Windows and Linux technicians are notified for issues on the servers running Linux.

When scopes are defined and resources assigned to them, you can:

- Restrict the resources displayed in the user interface (UI) to those assigned to the scope.
- Restrict user permissions to grant access only to the resources in a scope.
- Configure filtered email notifications for alerts based on previously-defined scopes.

Scope-enabled resource categories on page 118 lists the categories of resources that can be added to a scope. Some categories of resources cannot be added to a scope.

About trusting certificates

When adding a managed device, such as an iLO or a remote server -- the SSL certificate if associated with the managed device or remote server -- is fetched and displayed in a dialog box. Review the details of the fetched certificate and trust the certificate. Once you trust the certificate, it is added to the appliance trust store. All communication from HPE OneView to the managed device/remote server makes use of the trusted certificate. The same capability is available via REST API.

To review certificates, view the manage certificates screen in the online help.

HPE suggests replacing the self-signed certificate with a commercially signed CA certificate.

About user accounts

Authentication

HPE OneView supports both local and directory-based authentication. With local authentication, the authentication directory is hosted locally on the appliance. With directory-based authentication, an external directory service is used to authenticate access.

By default, HPE OneView is configured with a single local user account named `Administrator`. An `Administrator` is a person who is assigned to do a first time set up in HPE OneView and has full rights. The default password for this local administrator account is `admin`. This password must be changed at first login. The administrator login for the appliance is automatically assigned with full access (Infrastructure administrator) privileges, after the first login.

NOTE:

- You cannot rename the `Administrator` login name.
- Only an `Administrator` can change the password for the administrator account. The `Administrator` can use the following options to change the password:
 - If you remember the current password: Use **User and Groups > Actions > Edit** to update the password.
 - If you have forgotten the current password: Use **Maintenance Console >** Reset the administrator password option.
- You can create another user with an `Infrastructure Admin` role. However, an `Infrastructure Admin` cannot delete or edit the `Administrator` user.

You can use an external authentication directory service (also called an enterprise directory or authentication login domain) to grant permissions for groups of users instead of maintaining individual local login accounts. Each user in a group is assigned the same permission. An example of an authentication directory service is a corporate directory that uses LDAP (Lightweight Directory Access Protocol). Hewlett Packard Enterprise recommends limiting the number of local accounts by integrating the appliance with an enterprise directory solution such as Microsoft Active Directory or OpenLDAP.

See **About directory service authentication** on page 78 and **About emergency local login** on page 83 for additional considerations.

Authorization

Roles

HPE OneView defines a set of roles that describe the actions a user can perform on resource categories. When assigned to a user or directory group, a role grants the right to perform actions on categories of resources managed by the appliance.

Scopes

A scope is a user-defined set of resources. A resource can belong to multiple scopes.

Permissions

Permissions are used to control user access to the appliance and the resources managed by the appliance. The `Infrastructure administrator` grants rights to users and directory groups by assigning permissions. A permission consists of a role and an optional scope. The role grants access to resource categories. The scope further restricts the rights granted by the role to a subset of instances in the resource category. If a permission is not restricted by scope, the rights granted by the role apply to all resources managed by the appliance. Users and groups can be assigned multiple permissions.

NOTE: If the `Infrastructure Administrator` changes permissions while a user is logged on:

- Local users are logged out. The changed permissions are reflected the next time the user logs in.
- Enterprise Directory users can continue operating under the old permissions until they log out. The changed permissions are reflected the next time the user logs in.

You can (full access user) or (role-based specialist). For each of these users, authentication is confirmed by comparing the user login information to an authentication directory hosted locally on the appliance.

You can (full access user) or (role-based specialist). For each of these users, authentication is confirmed by comparing the user login information to an enterprise directory.

By default, the **Dashboard** displays status of the most relevant resources that are associated with assigned user roles. If you are assigned multiple roles, such as `Network` and `Storage` roles, the dashboard displays the combination of resources that each role would see on the dashboard. HPE OneView defines a set of roles that describe the actions a user can perform on resource categories. When assigned to a user or directory group, a role grants the right to perform actions on categories of resources managed by the appliance.

About user roles

User roles enable you to assign permissions and privileges to users based on their job responsibilities. You can assign full privileges to a user, or you can assign a subset of permissions to view, create, edit, or remove resources managed by the appliance.

Table 1: User role permissions

Role	Type of user	Permissions or privileges
Full	Infrastructure administrator	<p>View, create, edit, or remove resources managed or monitored by the appliance, including management of the appliance, through the UI or using REST APIs.</p> <p>An Infrastructure administrator can also manage information provided by the appliance in the form of activities, notifications, and logs.</p> <p>Only an Infrastructure administrator can restore an appliance from a backup file.</p>
Read only	Read only	<p>View managed or monitored resource information.</p> <p>Cannot add, create, edit, remove, or delete resources.</p>
Specialized	Backup administrator	<p>Create and download backup files, view the appliance settings and activities.</p> <p>Has the authority to use scripts to log in to the appliance and run scripts to back up the appliance.</p> <p>Cannot restore the appliance from a backup file.</p> <p>NOTE: This role is intended for scripts using REST APIs to log into the appliance to perform scripted backup creation and download so that you do not expose the Infrastructure administrator credentials for backup operations.</p> <p>Hewlett Packard Enterprise recommends that users with this role should not initiate interactive login sessions through the HPE OneView user interface.</p>
	Network administrator	<p>View, create, edit, or remove networks, network sets, connections, interconnects, uplink sets, and firmware bundles.</p> <p>View related activities, logs, and notifications.</p> <p>Cannot manage user accounts.</p>

Table Continued

Role	Type of user	Permissions or privileges
	Server administrator	<p>View, create, edit, or remove server profiles and templates, network sets, enclosures, and firmware bundles.</p> <p>Access the Onboard Administrator and physical servers, and hypervisor registration.</p> <p>View connections, networks, racks, power, and related activities, logs, and notifications.</p> <p>Add volumes, but cannot add storage pools or storage systems.</p> <p>Cannot manage user accounts.</p>
	Server firmware operator	<p>View managed or monitored resource information.</p> <p>Access the physical servers.</p> <p>Edit, but not create or delete, physical servers.</p> <p>Edits the server hardware, firmware baseline, firmware installation method, and activation schedule values on server profiles.</p>
	Server profile architect	<p>Create and manage server profiles, server profile templates, storage volumes, labels, and network sets.</p> <p>Use networks, enclosures, firmware drivers, server hardware, storage pools, and storage volume templates.</p>
	Server profile administrator	<p>Create and manage server profiles, storage volumes, labels, and network sets.</p> <p>Use networks, enclosures, firmware drivers, server hardware, server profile templates, storage pools, and storage volume templates.</p>
	Server profile operator	<p>Create, delete, and update labels.</p> <p>Update server hardware, and server profiles</p> <p>Use networks, network sets, enclosures, firmware drivers, server hardware, server profiles, storage pools, and storage volume templates.</p>
	Scope administrator	<p>Create and delete scopes.</p> <p>Update scopes, add, and remove scope resources.</p> <p>Cannot modify any resource other than scopes.</p>

Table Continued

Role	Type of user	Permissions or privileges
	Scope operator	Update scopes, add, and remove scope resources. Cannot modify any resource other than scopes. Cannot create or delete scopes.
	Storage administrator	View, add, edit, or remove storage systems. View or edit storage pools. View, create, edit, add, or delete volumes. View, create, edit, or delete volume templates. View, add, or edit SAN managers. View or edit SANs.

Action privileges for user roles

The following tables list the user action privileges associated with each user role.

The **Use** privilege is a special case that allows you to associate objects to objects that you own but you are not allowed to change. For example, in a logical interconnect group, a user assigned the role of Server administrator is not allowed to define logical interconnect groups, but can use them when adding an enclosure.

Table 2: Action privileges for user roles

Category	Action privileges for user roles					
	IA=Infrastructure administrator, admin=administrator					
	(C=Create, R=Read, U=Update, D=Delete, Use)					
	IA	Server admin	Network admin	Backup admin	Storage admin	Software admin
activities	CRUD	CRU	CRU	R	CRU	CRU
alerts	RUD	RUD	RUD	—	RUD	RUD
appliance	CRUD	R	R	R	R	R
audit logs	CR	R	R	—	R	—
backups	CRUD	R	R	CRD	R	R
certificates	CRUD	—	—	—	—	—
community string	RU	R	CRU	—	R	R

Table Continued

Category	Action privileges for user roles					
	IA=Infrastructure administrator, admin=administrator					
	(C=Create, R=Read, U=Update, D=Delete, Use)					
	IA	Server admin	Network admin	Backup admin	Storage admin	Software admin
connections	CRUD	R	CR	R	R	R
connection templates	CRUD, Use	R, Use	CRUD	R	R	R
console users	CRUD	—	—	—	—	—
data centers	CRUD	CRUD	R	R	R	R
debug logs	CRUD	CRU	CRU	—	R	CRU
device bays	CRUD	CRUD	R	R	R	R
domains	CRUD	R	CRU	R	R	R
enclosures	CRUD	CRUD	R	R	R	R
enclosure groups	CRUD, Use	CRUD, Use	R	R	R	R
Ethernet networks	CRUD	R	CRUD	R	R	R
events	CRU	CRU	CRU	—	R	CRU
fabrics	RUD ¹	R	RUD	R	R	R
FC aliases	CRUD	R	R	R	CRUD	R
FC device managers	CRUD	R	R	R	CRUD	R
FC endpoints	R	R	R	R	R	R
FC networks	CRUD	R	CRUD	R	R	R
FCOE networks	CRUD, Use	R	CRUD, Use	R	R	R
FC ports	R	R	R	R	R	R
FC providers	R	R	R	R	R	R
FC SANs	CRUD	R	R	R	CRUD	R

Table Continued

Category	Action privileges for user roles					
	IA=Infrastructure administrator, admin=administrator					
	(C=Create, R=Read, U=Update, D=Delete, Use)					
	IA	Server admin	Network admin	Backup admin	Storage admin	Software admin
FC SAN services	CRUD	R	R	R	CRUD	R
FC switches	R	R	R	R	R	R
FC tasks	R	R	R	R	R	R
FC zones	CRUD	R	R	R	CRUD	R
firmware drivers	CRUD	CRUD	CRUD	R	R	R
global settings	CRUD	CRUD	CRUD	R	CRUD	CRUD
group or role mappings	CRUD	—	—	—	R	—
hosts	CRUD	R	R	R	R	—
host clusters	CRUD	R	R	R	R	—
ID range ipv4	CRUD	RU	CRUD	R	R	R
ID range ipv4 subnet	CRUD	RU	CRUD	R	R	R
ID range vmacs (MAC addresses)	CRUD	R	CRU	R	R	R
ID range vsns (serial numbers)	CRUD	CRU	R	R	R	R
ID range vwwns (World Wide Names)	CRUD	R	CRU	R	R	R
infrastructure vms	CRUD	CRUD	R	R	R	R
integrated tools	CRUD	R	R	R	R	R
interconnects	CRUD	CR	CRUD	R	R	R
interconnect types	R, Use	R	CRUD	R	R	R

Table Continued

Category	Action privileges for user roles					
	IA=Infrastructure administrator, admin=administrator					
	(C=Create, R=Read, U=Update, D=Delete, Use)					
	IA	Server admin	Network admin	Backup admin	Storage admin	Software admin
labels	CRUD	CRUD	CRUD	R	CRUD	CRUD
licenses	CRUD	CR	R	R	R	R
logical downlinks	R	R	R	R	R	R
logical enclosures	CRUD, Use	CRUD, Use	R, Use	R	R, Use	R, Use
logical interconnects	RU, Use	R, Use	RU, Use	R	R	R
logical interconnects groups	CRUD, Use	R, Use	CRUD, Use	R	R	R
logical switches	—	—	—	—	—	—
login domains	CRUD	—	—	—	R	R
login sessions	CRUD	RU	RU	RU	RU	—
managed SANs	CRUD, Use	R	R, Use	R	CRUD, Use	—
migratable VC domains	CRUD, Use	—	—	—	—	R
networks	CRUD, Use	R, Use	CRUD, Use	R	R	—
network sets	CRUD, Use	CRUD ²	CRUD	R	R	R
notifications	CRUD	CRD	CRD	R	R	—
organizations	CRUD	—	—	—	R	—
ports	RU, Use	—	RU, Use	—	R	R
power devices	CRUD	CRUD	R	R	R	R
racks	CRUD	CRUD	R	R	R	R
reports	R	R	R	R	R	R

Table Continued

Category	Action privileges for user roles					
	IA=Infrastructure administrator, admin=administrator					
	(C=Create, R=Read, U=Update, D=Delete, Use)					
	IA	Server admin	Network admin	Backup admin	Storage admin	Software admin
repository manager	CRUD	CRUD	CRUD	R	R	R
restores	CRUD	—	—	—	—	—
roles	CRUD	—	—	—	—	—
SANS	CRUD, Use	R	R	R	CRUD, Use	—
SAN manager	CRUD, Use	R	R	R	CRUD, Use	—
scopes	CRUD, Use	R	R	R	R	R
server hardware	CRUD, Use	CRUD, Use	R	R	R	R
server hardware types	CRUD, Use	CRUD, Use	R	R	R	R
server profiles	CRUD	CRUD	R	R	R	R
server profile templates	CRUD, Use	CRUD, Use	—	R	R	R
storage pools	RU	R	R	R	RU	R
storage systems	CRUD	R	R	R	CRUD	R
storage target ports	CRUD	R	R	R	CRUD	R
storage volumes	CRUD	CRUD	R	R	CRUD	R
storage volume attachments	CRUD	CRUD	R	R	CRUD	R
storage volumes templates	CRUD	R	R	R	CRUD	R
storage volume sets	R	R	R	R	R	R
support	CRUD, Use	R, Use	R	R	R, Use	R, Use

Table Continued

Category	Action privileges for user roles					
	IA=Infrastructure administrator, admin=administrator					
	(C=Create, R=Read, U=Update, D=Delete, Use)					
	IA	Server admin	Network admin	Backup admin	Storage admin	Software admin
switches	CRUD, Use	RU	CRUD	R	R	R
tasks	R	R	R	R	R	R
trap forwarding	RU	R	R	R	R	R
unmanaged devices	CRUD	CRUD	R	R	R	R
update	R	—	—	—	—	—
uplink sets	CRUD	R	CRUD	R	R	R
users	CRUD	—	—	—	—	—
user preferences	CRUD	—	—	—	—	—

¹ Fabric is claimed when HPE OneView and HPE Composable Fabric Manager are configured together.

² Server administrators cannot edit bandwidths.

Table 3: Action privileges for specialized user roles

Category	Action privileges for specialized user roles						
	IA=Infrastructure administrator, admin=administrator						
	(C=Create, R=Read, U=Update, D=Delete, Use)						
	Read only	Scope admin	Scope operator	Server firmware operator	Server profile architect	Server profile admin	Server profile operator
activities	R	R	R	R	R	R	R
alerts	R	R	R	R	R	R	R
appliance	R	R	R	R	R	R	R
audit logs	—	—	—	—	—	—	—
backups	R	R	R	R	R	R	R
certificates	R	R	R	R	R	R	R

Table Continued

Category	Action privileges for specialized user roles						
	IA=Infrastructure administrator, admin=administrator						
	(C=Create, R=Read, U=Update, D=Delete, Use)						
	Read only	Scope admin	Scope operator	Server firmware operator	Server profile architect	Server profile admin	Server profile operator
community string	—	—	—	—	—	—	—
connections	R	R	R	R	R	R	R
connection templates	R	R	R	R	R	R	R
console users	—	—	—	—	—	—	—
data centers	R	R	R	R	R	R	R
debug logs	R	R	R	R	R	R	R
device bays	R	R	R	R	R	R	R
domains	R	R	R	R	R	R	R
enclosures	R	R, Use	R, Use	R	R, Use	R, Use	R, Use
enclosure groups	R	R, Use	R	R	R	R, Use	R, Use
enclosure types							
Ethernet networks	R	R, Use	R, Use	R	R, Use	R, Use	R, Use
events	R	R	R	R	R	R	R
fabrics	R	R	R	R	R	R	R
FC aliases	R	R	R	R	R	R	R
FC device managers	R	R	R	R	R	R	R
FC endpoints	R	R	R	R	R	R	R
FC networks	R	R, Use	R, Use	R	R, Use	R, Use	R, Use
FCOE networks	R	R, Use	R, Use	R	R, Use	R, Use	R, Use

Table Continued

Category	Action privileges for specialized user roles						
	IA=Infrastructure administrator, admin=administrator						
	(C=Create, R=Read, U=Update, D=Delete, Use)						
	Read only	Scope admin	Scope operator	Server firmware operator	Server profile architect	Server profile admin	Server profile operator
FC ports	R	R	R	R	R	R	R
FC providers	R	R	R	R	R	R	R
FC SANs	R	R	R	R	R	R	R
FC SAN services	R	R	R	R	R	R	R
FC switches	R	R	R	R	R	R	R
FC tasks	R	R	R	R	R	R	R
FC zones	R	R	R	R	R	R	R
firmware drivers	R	R, Use	R, Use	R	R, Use	R, Use	R, Use
global settings	R	R	R	R	R	R	R
group to role mappings	R	R	R	R	R	R	R
hosts	R	R	R	R	R	R	R
ID range vmacs (MAC addresses)	R	R	R	R	R	R	R
ID range vsns (serial numbers)	R	R	R	R	R	R	R
ID range vwwn (World Wide Names)	R	R	R	R	R	R	R
infrastructure vms	R	R	R	R	R	R	R
integrated tools	R	R	R	R	R	R	R
interconnects	R	R, Use	R, Use	R	R	R	R
interconnect types	R	R	R	R	R	R	R

Table Continued

Category	Action privileges for specialized user roles						
	IA=Infrastructure administrator, admin=administrator						
	(C=Create, R=Read, U=Update, D=Delete, Use)						
	Read only	Scope admin	Scope operator	Server firmware operator	Server profile architect	Server profile admin	Server profile operator
labels	R	R	R	R	CRUD	CRUD	CRUD
licenses	R	R	R	R	R	R	R
logical downlinks	R	R	R	R	R	R	R
logical enclosures	R	R, Use	R, Use	R	R	R	R
logical interconnects	R	R, Use	R, Use	R	R	R	R
logical interconnect groups	R	R, Use	R, Use	R	R, Use	R, Use	R
logical switch groups	R	R, Use	R, Use	R	R	R	R
logical switches	R	R, Use	R, Use	R	R	R	R
login domains	R	R	R	R	R	R	R
login sessions	RU	R	R	R	RU	RU	RU
managed SANs	R	—	—	R	R	R	R
migratable VC domains	—	—	—	—	—	—	—
networks	R	R	R	R	R	R	R
network sets	R	R, Use	R, Use	R	CRUD, Use	CRUD, Use	R, Use
notifications	R	R	R	R	R	R	R
organizations	R	R	R	R	R	R	R
ports	—	R		—	—	—	—
power devices	R	R	R	R	R	R	R

Table Continued

Category	Action privileges for specialized user roles						
	IA=Infrastructure administrator, admin=administrator						
	(C=Create, R=Read, U=Update, D=Delete, Use)						
	Read only	Scope admin	Scope operator	Server firmware operator	Server profile architect	Server profile admin	Server profile operator
racks	R	R	R	RU, Use	R	R	R
reports	R	R	R	R	R	R	R
repository manager	—	R	R	R	R	R	R
restores	R	R	R	R	R	R	R
roles	R	R	R	R	R	R	R
SANs	R	—	—	R	R	R	R
SAN manager	R	—	—	R	R	R	R
scopes	R	CRUD	RU	R	R	R	R
server hardware	R	R, Use	R, Use	RU, Use	RU, Use	RU, Use	RU, Use
server hardware types	R	R	R	R	R	R	R
server profiles	R	R, Use	R, Use	RU ¹	CRUD	CRUD	RU, Use
server profile templates	R	R	R	R	CRUD, Use	R, Use	R
storage pools	R	R, Use	R, Use	R	R, Use	R, Use	R, Use
storage systems	R	R	R	R	R	R	R
storage target ports	R	R	R	R	R	R	R
storage volumes	R	R, Use	R, Use	R	CRUD, Use	CRUD, Use	R, Use
storage volume attachments	R	R	R	R	R	R	R
storage volume templates	R	R, Use	R, Use	R	R, Use	R, Use	R, Use
support	—	R	R	R	R	R	R

Table Continued

Category	Action privileges for specialized user roles						
	IA=Infrastructure administrator, admin=administrator						
	(C=Create, R=Read, U=Update, D=Delete, Use)						
	Read only	Scope admin	Scope operator	Server firmware operator	Server profile architect	Server profile admin	Server profile operator
switches	R	R, Use	R, Use	R	R	R	R
switch domains	R	R	R	—	R	R	R
switch groups	R	R	R	R	R	R	R
tasks	R	R	R	R	R	R	R
trap forwarding	R	R	R	R	R	R	R
unmanaged devices	R	R	R	R	R	R	R
update	R	R	R	—	R	R	R
uplink sets	R	R	R	R	R	R	R
users	R	R	R	—	R	R	R
user preferences	R	R	R	—	R	R	R

¹ Server firmware operator can only update `manageFirmware`, `firmwareBaseline`, `forceInstallFirmware`, `firmwareInstallType`, `firmwareActivationType` and `serverHardwareUri` attributes.

Algorithms, cipher suites, and protocols for securing the appliance

NOTE: FIPS 140-2 and CNSA applies only to a VM appliance managing non-c7000 hardware.

HPE OneView offers options to configure management appliances to be compliant with the Federal Information Processing Standard FIPS-140-2 (FIPS 140-2) and Commercial National Security Algorithm (CNSA) standards or to continue using the legacy cryptography mode. In the FIPS 140-2 and CNSA modes, the appliance restricts protocol versions, cipher suites, and digital certificate strength to FIPS 140-2 and CNSA-compliant ones, respectively.

About cryptography mode settings provides details.

NOTE: Turning on FIPS may disable old APIs that are incompatible with the heightened security mode.

The CNSA-compliant cipher suites are a subset of the FIPS-compliant cipher suites that meet the more stringent security requirements of the CNSA specifications.

HPE OneView uses the following FIPS 140-2-validated modules for cryptographic operations:

- Hewlett Packard Enterprise SSL Cryptographic Module (Certificate number 3018)
- Hewlett Packard Enterprise NSS Cryptographic Module (Certificate number 2908)
- Hewlett Packard Enterprise Libgcrypt Cryptographic Module (Certificate number 2915)
- Hewlett Packard Enterprise Java Cryptographic Module (Certificate number 3138)

HPE OneView uses the following communication protocols and services that rely on the FIPS-validated cryptographic modules:

- Transport Layer Security (TLS) communication
 - OpenSSL, Apache, and Curl: Uses underlying FIPS 140-2-validated OpenSSL Cryptographic Module
 - Java: Uses underlying FIPS 140-2-validated Java Cryptographic Module
 - RabbitMQ: Uses underlying FIPS 140-2-validated OpenSSL Cryptographic Module
 - Firefox: Uses underlying FIPS 140-2-validated NSS Cryptographic Module
 - Digital signature algorithms: Uses underlying FIPS 140-2-validated OpenSSL and Java Cryptographic Modules
 - Public key algorithms: Uses underlying FIPS 140-2-validated OpenSSL and Java Cryptographic Modules
- SNMP communication:
 - Server management: Uses SNMP4J libraries for SNMP communications. SNMP4J uses standard JCE hashing and encryption algorithms provided by the FIPS 140-2-validated Java Cryptography Extension (JCE).
 - Interconnect management: Uses underlying FIPS-140-2-validated OpenSSL Cryptographic Module
- SSH communication
 - OpenSSH: Uses underlying FIPS 140-2 validated OpenSSL Cryptographic Module
- RPM signature validation: Uses underlying FIPS 140-2-validated Libgcrypt Cryptographic Module

A cipher suite is a set of algorithms that help secure a network connection that uses TLS for communication. The set of algorithms that cipher suites usually contain include: a key exchange algorithm, a bulk encryption algorithm, and a Message Authentication Code (MAC) algorithm.

This unit covers the following:

- **Protocols supported by the appliance**
- **Algorithms and cipher suites supported in legacy mode**
- **Algorithms and cipher suites supported in FIPS 140-2 mode**
- **Algorithms and cipher suites supported in CNSA mode**

NOTE: The cipher suites used in the FIPS 140-2 mode are a subset of the cipher suites used in the legacy mode that comply with the security strength requirements of the FIPS 140-2 mode. And, the cipher suites used in the CNSA mode are a subset of the FIPS 140-2 mode cipher suites that comply with the more stringent security requirements of the CNSA mode. HPE OneView gives preference to stronger protocols and cipher suites even in the legacy mode. However, depending on the protocol and cipher suite supported by the device, server or browser, the appliance allows communication with a lower strength protocol or cipher suite in the legacy mode.

Listed here are some of the common cryptographic algorithms and the functions they perform:

Algorithm	Function
Advanced Encryption Standard (AES)	Symmetric block cipher to protect information
Elliptic Curve Diffie Hellman (ECDH) Key Exchange	Asymmetric algorithm to establish keys
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm to verify digital signatures
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm to establish keys
RSA	Asymmetric algorithm to establish keys and digital signatures
Secure Hash Algorithm (SHA)	Algorithm to compute a condensed representation of information

Protocols supported by the appliance

The Transport Layer Security (TLS) protocols supported in the various cryptographic modes include:

- **Legacy mode:** TLS 1.0, TLS 1.1, and TLS 1.2
- **FIPS 140-2 mode:** TLS 1.1 and TLS 1.2
- **CNSA mode:** TLS 1.2

NOTE: To enable or disable a specific protocol on the appliance, use the REST API PUT `/rest/security-standards/protocol`. See the *HPE OneView API Reference* for more information.

Algorithms and cipher suites supported in legacy mode

This unit covers:

- **Legacy mode cipher suites for TLS**
- **Legacy mode cipher suites for SSH**
- **Legacy mode cipher suites for SNMP**

Legacy mode cipher suites for TLS

Table 4: OpenSSL, Apache, and Curl cipher suites

Cipher suite hex code	Cipher suite name
[0xc024]	ECDHE-ECDSA-AES256-SHA384
[0xc02c]	ECDHE-ECDSA-AES256-GCM-SHA384
[0xc014]	ECDHE-RSA-AES256-SHA
[0xc028]	ECDHE-RSA-AES256-SHA384
[0xc030]	ECDHE-RSA-AES256-GCM-SHA384
[0xc026]	ECDH-ECDSA-AES256-SHA384
[0xc02e]	ECDH-ECDSA-AES256-GCM-SHA384
[0xc02a]	ECDH-RSA-AES256-SHA384

Table Continued

[0xc032]	ECDH-RSA-AES256-GCM-SHA384
[0x6b]	DHE-RSA-AES256-SHA256
[0x9f]	DHE-RSA-AES256-GCM-SHA384
[0x3d]	AES256-SHA256
[0x9d]	AES256-GCM-SHA384
[0xc023]	ECDHE-ECDSA-AES128-SHA256
[0xc02b]	ECDHE-ECDSA-AES128-GCM-SHA256
[0xc027]	ECDHE-RSA-AES128-SHA256
[0xc02f]	ECDHE-RSA-AES128-GCM-SHA256
[0x67]	DHE-RSA-AES128-SHA256
[0xc013]	ECDHE-RSA-AES128-SHA
[0xc025]	ECDH-ECDSA-AES128-SHA256
[0x9e]	DHE-RSA-AES128-GCM-SHA256
[0xc02d]	ECDH-ECDSA-AES128-GCM-SHA256
[0xc029]	ECDH-RSA-AES128-SHA256
[0xc031]	ECDH-RSA-AES128-GCM-SHA256
[0x3c]	AES128-SHA256
[0x9c]	AES128-GCM-SHA256
[0xa3]	DHE-DSS-AES256-GCM-SHA384
[0xa2]	DHE-DSS-AES128-GCM-SHA256
[0x39]	DHE-RSA-AES256-SHA
[0x33]	DHE-RSA-AES128-SHA
[0x35]	AES256-SHA
[0x2f]	AES128-SHA
[0xc00e]	ECDH-RSA-AES128-SHA
[0xc00a]	ECDHE-ECDSA-AES256-SHA
[0xc005]	ECDH-ECDSA-AES256-SHA
[0xc009]	ECDHE-ECDSA-AES128-SHA
[0xc004]	ECDH-ECDSA-AES128-SHA
[0xc003]	ECDH-ECDSA-DES-CBC3-SHA
[0xc008]	ECDHE-ECDSA-DES-CBC3-SHA
[0xc012]	ECDHE-RSA-DES-CBC3-SHA
[0xc00d]	ECDH-RSA-DES-CBC3-SHA

Table 5: Java cipher suites

Cipher suite hex code	Cipher suite name
[0xc024]	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
[0xc02c]	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
[0xc014]	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
[0xc028]	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
[0xc030]	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
[0xc026]	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
[0xc02e]	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
[0xc02a]	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
[0xc032]	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
[0x6b]	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
[0x9f]	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
[0x3d]	TLS_RSA_WITH_AES_256_CBC_SHA256
[0x9d]	TLS_RSA_WITH_AES_256_GCM_SHA384
[0xc023]	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
[0xc02b]	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
[0xc027]	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
[0xc02f]	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
[0x67]	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
[0xc013]	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
[0xc025]	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
[0x9e]	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
[0xc02d]	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
[0xc029]	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
[0xc031]	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
[0x3c]	TLS_RSA_WITH_AES_128_CBC_SHA256
[0x9c]	TLS_RSA_WITH_AES_128_GCM_SHA256
[0xa2]	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
[0xa3]	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
[0x33]	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
[0x35]	TLS_RSA_WITH_AES_256_CBC_SHA
[0x2f]	TLS_RSA_WITH_AES_128_CBC_SHA
[0x39]	TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Table Continued

[0xc00e]	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
[0xc009]	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
[0xc004]	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
[0x40]	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
[0xc005]	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
[0x32]	TLS_DHE_DSS_WITH_AES_128_CBC_SHA
[0xc00f]	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
[0x6a]	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
[0xc00a]	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
[0x38]	TLS_DHE_DSS_WITH_AES_256_CBC_SHA
[0xc003]	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
[0xc008]	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
[0xc012]	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
[0xc00d]	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
Not applicable	SSL_RSA_WITH_3DES_EDE_CBC_SHA
Not applicable	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Not applicable	SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

Table 6: RabbitMQ cipher suites

Cipher suite hex code	Cipher suite name
[0xc024]	ecdhe_ecdsa,aes_256_cbc,sha384,sha384
[0xc014]	ecdhe_rsa,aes_256_cbc,sha
[0xc028]	ecdhe_rsa,aes_256_cbc,sha384,sha384
[0xc026]	ecdh_ecdsa,aes_256_cbc,sha384,sha384
[0xc02a]	ecdh_rsa,aes_256_cbc,sha384,sha384
[0xc02c]	ecdhe_ecdsa,aes_256_gcm,null,sha384
[0xc030]	ecdhe_rsa,aes_256_gcm,null,sha384
[0xc02e]	ecdh_ecdsa,aes_256_gcm,null,sha384
[0xc032]	ecdh_rsa,aes_256_gcm,null,sha384
[0x6b]	dhe_rsa,aes_256_cbc,sha256
[0x9f]	dhe_rsa,aes_256_gcm,null,sha384
[0x3d]	rsa,aes_256_cbc,sha256
[0x9d]	rsa,aes_256_gcm,null,sha384
[0xc023]	ecdhe_ecdsa,aes_128_cbc,sha256,sha256
[0xc02b]	ecdhe_ecdsa,aes_128_gcm,null,sha256

Table Continued

[0xc027]	ecdhe_rsa,aes_128_cbc,sha256,sha256
[0xc02f]	ecdhe_rsa,aes_128_gcm,null,sha256
[0x67]	dhe_rsa,aes_128_cbc,sha256
[0xc013]	ecdhe_rsa,aes_128_cbc,sha
[0xc025]	ecdh_ecdsa,aes_128_cbc,sha256,sha256
[0x9e]	dhe_rsa,aes_128_gcm,null,sha256
[0xc02d]	ecdh_ecdsa,aes_128_gcm,null,sha256
[0xc029]	ecdh_rsa,aes_128_cbc,sha256,sha256
[0xc031]	ecdh_rsa,aes_128_gcm,null,sha256
[0x3c]	rsa,aes_128_cbc,sha256
[0x9c]	rsa,aes_128_gcm,null,sha256
[0xa3]	dhe_dss,aes_256_gcm,null,sha384
[0xa2]	dhe_dss,aes_128_gcm,null,sha256
[0x39]	dhe_rsa,aes_256_cbc,sha
[0x33]	dhe_rsa,aes_128_cbc,sha
[0x35]	rsa,aes_256_cbc,sha
[0x2f]	rsa,aes_128_cbc,sha
[0xc00e]	ecdh_rsa,aes_128_cbc,sha
[0xc00a]	ecdhe_ecdsa,aes_256_cbc,sha
[0xc005]	ecdh_ecdsa,aes_256_cbc,sha
[0xc00f]	ecdh_rsa,aes_256_cbc,sha
[0xc009]	ecdhe_ecdsa,aes_128_cbc,sha
[0xc004]	ecdh_ecdsa,aes_128_cbc,sha
[0xc003]	ecdh_ecdsa,'3des_edc_cbc',sha
[0xc008]	ecdhe_ecdsa,'3des_edc_cbc',sha
[0xc012]	ecdhe_rsa,'3des_edc_cbc',sha
[0xc00d]	ecdh_rsa,'3des_edc_cbc',sha

Table 7: Firefox cipher suites

Cipher suite hex code	Cipher suite name
[0xc02c]	security.ssl3.ecdhe_ecdsa_aes_256_gcm_sha384
[0xc014]	security.ssl3.ecdhe_rsa_aes_256_sha
[0xc030]	security.ssl3.ecdhe_rsa_aes_256_gcm_sha384
[0xc02b]	security.ssl3.ecdhe_ecdsa_aes_128_gcm_sha256
[0xc02f]	security.ssl3.ecdhe_rsa_aes_128_gcm_sha256

Table Continued

[0xc013]	security.ssl3.ecdhe_rsa_aes_128_sha
[0x39]	security.ssl3.dhe_rsa_aes_256_sha
[0x33]	security.ssl3.dhe_rsa_aes_128_sha
[0x35]	security.ssl3.rsa_aes_256_sha
[0x2f]	security.ssl3.rsa_aes_128_sha
[0xcc14]	security.ssl3.ecdhe_ecdsa_chacha20_poly1305_sha256
[0xcc13]	security.ssl3.ecdhe_rsa_chacha20_poly1305_sha256
[0xc023]	security.ssl3.ecdhe_ecdsa_aes_128_sha
[0xc00a]	security.ssl3.ecdhe_ecdsa_aes_256_sha

Table 8: Digital signature algorithms

Algorithm
SHA256WITHRSA
SHA384WITHRSA
SHA512WITHRSA
SHA256WITHECDSA
SHA384WITHECDSA
SHA512WITHECDSA
NONEWITHDSA
SHA384WITHDSA
SHA256WITHDSA
SHA224WITHECDSA
SHA512WITHDSA
NONEWITHECDSA
MD5WITHRSA
SHA224WITHRSA
SHA1WITHDSA
SHA224WITHDSA
SHA1WITHECDSA
SHA1WITHRSA

Table 9: Public key algorithms

Algorithm
RSA:2048
RSA:3072

Table Continued

RSA:4096
RSA:1024
ECDSA:256
ECDSA:384
ECDSA:521
DSA:1024
ECDH:384
ECDH:256
ECDH:521
DH:2048
DH:3072
ECCDH:256
ECCDH:384
ECCDH:521
ECMQV:256
ECMQV:384
ECMQV:521
EC:224
EC:256
EC:384
EC:521
ECC:256
ECC:384
ECC:521
ECC:160
EC:192
EC:160

Legacy mode cipher suites for SSH

Table 10: Ciphers

aes128-ctr
aes192-ctr
aes256-ctr

Table 11: Message Authentication Code (MAC)

hmac-sha1
hmac-sha2-256
hmac-sha2-512

Table 12: Key Exchange

ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group- exchange-sha256
diffie-hellman-group14-sha1

Table 13: Host key algorithms (for clients)

ecdsa-sha2-nistp384
ecdsa-sha2-nistp256
ecdsa-sha2-nistp521
ssh-rsa:2048
ssh-dss:1024
ssh-rsa:3072
ssh-rsa:4096

Table 14: Host key algorithms (for servers)

rsa:2048
rsa:3072
rsa:4096
rsa:1024
dsa:1024

Legacy mode cipher suites for SNMP**Table 15: SNMP authentication protocols for interconnects**

SHA1
SHA-256
SHA-384
SHA-512

Table 16: SNMP privacy protocols for interconnects

3DES
AES-128
AES-192
AES-256
DES

Table 17: SNMP digest

SHA_512
SHA_384
SHA_256
SHA1
MD5

Table 18: SNMP symmetric key

AES:AESCTR256:256
AES:AES_256:256
AES:AESCTR192:192
AES:AES_192:192
AES:AESCTR128:128
AES:AES_128:128

Table 19: SNMP authentication protocols for trap forwarding

MD5
SHA1
SHA256
SHA384
SHA512

Table 20: SNMP privacy protocols for trap forwarding

3DES
AES-128
AES-192
AES-256
DES

SNMP server management

For SNMP Server management, wherever device support is available, SNMPv3 is used. The authentication and privacy protocols used vary based on the protocols supported by the specific version of the device.

Algorithms and ciphers suites supported in FIPS 140-2 mode

This unit covers:

- **FIPS 140-2 mode cipher suites for TLS**
- **FIPS 140-2 mode cipher suites for SSH**
- **FIPS 140-2 cipher suites for SNMP**

NOTE: FIPS 140-2 applies only to a VM appliance managing non-c7000 hardware.

FIPS 140-2 mode cipher suites for TLS

Table 21: OpenSSL, Apache, and Curl cipher suites

Cipher suite hex code	Cipher suite name
[0xc024]	ECDHE-ECDSA-AES256-SHA384
[0xc02c]	ECDHE-ECDSA-AES256-GCM-SHA384
[0xc014]	ECDHE-RSA-AES256-SHA
[0xc028]	ECDHE-RSA-AES256-SHA384
[0xc030]	ECDHE-RSA-AES256-GCM-SHA384
[0xc026]	ECDH-ECDSA-AES256-SHA384
[0xc02e]	ECDH-ECDSA-AES256-GCM-SHA384
[0xc02a]	ECDH-RSA-AES256-SHA384
[0xc032]	ECDH-RSA-AES256-GCM-SHA384
[0x3d]	AES256-SHA256
[0x9d]	AES256-GCM-SHA384
[0xc023]	ECDHE-ECDSA-AES128-SHA256
[0xc02b]	ECDHE-ECDSA-AES128-GCM-SHA256
[0xc027]	ECDHE-RSA-AES128-SHA256
[0xc02f]	ECDHE-RSA-AES128-GCM-SHA256
[0xc013]	ECDHE-RSA-AES128-SHA
[0xc025]	ECDH-ECDSA-AES128-SHA256
[0xc02d]	ECDH-ECDSA-AES128-GCM-SHA256
[0xc029]	ECDH-RSA-AES128-SHA256
[0xc031]	ECDH-RSA-AES128-GCM-SHA256

Table Continued

[0x3c]	AES128-SHA256
[0x9c]	AES128-GCM-SHA256
[0x35]	AES256-SHA
[0x2f]	AES128-SHA

Table 22: Java cipher suites

Cipher suite hex code	Cipher suite name
[0xc024]	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
[0xc02c]	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
[0xc014]	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
[0xc028]	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
[0xc030]	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
[0xc026]	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
[0xc02e]	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
[0xc02a]	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
[0xc032]	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
[0x3d]	TLS_RSA_WITH_AES_256_CBC_SHA256
[0x9d]	TLS_RSA_WITH_AES_256_GCM_SHA384
[0xc023]	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
[0xc02b]	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
[0xc027]	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
[0xc02f]	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
[0xc013]	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
[0xc025]	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
[0xc02d]	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
[0xc029]	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
[0xc031]	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
[0x3c]	TLS_RSA_WITH_AES_128_CBC_SHA256
[0x9c]	TLS_RSA_WITH_AES_128_GCM_SHA256
[0x35]	TLS_RSA_WITH_AES_256_CBC_SHA
[0x2f]	TLS_RSA_WITH_AES_128_CBC_SHA
[0xc00e]	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
[0xc009]	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
[0xc004]	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
[0xc005]	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA

Table Continued

[0xc00f]	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
[0xc00a]	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

Table 23: RabbitMQ cipher suites

Cipher suite hex code	Cipher suite name
[0xc024]	ecdhe_ecdsa,aes_256_cbc,sha384,sha384
[0xc014]	ecdhe_rsa,aes_256_cbc,sha
[0xc028]	ecdhe_rsa,aes_256_cbc,sha384,sha384
[0xc026]	ecdh_ecdsa,aes_256_cbc,sha384,sha384
[0xc02a]	ecdh_rsa,aes_256_cbc,sha384,sha384
[0x3d]	rsa,aes_256_cbc,sha256
[0xc023]	ecdhe_ecdsa,aes_128_cbc,sha256,sha256
[0xc027]	ecdhe_rsa,aes_128_cbc,sha256,sha256
[0xc02f]	ecdhe_rsa,aes_128_gcm,null,sha256
[0xc013]	ecdhe_rsa,aes_128_cbc,sha
[0xc025]	ecdh_ecdsa,aes_128_cbc,sha256,sha256
[0xc029]	ecdh_rsa,aes_128_cbc,sha256,sha256
[0x3c]	rsa,aes_128_cbc,sha256
[0x35]	rsa,aes_256_cbc,sha
[0x2f]	rsa,aes_128_cbc,sha

Table 24: Firefox cipher suites

Cipher suite hex code	Cipher suite name
[0xc02c]	security.ssl3.ecdhe_ecdsa_aes_256_gcm_sha384
[0xc014]	security.ssl3.ecdhe_rsa_aes_256_sha
[0xc030]	security.ssl3.ecdhe_rsa_aes_256_gcm_sha384
[0xc02b]	security.ssl3.ecdhe_ecdsa_aes_128_gcm_sha256
[0xc02f]	security.ssl3.ecdhe_rsa_aes_128_gcm_sha256
[0xc013]	security.ssl3.ecdhe_rsa_aes_128_sha
[0x35]	security.ssl3.rsa_aes_256_sha
[0x2f]	security.ssl3.rsa_aes_128_sha
[0xcc14]	security.ssl3.ecdhe_ecdsa_chacha20_poly1305_sha256
[0xcc13]	security.ssl3.ecdhe_rsa_chacha20_poly1305_sha256

Table 25: Digital signature algorithms

Algorithm
SHA256WITHRSA
SHA384WITHRSA
SHA512WITHRSA
SHA256WITHECDSA
SHA384WITHECDSA
SHA512WITHECDSA
SHA1WITHDSA *
SHA1WITHECDSA *
SHA1WITHRSA *

* SHA1 algorithms are not supported on appliance certificates, but are allowed on external server or managed device certificates. Any such SHA1 appliance certificates must be recreated and re-imported before you attempt a mode switch.

Table 26: Public key algorithm

Algorithm
RSA:2048
RSA:3072
RSA:4096
RSA:1024 *
ECDSA:256
ECDSA:384
ECDSA:521
DSA:1024 *
ECDH:384
ECDH:256
ECDH:521
DH:2048
DH:3072
ECCDH:256
ECCDH:384
ECCDH:521
ECMQV:256
ECMQV:384
ECMQV:521

Table Continued

EC:256
EC:384
EC:521
ECC:256
ECC:384
ECC:521
EC:192 *

* These algorithms are allowed under legacy-use clause of FIPS 140-2 specifications for external server or managed device certificates, but are not used for appliance certificates.

FIPS 140-2 mode cipher suites for SSH

Table 27: Ciphers

aes128-ctr
aes192-ctr
aes256-ctr

Table 28: Message Authentication Code (MAC)

hmac-sha1
hmac-sha2-256
hmac-sha2-512

Table 29: Key Exchange

ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group- exchange-sha256
diffie-hellman-group14-sha1

Table 30: Host key algorithms (for clients)

ecdsa-sha2-nistp384
ecdsa-sha2-nistp256
ecdsa-sha2-nistp521
ssh-rsa:2048
ssh-rsa:3072
ssh-rsa:4096

Table 31: Host key algorithms (for servers)

rsa:2048
rsa:3072
rsa:4096
ecdsa:256
ecdsa:384
ecdsa:521

FIPS 140-2 cipher suites for SNMP**Table 32: SNMP authentication protocols for interconnects**

SHA1
SHA-256
SHA-384
SHA-512

Table 33: SNMP privacy protocols for interconnects

AES-128
AES-192
AES-256

Table 34: SNMP authentication protocols for trap forwarding

MD5
SHA1
SHA256
SHA384
SHA512

Table 35: SNMP privacy protocols for trap forwarding

3DES
AES-128
AES-192
AES-256
DES

Table 36: SNMP digest

SHA_512
SHA_384
SHA_256
SHA1

Table 37: SNMP symmetric key

AES:AESCTR256:256
AES:AES_256:256
AES:AESCTR192:192
AES:AES_192:192
AES:AESCTR128:128
AES:AES_128:128

SNMP server management

For SNMP Server management, wherever device support is available, SNMPv3 is used. HPE OneView uses the ILO SNMP interface for server management. However, this interface is not FIPS-compliant. The authentication and privacy protocols used vary based on the protocols supported by the specific version of the device.

Algorithms and ciphers supported in CNSA mode

This unit covers:

- **CNSA mode cipher suites for TLS**
- **CNSA mode cipher suites for SSH**
- **CNSA mode cipher suite for SNMP**

NOTE:

- When the iLO of a managed server is in the CNSA or Suite B mode, the iLO user interface or console is not accessible from the HPE OneView console.
- In the CNSA mode, both p-384 and p-521 curves are supported.

NOTE: CNSA applies only to a VM appliance managing non-c7000 hardware.

CNSA mode cipher suites for TLS**Table 38: OpenSSL, Apache, and Curl cipher suites**

Cipher suite hex code	Cipher suite name
[0xc02c]	ECDHE-ECDSA-AES256-GCM-SHA384
[0xc028]	ECDHE-RSA-AES256-SHA384
[0xc030]	ECDHE-RSA-AES256-GCM-SHA384

Table 39: Java cipher suites

Cipher suite hex code	Cipher suite name
[0xc02c]	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
[0xc028]	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
[0xc030]	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Table 40: RabbitMQ cipher suites

Cipher suite hex code	Cipher suite name
[0xc028]	ecdhe_rsa,aes_256_cbc,sha384,sha384

Table 41: Digital signature algorithms

Algorithm
SHA384WITHRSA
SHA512WITHRSA
SHA384WITHECDSA
SHA512WITHECDSA

Table 42: Public key algorithms

Algorithm
RSA:3072
RSA:4096
ECDSA:384
ECDSA:521
EC:384
EC:521
ECC:384
ECC:521

CNSA mode cipher suites for SSH**Table 43: Ciphers**

aes256-ctr

Table 44: Message Authentication Code (MAC)

hmac-sha2-512

Table 45: Key Exchange

ecdh-sha2-nistp384
ecdh-sha2-nistp521

Table 46: Host key algorithms (for clients)

ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
ssh-rsa:3072
ssh-rsa:4096

Table 47: Host key algorithms (for servers)

rsa:3072
rsa:4096
ecdsa:384
ecdsa:521

CNSA mode cipher suite for SNMP**Table 48: SNMP authentication protocols for interconnects**

SHA-384
SHA-512

Table 49: SNMP privacy protocols for interconnects

AES-256

Table 50: SNMP authentication protocols for trap forwarding

MD5
SHA1
SHA256
SHA384
SHA512

Table 51: SNMP privacy protocols for trap forwarding

3DES
AES-128
AES-192
AES-256
DES

Table 52: SNMP digest

SHA_512
SHA_384

Table 53: SNMP symmetric key

AES:AESCTR256:256
AES:AES_256:256

SNMP server management

For SNMP Server management, wherever device support is available, SNMPv3 is used. HPE OneView uses the ILO's SNMP interface for server management. This interface is however, not FIPS-compliant. The authentication and privacy protocols used vary based on the protocols supported by the specific version of the device.

Scope-enabled resource categories

Only the following resource types can be added to or removed from a scope:

- Enclosures
- Server Hardware
- Networks (Ethernet, FC, and FCoE)
- Network Sets
- Interconnects, excluding SAS resources
- Logical Interconnects, excluding SAS resources
- Logical Interconnect Groups, excluding SAS resources
- OS Deployment Plans
- Switches
- Logical Switches
- Logical Switch Groups
- Rack Managers
- Storage Pools
- Volumes
- Volume Templates
- Volume Sets

! **IMPORTANT:** For email notification of alerts, resources that are not categorized here are included in any scope. An email notification filter that specifies one or more scopes does not eliminate alerts generated by resources that are not currently categorized here.

Inhibiting alerts from non-scope resources requires the use of associated resource categories, which is described in “Edit an email recipient and filter entry” in the online help.

More information

Security-hardened appliance

HPE OneView is delivered as a security-hardened virtual appliance. The following factors secure (harden) the appliance and its operating system.

- HPE OneView can be switched to FIPS and CNSA cryptography modes, wherein you can apply stricter security protection of FIPS-140-2 and an even stricter CNSA specification.
- Some examples of best-practice security hardening used within the HPE OneView virtual appliance are:
 - The appliance uses a customized operating system that eliminates all nonessential services to reduce its attack surface.
 - The appliance minimizes its vulnerability by running only the services required to provide functionality.
 - The appliance OS enforces mandatory access controls.
 - The appliance supports two-factor authentication.
 - The operating system bootloader is password protected. The appliance cannot be compromised by someone attempting to boot in single-user mode.
 - An IP firewall only allows access to the ports required by HPE OneView services. See **Ports required for HPE OneView** for the list of network ports.
 - Key services do not run as privileged OS users.
 - There are no users allowed at the operating system level (no interactive OS logins are allowed). Users interact with HPE OneView strictly through:
 - REST APIs (either programmatically or through the GUI)
 - The State Change Message Bus (AMPQ interface)
 - The maintenance console through SSH or from the appliance console for appliance management
 - A web server that provides the html pages for the GUI and the online help
- HPE OneView is designed to operate entirely on an isolated management LAN.
- RBAC (role-based access control) enables an administrator to establish access control and authorization for users based on their responsibilities for specific resources. RBAC also simplifies what is shown in the UI:
 - Users can initiate actions only for the types of resources for which they are authorized. For example, users with the role of Network administrator can initiate actions for the network resources only, and users with the role of Server administrator can initiate actions for the server resources only.
 - Users with the role of Infrastructure administrator have full access to all screens and actions.
- SBAC (scope-based access control) enables an administrator to establish access control for users by allowing a role to be restricted to a subset of resources managed by the appliance. The infrastructure administrator grants rights to users and directory groups by assigning permissions. A permission consists of a role and an optional scope. A scope is a user-defined set of resources. A resource can belong to multiple scopes. The role grants access to resource categories. The scope further restricts the rights granted by the role to a subset of instances in the resource category.
- HPE OneView supports integration with Microsoft Active Directory or OpenLDAP for user authentication. Local user accounts can be disabled when enterprise directories are in use. See "About directory service authentication" in the online help.
- The Administrator account has a default password for initial appliance installation. The appliance enforces a password change at first login and the default password **cannot** be used again.

- The appliance supports self-signed certificates and certificates issued by a certificate authority.

The appliance is initially configured with a self-signed certificate. As the Infrastructure administrator, you can generate a CSR (certificate signing request) to submit to a corporate or third-party CA and, upon receipt, upload the certificate. This certificate ensures the integrity and authenticity of your HTTPS connection to the appliance.

Similarly, by default, the communication between HPE OneView and managed devices is secured using self-signed certificates. Using REST interfaces for each managed device, you can generate a CSR to submit to a corporate or third-party CA and, upon receipt, upload the signed certificate to the managed device. This certificate ensures the integrity and authenticity of the management communications between the appliance and each managed device.

- All browser operations and REST API calls use HTTPS/TLS.
- The appliance supports a secure update procedure for installing patches or upgrading to the next version. The updates are digitally signed by Hewlett Packard Enterprise and the update procedure verifies the digital signature. The signature and verification ensures the authenticity and integrity of software updates.
- Support dumps created by users who are not an Infrastructure administrator are encrypted; Infrastructure administrator users have the option to not encrypt a support dump. The default encryption protects any sensitive customer data contained in the support dump (such as IP addresses, IP address pools, hostnames, and WWNs). An unencrypted dump is available for an Administrator to validate the type of data being sent back to Hewlett Packard Enterprise. No credential data is ever included in a support dump.
- Hewlett Packard Enterprise closely monitors security bulletins for threats to appliance software components and, if necessary, issues software updates.

Creating a login session

You create a login session when you log in to the appliance through the browser. Additional requests to the appliance use the session ID, which must be protected because it represents the authenticated user. To protect the session ID, use a supported web browser when using the UI. When writing a client of the OneView REST interface, the programmer must not reveal the session ID.

A session remains valid until you log out or the session times out (for example, if a session is idle for a longer period of time than the session idle timeout value).

The default timeout value is 24 hours. To change the value on a per-session basis, use `POST /rest/sessions/idle-timeout`. You can change the value to 24 hours or less.


Authentication for appliance access

You can authenticate users to access HPE OneView using any one of the following methods:

- User name and password login: You can configure the appliance to perform authentication using a user name and password.

NOTE: If you had opted for a customer-provided password using the Factory Express process, the default **administrator** / **admin** login password fails. In this case, use the user name and password that you specified in the Factory Express process form.

- Two-factor login: You can configure the appliance to perform smart certificate authentication using the two-factor login. When two-factor authentication is enabled in the Security settings screen, you must use a smart card and a valid personal identification number (PIN) to authenticate access to HPE OneView.

 **IMPORTANT:** When **Smart card only login** is enabled in the Security settings screen, only the two-factor login option is displayed on the HPE OneView login screen. Customers who require the highest level of security mandate the use of the **Smart card only login**.

NOTE: If you are unable to login to the appliance using two-factor authentication, check the **Directory domain** configuration under **Edit security > Client Login Certificate Configuration**. If the certificates are missing the directory domain information, use the **Manually specify** option to manually enter your domain details.

The following are the prerequisites to log into the HPE OneView appliance using a smart card:

- The user, when prompted by their browser, must enter a valid PIN.

NOTE: A valid PIN allows the browser to access the certificate contents and pass them to HPE OneView.

- The certificate must be valid (properly signed, not expired, proper X.509 format).
- The certificate must not have been revoked.
- The certificate must contain at least one user name that can be extracted from the configured certificate fields.
- At least one user name from the certificate must be a valid user in one of the configured directories.
- The certificate must contain the directory domain information or the administrator must have manually specified the same.

If all these requirements are met, HPE OneView retrieves the list of groups to which the user belongs from the enterprise directory. HPE OneView uses the group membership information to determine which role to assign to the user. The role informs HPE OneView which resources the user must have access to and what operations they can perform.

User accounts are configured on the appliance or in an enterprise directory (required for two-factor authentication). All access (browser and REST APIs), including authentication, occurs over Transport Layer Security (TLS) to protect the credentials during a transmission over the network.

More information

- "Security/Edit Security screen details" in the online help.
- **Two-factor Authentication** on page 121

Two-factor Authentication

Passwords, no matter how complex, provide insufficient security for many applications. For additional security, use two-factor authentication. With two-factor authentication, two factors are required for HPE OneView authentication. The two factors are something the user possesses (a smart card), and something the user knows (a personal identification number).

HPE OneView user and password authentication

Users can be configured in HPE OneView as local users, or remotely in an enterprise directory.

The traditional user name and password login sequence are as follows:

1. The user enters their user name and password.
2. HPE OneView authenticates the user name and password.
 - If the user name is that of a local user configured in HPE OneView, HPE OneView validates a manually specified user name and password using the HPE OneView database.
 - If your environment is configured to use an enterprise directory, HPE OneView immediately forwards the user name and password to a configured directory server for authentication.
3. Once authentication is successful, HPE OneView determines the authorization permissions for the user.

- If it is a local user login, authorization permissions are decided based on the roles associated with the user.
- If it is an enterprise directory login, HPE OneView sends a request to the directory server to retrieve the group name associated with the user. It uses the group name to determine the authorization permission for the user configured in HPE OneView.

HPE OneView two-factor authentication

Enabling two-factor authentication allows you to use smart cards — for example, Common Access Cards (CAC), or Personal Identity Verification (PIV) cards — to authenticate within HPE OneView. The smart card reader plugin in the browser reads the smart card and accesses the certificate in the card using the PIN specified by the user. The client certificate embedded in the smart card is presented to HPE OneView by the browser. The client certificate must be signed by a root or intermediate Certificate Authority (CA) that has been previously imported into HPE OneView. The appliance authenticates the client certificate to validate that the user name specified in the certificate is that of a valid user recognized by the directory server configuration in HPE OneView.

When two-factor authentication is enabled, HPE OneView uses a Microsoft Active Directory service account setup and owned by the user to access an Active Directory entry for the user, rather than using an account associated with the user name received during first-time login.

NOTE:

- The Active Directory is not part of the HPE OneView appliance. You must separately install an Active Directory in your environment.
- In HPE OneView, two-factor authentication is supported on an Active Directory configured with service account binding type.

When you configure HPE OneView to use an enterprise directory such as Active Directory or OpenLDAP, the directory is assigned a name for use in the HPE OneView user interface. This directory can be serviced by multiple directory servers for high availability. Directory groups are assigned HPE OneView roles and the directory users that are members of those groups are assigned those HPE OneView roles. An HPE OneView directory with its corresponding directory servers can only be defined once, and use a single set to group role mappings. Assigning additional, different HPE OneView directory names for the same set of directory servers is not supported.

An Infrastructure administrator also has the flexibility to customize the rules HPE OneView applies during client certificate authentication. The Infrastructure administrator can configure the locations within the certificate from which HPE OneView retrieves the user name, domain name, and the OIDs that must be present for the certificate to be valid.

The certificates stored on CAC/PIV cards are X.509 security certificates. They contain fields of information used to identify the certificate owner, the certificate issuer, and other certificate identification elements. When you enable two-factor authentication, you can specify which certificate fields HPE OneView must use to validate a user. See "Client Login Certificate Configuration Screen Details" in the online help.

NOTE: When using REST APIs to authenticate smart card login, the REST client used must be capable of supporting client certificate authentication requested by HPE OneView.

Using the command line to login to HPE OneView based on two-factor authentication

You can remotely log into an appliance using the REST API `/rest/login-sessions/smartcards`. One possible way of doing this is to use curl-7.54.1-1 version or higher, which in turn uses libssh2. Here is an example command:

```
# curl -v -i -X POST -H "Accept-Language:en-US" -H "X-Api-Version:<version number>" --cert ./client-cert.pem:<PEM pass phrase>
https://{appliance-IP}/rest/login-sessions/smartcards --cacert ./rootsplintermediate.cer
```

NOTE: The client-cert.pem file might be generated using OpenSSL or any other equivalent method. This file has both the client certificate and the pass phrase-protected private key. Replace **<PEM passphrase>** with the actual passphrase. The rootsplsintermediate.cer file contains the root and the chain of intermediate certificates that was used to sign the HPE OneView server certificate. Alternately the rootsplsintermediate.cer might have the self-signed certificate of the HPE OneView server.

See the *HPE OneView API Reference* for more information.

Certificate owner - Subject alternative name attributes

By default, the attribute entry box associated with the “Subject Alternative Name” item, within the “Certificate owner” entry, contains **OtherName.UPN=(.*)**. This tells HPE OneView to extract the *user name* from the “OtherName.UPN” attribute within the *Subject Alternative Name* field of the certificate on the smart card. This is the *user name* that HPE OneView uses to query the enterprise directory.

You can edit the value to enable HPE OneView to search for the *user name* within other additional attributes within *Subject Alternative Name*. The options include:

- **OtherName.UPN=(.*)**

The Microsoft certificate viewer displays “OtherName.UPN” under *Subject Alternative Name* as:

Other Name:
Principal Name=John.Doe@test.com

- **OtherName.RFC822Name=(.*)**

The Microsoft certificate viewer displays **OtherName.RFC822Name** as:

Other Name:
RFC822 Name=John.Doe@test.com

- **RFC822Name=(.*)**

The Microsoft certificate viewer displays **RFC822Name** as:

RFC822 Name=John.Doe@test.com

- **DirName=(.*)**

The Microsoft certificate viewer displays “DirName” under *Subject Alternative Name* as:

Directory Address:
CN=John Doe
OU=Test Group
O=Test Org
C=US
DC=test
DC=com

Use a comma-separated list to include multiple values in the entry field, allowing HPE OneView to search multiple *Subject Alternative Name* attributes for a valid *user name*.

NOTE: You can instruct HPE OneView to search for the *user name* within the attributes of the “Subject” field of the smart card certificate (either in addition to, or instead of, searching within “Subject Alternative Name” attributes). See subject entry in the “Certificate owner” field for details.

Subject Alternative Name multiple attribute entry example

```
OtherName.UPN=(.*),OtherName.RFC822Name=(.*) ,RFC822Name=(.*) ,DirName=(.*)
```

Certificate owner - Subject attributes

By default, the attribute entry box associated with the “Subject” entry, within the “Certificate owner” field, contains **CN= (. *)**. With this value, HPE OneView extracts the first *user name* it encounters within a “CN” attribute within the “Subject” field in the smart card certificate. You can edit the regular expression for the “CN” attribute using regular expressions to refine the list of acceptable values.

You can edit the value if you need HPE OneView to search for the *user name* within other additional attributes within the certificate “Subject” field. The choices include:

- **CN= (. *)**
- **E= (. *)**
- **UID= (. *)**
- **DN= (. *)**

Microsoft Active Directory users must note that the DN is extracted as an aggregate of the subject attributes from the certificate. This should match the DN value configured for the user in the Active Directory. If this is not an exact match, the login operation fails.

Use a comma separated list to include multiple values in the entry field, allowing HPE OneView to search multiple Subject attributes for a valid *user name*.

NOTE: You can instruct HPE OneView to search for the *user name* within the attributes of the “Subject” field of the smart card certificate (either in addition to, or instead of, searching within “Subject Alternative Name” attributes).

Subject multiple attribute entry example

```
CN= ( . * ) ,E= ( . * ) ,UID= ( . * ) ,DN= ( . * )
```

Variations for the CN attribute: examples

- To match only user names starting with "J_" use **CN= (^J_.*\$)**
- To match names in "LastName, FirstName" format use **CN=([a-zA-Z]*,[a-zA-Z-Z]+)\$)**
- To match user names containing only numbers **CN= (^ [0-9] +\$)**

NOTE: This is applicable when there are multiple CN attributes configured in a certificate and the user wants to specify a specific attribute rather than the first available in the CN attribute. It is recommended to use patterns that begin with '^' and end with '\$' so that the system can perform an exact match.

Directory domain

The **Directory domain** control allows you to specify which domain or directory to use when searching for the user in an enterprise directory. The domain name must match the Base DN of at least one of the directories added to HPE OneView. The options include:

- Subject
- Subject Alternative Name

- Issuer
- Manually specify

After you select which certificate field HPE OneView must use to extract the domain name, the name is extracted from the DC attributes specified therein. The `DC=(.*)` configuration extracts the first domain component from the field. The administrator can only specify `DC=(.*)` here.

If you select **Manually specify**, you can enter a specific domain using dot notation, or an alternate certificate location from which to retrieve domain information to use when querying the directory. You can specify multiple entries or domains in the configuration using `,`. Additionally, you can specify the subject, subject alternative name and Issuer DC attributes to support multiple card configuration.

Examples: Selection values for the 'Manually specify' control

In the fields of a certificate, the domain components are usually represented by multiple “DC=” entries. A domain BaseDN, like `abc.example.com`, is represented by the three entries “DC=abc”, “DC=example”, and “DC=com”.

- Use “example.com” as the domain to use when searching for users in an enterprise directory:

`example.com`

- Configure HPE OneView to look in multiple certificate locations for domain information. HPE OneView tries each item in order until it finds a successful user entry in the enterprise directory.

`Subject.DC=(.*) , Issuer.DC=(.*) , SubjectAlternativeName.DirName.DC=(.*) , groupA.example.com , groupB.example.com`

Requirements to validate the certificate

The **Requirements to validate the certificate** control allows you to configure who can access HPE OneView by specifying the Key Usage, Extended Key Usage and Policy ID Object Identifiers (OIDs) that must be present within a smart card certificate in order for the user associated with the card to be authenticated. You can configure up to five OID combinations to accommodate different groups of users within your organization.

By default, one combination is configured, containing the OID combination Smart Card Logon (1.3.6.1.4.1.311.20.2.2), Client Authentication (1.3.6.1.5.5.7.3.2). This combination requires the certificate on the smart card to be configured to allow the certificate to be used for smart card logon and for client authentication. It should work for most installations. You can edit this field to opt for a different combination of OIDs, or to add additional OIDs. A maximum of ten OIDs can be configured in a single combination box.

To configure additional OID combinations, use **Add a required validation**.

NOTE: If you specify multiple OID combinations and one is a super-set of another, configure the more restrictive combination first.

Controlling access for authorized users

Access to the appliance is controlled by roles and scope, which describe what an authenticated user is permitted to do on the appliance. Each user must be associated with at least one role. Scope is a user-defined set of resources. The scope further restricts the rights granted by the role to a subset of instances in the resource category. Permissions granted to the user control user access to the appliance and the resources managed by the appliance. For information about scopes and permissions, see the *HPE OneView Online Help*.

Specifying user accounts and roles

User login accounts on the appliance must be assigned a role, which determines what the user has permission to do.

For information on how to add, delete, and edit user accounts, see the online help.

Mapping of SSO roles for iLO and OA

The appliance enables SSO (single sign-on) to iLO and OA (Onboard Administrator) without storing user-created iLO or OA credentials. The following table describes the mapping of roles between the appliance, iLO, and OA.

Appliance role	SSO to iLO roles	SSO to OA roles
Infrastructure administrator	Admin	Admin
Server administrator	Admin	Admin
Server firmware operator	Admin	User
Server profile architect	Admin	User
Server profile administrator	Admin	User
Network administrator	User	User
Read only	User	User
Backup administrator	User	None
Storage administrator	User	User
Scope administrator	User	User
Scope operator	User	User

Appliance roles

"About user roles" in the online help provides a list of available roles.

iLO roles

- Administrator privileges enable assigning all administrative rights for server reset, remote console, and login tasks. User privileges enable full information access but no control capability.
- User privileges enable full information access but no control capability.

OA roles

- Administrator privileges grant full rights which includes the ability to manage the enclosure and bays.
- User privileges enable full information access but no control capability.

Mapping appliance interactions with iLO, OA, and iPDU

The appliance performs configurations on the iLO, OA, and Intelligent Power Distribution Unit (iPDU). The following table summarizes how the appliance interacts with these devices.

For firewall information, see **Ports required for HPE OneView**.

Protocol or interaction	Description	iLO	OA	iPDU
		Configure	Configure	Configure
NTP	Configures NTP	✓	✓	
SNMP	Enables and configures SNMP to collect information	✓	✓	✓
SNMP traps	Enables and configures SNMP traps sent to appliance	✓	✓	✓
HTTPS (RIBCL/SOAP/JSON)	Collects information (the specific protocol varies, but all use TLS)	✓		
Remote Console	Links from the UI to the iLO Remote Console	✓		
SSH	Not used			
Telnet	Not used			
XML reply	Collects generic system information	✓		
SSO	Enables and configures an SSO certificate for UI access. See Mapping of SSO roles for iLO and OA for the privileges that are granted.	✓	✓	
Appliance user account (_HPOneViewAdmin)	Configures and manages the system using an administrator-level user account (and randomly generated long password)	✓		✓

Secure Shell access

HPE OneView supports Secure Shell (SSH) to remotely access the appliance to perform maintenance and recovery operations. Without SSH access, you must access the virtual machine system console. To avoid requiring a console access, SSH access is enabled by default. However, remote access to maintenance and recovery operations is considered a security risk by some users. Therefore, HPE OneView provides the option to disable remote access to the appliance via SSH.

More information

"Enable or disable SSH access" in the online help

Protecting credentials

Local user account passwords are stored using a salted hash; that is, they are combined with a random string, and then the combined value is stored as a hash. A hash is a one-way algorithm that maps a string to a unique value so that the original string cannot be retrieved from the hash.

Passwords are masked in the browser. When transmitted between appliance and the browser over the network, passwords are protected by TLS.

Local user account passwords must be a minimum of eight characters, with at least one uppercase character. HPE OneView does not enforce additional password complexity rules. Site security policy determines password strength and expiration (see **Best practices for maintaining a secure appliance**). Hewlett Packard Enterprise recommends that you integrate an external authentication directory service (also known as an enterprise directory) with HPE OneView. The directory service (required with two-factor authentication) enforces password management policies such as minimum length and complexity.

About audit log

The audit log contains a record of actions performed on the appliance, which you can use for individual accountability. Because the logs are rolled over periodically to prevent them from getting too large, Hewlett Packard Enterprise recommends downloading the audit logs to monitor the actions being performed. You can also download the audit logs periodically to maintain a long-term audit history.

Each user has a unique logging ID per session, enabling you to follow a user's trail in the audit log. Some actions are performed by the appliance and might not have a logging ID.

You must have Infrastructure administrator privileges to download the audit log.

For information on downloading the audit log from the UI, see "Download the audit logs" in the online help.

A breakdown of an audit entry follows:

Token	Description
Date/time	The date and time of the event
Internal component ID	The unique identifier of an internal component
Reserved	The organization ID. Reserved for internal use
User domain	The login domain name of the user
User name/ID	The user name
Session ID	The user session ID associated with the message
Task ID	The URI of the task resource associated with the message
Client host/IP	The client (browser) IP address identifies the client machine that initiated the request

Table Continued

Token	Description																				
Result	<p>The result of the action, which can be one of the following values:</p> <ul style="list-style-type: none">• SUCCESS• FAILURE• SOME_FAILURES• CANCELED• KILLED																				
Action	<p>A description of the action, which can be one of the following values:</p> <table><tr><td>• ADD</td><td>• LIST</td><td>• UNSETUP</td><td>• CANCELED</td></tr><tr><td>• MODIFY</td><td>• ENABLE</td><td>• DEPLOY</td><td>• LOGIN</td></tr><tr><td>• DELETE</td><td>• DISABLE</td><td>• START</td><td>• LOGOUT</td></tr><tr><td>• ACCESS</td><td>• SAVE</td><td>• DONE</td><td>• DOWNLOAD_START</td></tr><tr><td>• RUN</td><td>• SETUP</td><td>• KILLED</td><td></td></tr></table>	• ADD	• LIST	• UNSETUP	• CANCELED	• MODIFY	• ENABLE	• DEPLOY	• LOGIN	• DELETE	• DISABLE	• START	• LOGOUT	• ACCESS	• SAVE	• DONE	• DOWNLOAD_START	• RUN	• SETUP	• KILLED	
• ADD	• LIST	• UNSETUP	• CANCELED																		
• MODIFY	• ENABLE	• DEPLOY	• LOGIN																		
• DELETE	• DISABLE	• START	• LOGOUT																		
• ACCESS	• SAVE	• DONE	• DOWNLOAD_START																		
• RUN	• SETUP	• KILLED																			
Severity	<p>A description of the severity of the event, which can be one of the following values, listed in descending order of importance:</p> <ul style="list-style-type: none">• INFO• NOTICE• WARNING• ERROR• ALERT• CRITICAL																				
Resource category	For REST API category information, see the <i>HPE OneView API Reference</i> .																				
Resource URI/name	The resource URI/name associated with the task																				
Message	The output message that appears in the audit log																				

Maintenance console entries

The audit log includes entries for all Maintenance console events except for viewing.

About audit log forwarding

Audit log forwarding enables the Infrastructure administrator to forward audit logs to remote Security Information and Event Management (SIEM) systems. Such systems enable centralized audit compliance, monitoring, log analysis, and controlled retention policies.

The forwarding protocol used is the standard UDP-based syslog protocol described in RFC5424 and RFC5426. The syslog protocol is supported by all common syslog servers such as rsyslog, syslog-ng and SIEM products.

NOTE: Ensure that any firewalls between HPE OneView and the remote syslog server allow UDP traffic. The default UDP port used is 514.

As audit log entries are forwarded over UDP, the entries are not encrypted and delivery is not guaranteed. Even when you have HPE OneView and all managed devices on a dedicated, isolated management LAN, forwarding audit log entries to external systems can pose a security risk. In an environment where encryption is required, use the REST API `/rest/audit-logs` to schedule a job to download the appliance audit logs. See the *HPE OneView API Reference* for more information.

More information

"Forward an audit log" topic in the *HPE OneView Online Help*

Choosing a policy for the audit log

Choose a policy for downloading and examining the audit log.

The audit log contains a record of actions performed on the appliance, which you can use for individual accountability. As the audit log gets larger, older information is deleted. To maintain a long-term audit history, you must periodically download and save the audit log.

For more information about the audit log, see [Understanding the audit log](#).

Appliance access over TLS

All access to the appliance is through HTTPS (HTTP over TLS), which encrypts data over the network and helps to ensure data integrity. For a list of supported cipher suites, see "Algorithms for securing the appliance" in the online help.

Managing certificates from a browser

A certificate authenticates the appliance over TLS. The certificate contains a public key, and the appliance maintains the corresponding private key, which is uniquely tied to the public key.

This section discusses certificate management from the perspective of the browser. For information on how a non-browser client (such as cURL) uses the certificate, see the documentation for that client.

NOTE: In most cases, when accessing an appliance through its default self-signed certificate, the browser will issue a security warning that must be bypassed before getting to the appliance. While some browsers allow you to store a self-signed certificate indefinitely, you cannot permanently store a self-signed certificate in the Google Chrome browser -- the certificate will expire after a few days. For easier access, Hewlett Packard Enterprise recommends that you create a signed certificate for use with the appliance.

The certificate also contains the name of the appliance, which the TLS client uses to identify the appliance.

The certificate has the following boxes:

- **Common Name (CN)**

This name is required. By default it contains the fully qualified host name of the appliance.

- **Alternative Name**

The name is optional, but Hewlett Packard Enterprise recommends supplying it because it supports multiple names (including IP addresses) to minimize name-mismatch warnings from the browser.

By default, this name is populated with the fully qualified host name (if DNS is in use), a short host name, and the appliance IP address.

NOTE: If you enter **Alternative Names**, one of them must be your entry for the **Common Name**.

These names can be changed when you manually create a certificate signing request or create a self-signed certificate.

Use a certificate authority

Use a trusted CA (certificate authority) to simplify certificate trust management; the CA issues certificates that you import. If the browser is configured to trust the CA, certificates signed by the CA are also trusted. A CA can be internal (operated and maintained by your organization) or external (operated and maintained by a third party).

You can import a certificate signed by a CA, and using it instead of the self-signed certificate. The overall steps are as follows:

Procedure

1. You generate a CSR (certificate signing request).
2. You copy the CSR and submit it to the CA, as instructed by the CA.

NOTE: Request that the certificate be generated with a 2048-bit key and with a digital signature algorithm of SHA256 or higher.

3. The CA authenticates the requestor.
4. The CA sends the certificate to you, as stipulated by the CA.
5. You import the certificate.

See [Create an appliance certificate signing request](#) and [Import a certificate](#).

Self-signed certificate

The default certificate generated by the appliance is self-signed; it is not issued by a trusted certificate authority.

By default, browsers do not trust self-signed certificates because they lack prior knowledge of them. The browser displays a warning dialog box; you can use it to examine the content of the self-signed certificate before accepting it. Do not use a self-signed certificate without examining it before accepting it into your browser.

Hewlett Packard Enterprise recommends that you create a signed certificate for use with the appliance. However, if you choose to use a self-signed certificate, accept the certificate into all of the browsers that will be used to access the appliance. If PowerShell scripts use the HPE OneView REST API, extra code is required which leaves the scripts open to attackers using self-signed certificates.

More information

[Download a self-signed certificate](#) on page 135

Create an appliance certificate signing request

The appliance uses a certificate for authentication over TLS. The certificate contains a public key, and the appliance maintains the corresponding private key, which is uniquely tied to the public key.

A CA is a trusted party that issues a certificate that enables others, who trust the CA, to also trust the host. In essence, the CA vouches for the host.

For information on creating a self-signed certificate, see [Create an appliance self-signed certificate](#) on page 132.

Prerequisites

- Privileges: Infrastructure administrator.
- Gather the information for the request, as required by the certificate authority (CA).
- Obtain the CA challenge password.

Procedure

1. From the main menu, select **Settings**.
2. Click **Security**.
3. Select **Actions** > **Create certificate request**.
4. Supply the data requested on the screen.
5. Click **OK**.
6. Copy the certificate request data from the dialog box and send it to the CA. The CA designates how and where to send the certificate request data.
7. Click **OK**.

Next steps: After you receive the certificate from the CA, see [Import an appliance certificate](#) on page 134.

Create an appliance self-signed certificate

The appliance uses a certificate for authentication over TLS. The certificate contains a public key, and the appliance maintains the corresponding private key, which is uniquely tied to the public key.

A self-signed certificate indicates that a host vouches for itself, which, in some cases, might be adequate. By default, browsers do not trust self-signed certificates and display a warning.

A more secure alternative is a certificate issued by a third-party certificate authority. For information on these certificates, see [Create an appliance certificate signing request](#) on page 131.

Prerequisites

Minimum required privileges: Infrastructure administrator

Procedure

1. From the main menu, select **Settings**.
2. Click **Security**.
3. Select **Actions** > **Create self-signed certificate**.
4. Supply the data requested on the screen.
5. Enter optional information, as needed.
6. Click **OK**.
7. Verify that the certificate was created. The certificate information is shown on the screen.

Create a CA-signed client certificate for SCMB

The following procedure describes how to generate a CA-signed client certificate that can be used to connect to the State Change Message Bus (SCMB).

Prerequisites

- An environment with OpenSSL installed, or equivalent.
- Access to a commercial or custom certificate authority (CA) for signing requests.

Procedure

1. Create a new key pair for the client certificate.

This command generates a new private key with a file name of `cert.key` with 3072-bit encryption:

```
openssl genrsa -out cert.key 3072
```

2048-bit encryption will also work in generating a key pair, but the resulting client certificate will not work when HPE OneView is in CNSA mode.

2. Using the new key pair, create a Certificate Signing Request (CSR) for the client certificate.

This command creates a CSR using data input through interactive prompts:

```
openssl req -new -key cert.key -out cert.csr
```

The common name for this command must be set to `rabbitmq_readonly`, because the SCMB server is configured to accept connections from this user. For the other prompts, provide appropriate inputs for your organization.

3. Create a client certificate that will be used to connect to the SCMB server, using the signing method that corresponds to your relationship with the CA.

- a. If the CA is provided by a commercial entity or other organization, follow the instructions provided by the CA for signing a client certificate.
- b. If direct access to a CA root certificate and key is available, create a configuration file (`openssl.cnf`) with the necessary options for an operational client certificate.

For example:

```
[ client ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = clientAuth, msSmartcardLogin
nsCertType = client
subjectAltName = @alt_names

[ alt_names ]
email = .
```

The `basicConstraints`, `extendedKeyUsage:clientAuth`, and `nsCertType` fields are all required to specify a client certificate. An OpenSSL expert can apply other settings, according to organizational requirements and an understanding of the effects. Refer to the OpenSSL documentation for more information.

- c. Use the resulting configuration file to sign the CSR and generate a client certificate.

For example:

```
openssl x509 -req -CA ca.pem -CAkey ca.key -in
cert.csr -out cert.pem -days 365 -set_serial 1
-extfile openssl.cnf -extensions client
```

4. Ensure the CA root certificate, as well as any intermediate CA used to sign the SCMB client certificate, is trusted by the appliance. The SCMB server on the appliance will accept a client certificate only if it trusts the CA that signed the certificate. If this trust is not already established, do so now.

NOTE: The intermediate CA certificates that signed the client should be added to the client program and not to the appliance.

- a. Go to **Security Settings > Manage Certificate Authority Certificates** and add the CA to the appliance.

Any active connections to the SCMB server will break and need to be re-established as a result.

5. Using a client program of your choice, connect to the SCMB server on the appliance. A successful connection requires the key pair created in Step 1, the client certificate created in Step 3, and a CA certificate file containing the root certificate for the CA that signed the SCMB server certificate and any intermediate CA certificates used in signing the client certificate.
6. If you are still unable to connect to the SCMB server, **follow these troubleshooting steps**.

Import an appliance certificate

After sending a certificate signing request to the CA and receiving a certificate, you must import it.

There are two ways to import a CA-signed appliance certificate. You can choose either of the following:

- Import the full certificate chain of a CA-signed appliance certificate in the **Import appliance certificate** screen.
- Add root CA and intermediate CA certificates or either of them to the appliance in the **Add certificates** screen. Then, import the leaf level CA-signed appliance certificate in the **Import appliance certificate** screen.

NOTE: The maximum number of CA certificates that can be present in the certificate chain is nine. Setting a maximum certificate chain depth means that appliance rejects any certificate from being imported if the certificate chain depth is higher than the maximum limit. The maximum certificate chain depth is set by default on the appliance, and cannot be customized by the user.

Additionally, each CA certificate can have the **Path Length Constraint** attribute set under the **Basic Constraints** extension. The **Path Length Constraint** attribute defines the maximum number of non self-issued intermediate certificates that can follow the CA certificate in a valid certification path.

The maximum chain depth and path length constraint applies to appliance web server certificates as well as external device and server certificates. The appliance fails to connect to any device or server if it has a certificate chain depth higher than the maximum limit.

Prerequisites

- Privileges: Infrastructure administrator.
- Ensure that no other users are logged into the appliance.

Procedure

1. From the main menu, select **Settings**.
2. Click **Security**.
3. Select **Actions > Import appliance certificate**.
4. Copy the full certificate text and paste it into the box in the following order:

- a. Leaf level CA-signed appliance certificate
 - b. Intermediate CA certificates
 - c. Topmost root CA certificate
5. Click **OK**.
6. After the appliance web server restarts and reconnects, log in to the appliance.
This certificate is also used as the SCMB server certificate.

More information

"Add a certificate" in the online help.

Trusting a certificate

HPE suggests replacing the self-signed certificate with a commercially signed certificate.

Prerequisites

- For trusting a CA root or intermediate certificate: Infrastructure Administrator privileges.
- Adding a managed device.

Procedure

1. When adding a managed device, such as an iLO or a remote server, the SSL certificate, if associated with the managed device or remote server, is fetched and displayed in a dialog box if it is not already trusted by the appliance.
A certificate is trusted if it is a self-signed certificate and has been earlier imported into the appliance or if it is a CA signed certificate and the CA that has signed the certificate has been imported into the appliance earlier.
2. Review the details of the fetched certificate and click **Yes, trust**.

The certificate is added to the appliance trust store. All communication from HPE OneView to the managed device/ remote server hence forth will make use of the trusted certificate. The same capability is available through REST API for scripting users.

View the Certificate settings

Prerequisites

Minimum required privileges: All users

Procedure

1. Navigate from the main menu to the **Settings** screen.
2. Select **Overview > Security > Certificate**.

Download a self-signed certificate

The advantage of downloading and importing a self-signed certificate is to circumvent the browser warning.


In a secure environment, it is never appropriate to download and import a self-signed certificate, unless you have validated the certificate and know and trust the specific appliance.

In a lower security environment, it might be acceptable to download and import the appliance certificate if you know and trust the certificate originator. However, this is not a recommended practice.

Microsoft Internet Explorer and Google Chrome share a common certificate store. A certificate downloaded with Internet Explorer can be imported with Google Chrome as well as Internet Explorer. Likewise, a certificate downloaded with Google Chrome can also be imported by both browsers. Mozilla Firefox has its own certificate store, and must be downloaded and imported with that browser only.

The procedures for downloading and importing a self-signed certificate differ with each browser. The following steps use Microsoft Internet Explorer as an example.

Procedure

1. Click the certificate error in your browser window .
2. Click **View certificates**.
3. Click the **Details** tab.
4. Verify the certificate.
5. Select **Copy to File...**
6. Use the Certificate Export Wizard to save the certificate.
 - a. Select **Base-64 encoded x.509**.
 - b. Specify a file name and location to store the file.
7. **Import a self-signed certificate.**

Import a self-signed certificate

After **downloading a self-signed certificate**, import it into your environment. The following steps use Internet Explorer.

Procedure

1. From the browser menu, select **Tools > Internet Options**.
2. Click the **Content** tab.
3. Click **Certificates**.
4. Click **Import**.
5. Use the Certificate Import Wizard.
 - a. Select the file you downloaded.
 - b. When it prompts you for the certificate store, select **Place all certificates in the following store** and select the **Trusted Root Certification Authorities** store.
 - c. Click **OK** at the security warning.

The next time you log into the appliance, you will not receive the certificate error.

Verify a certificate

You can verify the authenticity of the certificate by viewing it with your browser.

After logging in to the appliance, choose **Settings** > **Security** to view the certificate. Make note of these attributes for comparison:

- Fingerprints (especially)
- Names
- Serial number
- Validity dates

Compare this information to the certificate displayed by the browser, that is, when browsing from outside the appliance.

Nonbrowser clients

The appliance supports an extensive number of REST APIs. Any client, not just a browser, can issue requests for REST APIs. The caller must ensure that they take appropriate security measures regarding the confidentiality of credentials, including:

- The session token, which is used for data requests.
- Responses beyond the encryption of the credentials on the wire using HTTPS.

Passwords

Passwords are likely displayed and stored in clear text by a client like cURL.

Take care to prevent unauthorized users from:

- Viewing displayed passwords
- Viewing session identifiers
- Having access to saved data

TLS connection

The client should specify HTTPS as the protocol to ensure TLS is used on the network to protect sensitive data. If the client specifies HTTP, it will be redirected to HTTPS to ensure that TLS is used.

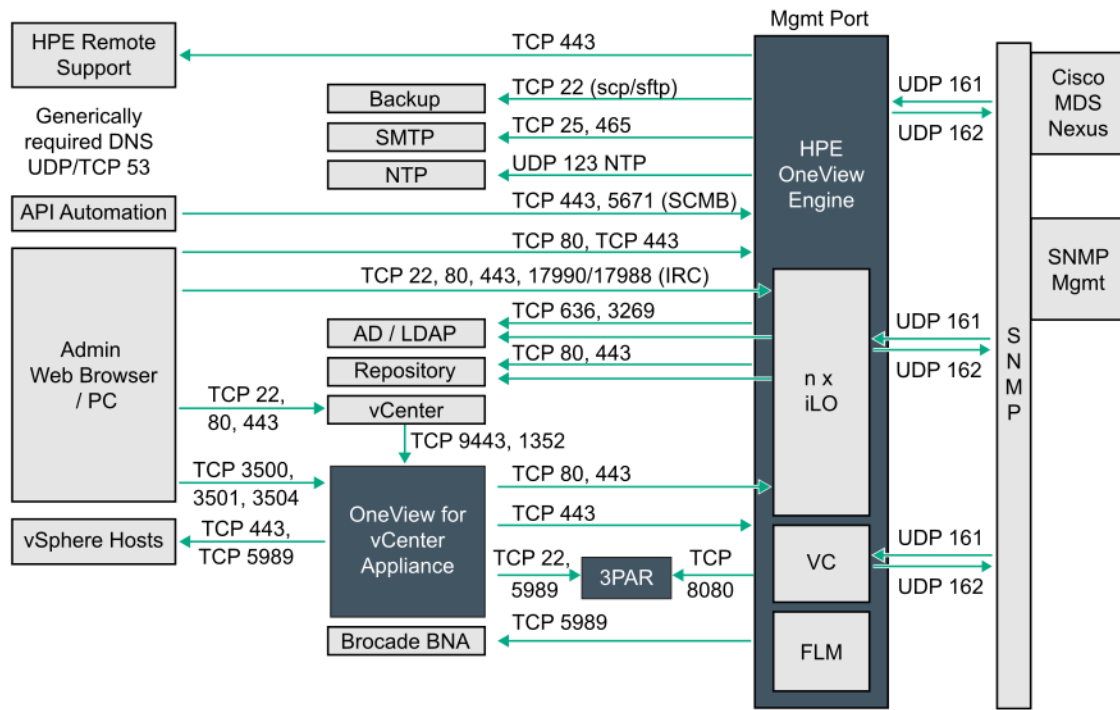
The appliance certificate, which the client requires, allows the TLS connection to succeed. A convenient way to obtain a certificate is to use a browser pointed at the appliance; for more information on obtaining a certificate with a browser, see [**Managing certificates from a browser**](#).

SSH connection

An SSH connection to the appliance is allowed for a maintenance user (to access the maintenance console). The SSH connection connects directly to the maintenance console menu. Enter the user name `maintenance` at the login prompt.

Ports required for HPE OneView

HPE OneView requires specific ports to be available to the appliance to manage servers, enclosures, and interconnects.



Legend:

SCMB = State-Change Message Bus
IRM = iLO Integrated Remote Console

Note: Only default port settings are listed, some are changeable.

Table 54: Ports required for HPE OneView

Port number	Protocol	Use	Description
22	TCP	Inbound and Outbound	Used for SSH and SFTP. SSH is required to communicate with VC Ethernet and FlexFabric interconnect modules. SFTP is required for actions such as firmware upgrades and support dumps.
53	UDP and TCP	Outbound	Used for DNS client queries.
80	TCP	Inbound	Used for the HTTP interface. Typically, this port redirects to port 443; this port provides the access required by the iLO. This port is used by SUT and iSUT for VMware ESXi to connect to the HPE OneView web server.
123	UDP	Inbound	HPE OneView acts as an NTP server, iLO and Onboard Administrator requires access.
123	UDP	Outbound	Used as an NTP client to synchronize the appliance time.

Table Continued

Port number	Protocol	Use	Description
161	UDP	Inbound and Outbound	<p>Supports SNMP GET calls to monitored and managed devices, such as, server iLOs, iPDU, and SAN Managers.</p> <p>Supports SET calls using SNMPv3 for managed devices and SNMPv1 for iPDUs, such as toggling iPDU locator lights and outlet power control.</p>
162	UDP	Inbound and Outbound for trap forwarding from HPE OneView	Used for SNMP trap support from the iLO, Onboard Administrator, and iPDU devices. This port is also used to monitor the VC interconnects and trap forwarding.
443	TCP	Inbound	Used for the HTTPS interface to user interface and APIs. This port is used by SUT for VMware ESXi to connect to the HPE OneView web server.
443	TCP	Outbound	<p>Used for secure SSL access to the iLO, Onboard Administrator, remote support access to Hewlett Packard Enterprise, and other devices.</p> <p>Used for Redfish, RIBCL, SOAP, and iPDU communication.</p>
636	TCP	Outbound	Secure LDAP. Used for enterprise directory integration (Microsoft Active Directory, OpenLDAP)
2162	UDP	Inbound	Used as an alternative SNMP trap port.
3269	TCP	Outbound	Used for Microsoft Active directory LDAP global catalog port.
5671	TCP	Inbound	Allows external scripts or applications to connect to and monitor messages from the SCMB (State-Change Message Bus).
17988	TCP	iLO Integrated Remote Console to iLO	Integrated Remote Console initiating a connection to the iLO.
17990	TCP	Browser to iLO	Provides browser access to the integrated remote console.
50443	TCP	Outbound	Used for RIBCL protocol communication over SSL. This port manages iPDU and related actions. The port collects utilization data to monitor the status and health of iPDU.
63001 and 63002	TCP	Local, on host OS	Used on the host OS where SUT (Smart Update Tools) is installed. The communication is on the localhost between the SUT and SUM (Smart Update Manager) processes.

Controlling access to the appliance console

Use the hypervisor management software to restrict access to the appliance, which prevents unauthorized users from accessing the password reset and service access features. See **Restricting console access** on page 141.

Typical legitimate uses for access to the console are:

- Troubleshooting network configuration issues
- Resetting an appliance administrator password
- Enabling service access by an authorized technical support representative

The virtual console is displayed in a graphical console; password reset and Hewlett Packard Enterprise Services access use a non-graphical console.

Switching from one console to another (VMware vSphere and Microsoft Hyper-V)

The virtual appliance console is displayed in a graphical console; password reset and Hewlett Packard Enterprise Services access use a non-graphical console.

Procedure

1. Open the virtual appliance console.
2. Press and hold **Ctrl+Alt**.
3. Press and release the space bar.
4. Press and release **F1** to select the non-graphical console or **F2** to select the graphical console.

Switching from one console to another (KVM)

The virtual appliance console is displayed in a graphical console; password reset and Hewlett Packard Enterprise Services access use a non-graphical console.

Procedure

1. Open the Virtual Machine Manager.
2. In the Menu bar, select **Send Key** > **Ctrl+Alt+F1** for the non-graphical console or select **Send Key** > **Ctrl+Alt+F2** for the graphical console.

Enable or disable authorized services access

When you first start up the appliance, you can choose to enable or disable access by authorized technical support. By default, authorized technical support personnel are allowed to access your system through the appliance console and diagnose issues that you have reported.

NOTE: There are several ways to allow authorized support representatives to access the appliance for advanced troubleshooting operations:

- If on site, the authorized support representative can use the appliance console or an SSH session to the HPE OneView maintenance console.
- A shared virtual desktop session where the authorized support representative works with you to obtain a one-time password and you allow him to access the appliance console or maintenance console through the virtual desktop.
- You can enable service console access and the service sessions features to allow the authorized support representative to access HPE OneView directly through a secure tunnel.

Support access is privileged, which enables the authorized technical support representative to debug any problems on the appliance. Access to the services access account requires the technician to obtain a one-time password using a challenge/response mechanism similar to the one for a password reset.

Any time after the initial configuration of the appliance, an Infrastructure administrator can enable or disable services access through the user interface.


Prerequisites

Privileges: Infrastructure administrator

Procedure

1. From the main menu, select **Settings**.
2. Click the **Edit** icon in the **Security** panel.
The **Edit Security** window opens.
3. Select the appropriate setting for **Service console access**:
 - a. **Disabled** to prevent access to the console.
 - b. **Enabled** to allow access to the console.
4. Click **OK**.

You can also use a `/rest/appliance/settings/enableServiceAccess` REST API to enable or disable services access.

 **CAUTION:** Hewlett Packard Enterprise recommends that you enable access to allow the authorized support representative to access the appliance to troubleshoot the issues.

More information

About the appliance maintenance console

Restricting console access

You can restrict console access to the virtual appliance through secure management practices of the hypervisor itself.

For VMware vSphere, this information is available from the VMware website:

<http://www.vmware.com>

In particular, search for topics related to vSphere's Console Interaction privilege and best practices for managing VMware's roles and permissions.

For Microsoft Hyper-V, restrict access to the console through role-based access. For information, see the Microsoft website:

<http://www.microsoft.com>

Files you can download from the appliance

You can download the following data files from the appliance:

- **Support dump**

By default, all data in the support dump is encrypted and accessible by an authorized technical support only. The encryption protects any sensitive customer data contained in the support dump (such as IP addresses, IP address pools, hostnames, and WWNs).

- **Backup file**

All data in the backup file is in a proprietary format. Hewlett Packard Enterprise recommends that you encrypt the file according to your organization's security policy.

- **Audit logs**

Session IDs are not logged, only the corresponding logging IDs are logged. Passwords and other sensitive data are not logged.

More information

Understanding the audit log

Handling MD5 certificates

Older devices, such as, servers with iLO 2 management processors can have Transport Layer Security (TLS) certificates with digital signatures based on the MD5 hashing algorithm. Such certificates are a serious security risk. The MD5 algorithm has been replaced by the Secure Hash Algorithm, such as SHA-256, for modern certificate digital signatures.

HPE OneView 4.2 performs periodic status checks on the certificates in the trust store. If a certificate using an MD5 hashing algorithm is found, the following alert is displayed:

- **Message:** Certificate with alias name **<alias name>** is using an insecure digital signature with MD5 hashing algorithm.
- **Resolution:** Certificates with MD5 digital signatures are insecure and deprecated. They will not be supported in future HPE OneView releases. If this is a device certificate, update the certificate with a strong digital signature. If this is a CA root or intermediate certificate, work with your public key infrastructure (PKI) administrator to update the certificate.

NOTE: Updating the certificate might need firmware update on the managed device.

These MD5 certificates are marked as *Deprecated* in HPE OneView on the **Settings > Manage Certificates** screen.

For iLO2, all the HPE OneView iLO2 firmware versions support SHA-based certificates. However, iLO firmware upgrades do not change an existing certificate of the device. Only iLO factory reset operations and change in the hostname of iLO regenerated the self-signed certificates of iLO. Similarly, certificate authority issued certificates might also contain MD5 digital signatures and a new iLO certificate signing request is required to obtain an updated certificate. For more information, see the *iLO User Guide*.

You can determine the devices that are using certificates with MD5 digital signatures by using `HPE OneView / rest/certificates` REST API. You can use the HPE OneView PowerShell interface, POSH-HPOneView, available at <https://hewlettpackard.github.io/POSH-HPOneView>.

For example:

- `Connect-HPOVMgmt -Hostname <your appliance> -Username <OneView username> [-AuthLoginDomain <AD or LDAP domain>]`
- `$certs = Send-HPOVRequest "/rest/certificates"`
- `$md5certs = @()`
- `$certs.members | foreach-object {$md5certs += New-Object PSObject -property @{commonName=$_.certDetails.commonName; aliasName=$_.aliasName; signature=$_.certDetails.signatureAlgorithm }}`
- `$md5certs | ? {$_.signature -match "MD5" } | format-table`

NOTE: This technique only identifies certificates that are present in the HPE OneView trust store. The certificates include certificate authority root and intermediate certificates and any device self-signed certificates. When the device has a CA-signed certificate, the leaf certificate may not be present in the OV trust store and the information is not displayed in an alert message. For such device certificates, examine the certificate configured on the individual device itself.

Modeling scope-based access control in HPE OneView

I want to ...	Learn more
<ul style="list-style-type: none">• <u>Implement scope-based access control</u>• "Troubleshoot authorization failures" in the Online help• "See more tasks" in the Online help	<ul style="list-style-type: none">• <u>About user accounts</u>• <u>About permissions</u>• <u>About user roles</u>• <u>About scope-based access control</u>• <u>About scopes</u>

About scope-based access control

HPE OneView uses a role-based access control (RBAC) mechanism to define privileges and control user access. Under RBAC, the access rights defined by the role apply to all resources in a resource category. Scope-based access control (SBAC) is an extension of the RBAC mechanism that allows you to restrict the rights granted by a role to a subset of resources.

You can use scope-based access control to grant privileges to users or directory groups in the form of permissions. A permission consists of a role and an optional scope. Roles grant access rights to perform actions (create, read, update, delete or use) on all resources in a resource category. A resource can be assigned to zero or more scopes in order to restrict operations that can be performed on it. When specified as part of a permission, a scope further restricts the rights granted by the role to a subset of resources. You can assign multiple permissions to a user or a directory group.

More information

About scopes

Scope-based access control authorization semantics

Scope-based access control facts

Scope-based access control implementation process

Scope-based access control authorization semantics

Multiple authorization checks might be required to authorize a single HPE OneView request. For example, an `Update` authorization check is always performed when an update request is received. In addition, if the `Update` request forms a new association (for example, assigns a server profile to a server hardware, assigns a network to a network set, or assigns a volume template to a server profile template), a `Use` check is required to authorize creation of the new association. While a single authorization check request is required to change the name of a server profile, a request to add a network and a volume to a server profile requires one `Update` and two `Use` authorization checks. For a single `Create` or `Update` request, these multiple `Use` checks can be authorized by different permissions.

The following table describes the five types of authorization checks HPE OneView performs:

Action	Action semantic	Authorization check semantics	Example
Create	Controls the right to create a resource.	<p>A permission must grant the user <code>Create</code> rights on the resource category. If a single scope-restricted permission grants <code>Create</code>, the resource is assigned to the permission scope. If multiple scoped permissions grant <code>Create</code>, the desired scope must be specified.</p> <hr/> <p>NOTE: When resource creation is granted by one or more scoped permissions it must be assigned to one of the scopes in order for the user to be able to operate on it.</p> <hr/>	If a user is granted server administrator rights in the Test scope, that user is allowed to create server profiles in the Test scope only. If the user is granted server administrator rights in the Test and Production scopes, that user is only allowed to create server profiles in the Test and Production scopes.
Delete	Controls the right to delete a resource.	<p>A permission must grant the user <code>Delete</code> rights on the resource category. If the permission is restricted by scope, the user is only allowed to delete resources assigned to the permission scope.</p> <hr/> <p>NOTE: Unless explicitly noted in the API documentation as an exception, no further authorization checks are performed on a delete request. This includes actions performed by HPE OneView to bring the data model to a consistent state (for example, removing the definition of server hardware and interconnects when removing an enclosure). See the <i>HPE OneView API Reference</i> for more information.</p> <hr/>	If a user is granted Server administrator rights in the Test scope, that user is only allowed to delete server profiles assigned to the Test scope.
Update	Controls the right to modify a resource. This includes changing the state of a resource.	A permission must grant the user <code>Update</code> rights on the resource category. If the permission is restricted by scope, the user is only allowed to update resources assigned to the permission scope.	If a user is granted Server administrator rights in the Test scope, that user is only allowed to power on/off servers assigned to the Test scope.

Table Continued

Action	Action semantic	Authorization check semantics	Example
Read	Controls the right to view a resource.	A permission must grant the user Read rights on the resource category. Read rights are not restricted by scope.	
Use	<p>Controls the right to associate one resource with another resource. Use rights are always checked in the context of a Create or Update operation. Use rights are not checked when a resource is unassigned.</p> <p>Exception: Use rights are required to unassign a template (for example, server profile template or volume template) from its associated resource.</p>	<p>A permission must grant the user the following rights:</p> <ul style="list-style-type: none"> The role must have Create or Update rights to the request resource category. The role must have Use rights on the associated resource category. If the permission is restricted by scope, both the request resource and associated resource must be assigned to the permission scope. <p>NOTE: The resource which is being assigned is referred to as the associated resource and the resource to which it is being assigned is referred to as the request resource.</p>	<p>If a user is granted Server administrator rights in the Test scope, that user is allowed to assign a server hardware to a server profile or assign a network to a network set in the Test scope only.</p> <p>However, no Use checks are performed when you set the server hardware to unassigned in a server profile or remove a SAN storage volume.</p>

More information

About permissions

"Assign a resource to a scope from the Scopes page" in the online help

Scope-based access control facts

- You can continue to use role-based access control without restricting a user's rights by scope. HPE OneView uses the notation, `All resources`, to indicate that a permission is not restricted by scope. `All resources` is not a scope.
- Authorization checks are only performed on changes explicitly requested by the user. For example, if a user assigns a server to a server profile, HPE OneView performs an `Update` check on the server profile, and a `Use` check on the server. No other `Use` checks are performed. **SBAC Authorization Semantics** provides details.
- Not all resource categories support scope. A scope check is not performed on resource categories that do not support scope. **Scope-enabled resource categories** lists the resource categories that support scope.
- Scope-enabled resources that are not assigned to a scope are only manageable by users whose permissions are not restricted by scope. For example, an Infrastructure administrator whose rights are not restricted by scope, can manage any resource. However, a user who is granted Server administrator rights in the Test scope can only manage resources assigned to the Test scope.
- The Scope operator and Scope administrator grant users the right to manage scopes. The rights granted by these roles may be restricted by scope. Users can only manage scopes that are assigned to the permission scope. For example, if the Infrastructure administrator wants to grant a user the right to assign Production resources to either the Finance or Marketing scopes, the Infrastructure administrator must:

- Assign (Scope operator, Production) permission to the user.
- Assign Finance and Marketing scopes to the Production scope.

NOTE: Assigning Finance scope to the Production scope does not assign Finance resources to the Production scope. It merely assigns the Finance scope instance to the Production scope. As the Finance scope is assigned to the Production scope, the user is allowed to update the Finance scope. The user is not allowed to update the Production scope as the user is not assigned to the Production scope. A permission grants rights to resources that are assigned to the permission scope. It does not grant rights to the permission scope.

- Resources discovered or created as a consequence of a user-initiated `Create` request are assigned to the scope specified by the user on the request. For example, logical interconnects created during a 'Create logical enclosure' request are assigned to the same scopes as the logical enclosure.
- Resources automatically discovered by HPE OneView are not assigned to a scope. If required, the resources must be explicitly assigned to a scope.

NOTE: Rights assigned to the Hardware Setup user are not restricted by scope. Hence, resources explicitly added by the Hardware Setup user (for example, rackmount servers) are not assigned to the scope.

Scope-based access control implementation process

Design the authorization model

To design your authorization model:

1. **Describe users and groups who need HPE OneView access**
2. **Determine the role that best aligns with the desired rights**
3. **Determine resources to include in scopes to restrict rights**

You might need to iterate between these steps, refining your requirements, as you define your model.

Describe users and groups who need HPE OneView access

1. Make a list of the users and groups who need access to HPE OneView.
2. Identify categories of users requiring the same rights, for example, IT managers who need read-only access to HPE OneView, IT senior staff who need full access to HPE OneView, test engineers who need to upgrade the firmware on the test servers.
3. Identify the scripts or client applications that use the HPE OneView API to retrieve data or perform operations. For example, consider an inventory reporting application or a daily critical alert report application that requires read access to HPE OneView.

More information

Scope-based access control example: Scenario overview

Example: Identify users and groups

Determine the role that best aligns with the desired rights

Once you have identified the users and groups, do the following:

1. For each class of users, determine the HPE OneView role that most closely matches the desired privileges. Your goal should be to find the least privileged role that grants the required privileges. **Action privileges for user roles** provides details on the rights granted by each role.
2. Determine if the rights granted by the role must be restricted by scope.
3. For each class of users, describe the actions the users can perform. Focus on actions that require create, delete or update rights.
4. Identify the HPE OneView resource categories the user should be able to manage.
5. Consider the actions a user must not be allowed to perform.

Role definitions grant rights to a variety of secondary resource categories. Within a role definition, the rights assigned to the secondary resource categories are defined to be consistent with the rights assigned to the main resource categories. Focus on the categories listed in the HPE OneView main menu. The following table provides the mapping:

HPE OneView main menu	Related role category names
Firmware Bundles	firmware-drivers
Interconnects	interconnects, sas-interconnects
Logical Interconnect Groups	logical-interconnect-groups, sas-logical-interconnect-groups
Logical Interconnects	logical-interconnects, sas-logical-interconnects
Networks	ethernet-networks, fcoe-networks, fc-networks
Power Delivery Devices	power-devices
SAN Managers	fc-device-managers
SANs	fc-sans
Settings	appliance
Users and Groups	users, grouptorolemappings
Volume Sets	storage-volume-sets
Volume Templates	storage-volume-templates
Volumes	storage-volumes

A role might need to be excluded from consideration if it grants a user the right to perform an action you do not want to allow. But, do not exclude the role from consideration yet. If the category supports scope, it might be possible to use scope restrictions to prevent the user from performing the action (with the exception of `Create`).

More information

Scope-based access control example: Scenario overview

Example: Determine the best fit HPE OneView role

Determine resources to include in scopes to restrict rights

NOTE: You can skip this step for permissions that are not restricted by scope.

1. Define the set of resources that must be included in the permission scopes used to restrict rights.
2. Identify resource categories that support scope. **Scope-enabled resource categories** lists the resource categories that support scope.

NOTE:

- HPE OneView checks only role permissions on resources in resource categories that are not scope-enabled.
 - The need to assign resources to scopes is driven by the **Scope-based access control authorization semantics**.
-

More information

Scope-based access control example: Scenario overview

Example: Define permission scopes

Configure the authorization model

To configure the authorization model in HPE OneView:

1. **Create** a scope.
2. Assign a resource to a scope either from the **scopes page** or the **resource page**.
3. **Add a local user with specialized access** or **Add a group with directory-based authentication**.
4. **Verify** that the rights defined for the user are consistent with your expectations.

Scope-based access control example: Scenario overview

An example scenario is used throughout this section to highlight how scope-based access control can be used to restrict access. In this scenario, Company X is launching a cloud-based pilot project for both virtual machines (VM) and bare-metal servers.

A single HPE OneView appliance is configured to host both the environments. Corporate IT is responsible for managing hardware support as well as shared infrastructure components. VM Cloud IT is responsible for managing the VM cloud environment. Service (SRV) Cloud IT is responsible for managing the bare-metal server reservation process. Finance and Human Resource (HR) users are the consumers of the bare-metal servers. All five groups need access to HPE OneView. The solution must ensure that users are only allowed to manage the assigned resources.

A rack with three enclosures is used exclusively for the VM Cloud pilot. A rack with two enclosures is used exclusively for the SRV Cloud pilot. The Finance and HR departments are allocated servers in the enclosures assigned to the SRV Cloud pilot.

More information

Example: Identify users and groups

Example: Determine the best fit HPE OneView role

Example: Define permission scopes

Example: Identify users and groups

Corporate IT works with VM Cloud IT, SRV Cloud IT and Corporate Security to identify the groups who need access to HPE OneView. Users in five departments (Corporate IT, Finance, Human Resources, SRV Cloud IT and VM Cloud IT) need access to the HPE OneView appliance. Corporate IT and VM Cloud IT users are organized by function. Different functions have different rights.

The results of the exercise are summarized in the following table:

Department	Function	Responsibility
Corporate IT	Senior technologists	HPE OneView appliance and all managed resources
Corporate IT	Server administrators	All server resources
Corporate IT	Network administrators	All network resources
Corporate IT	Storage administrators	All storage resources
Finance	OS and Application administrators	OS and applications operating on servers assigned to the Finance department
Human Resources	OS and Application administrators	OS and applications operating on servers assigned to the Human Resources department
SRV Cloud IT	Server Cloud administrators	SRV Cloud provisioning and allocation process
VM Cloud IT	Server administrators	All VM Cloud server resources
VM Cloud IT	Network administrators	All VM Cloud network resources

Example: Determine the best fit HPE OneView role

The Corporate IT Server administrator, Network administrator, and Storage administrator functions align well with the rights defined by the similarly named HPE OneView roles. Corporate IT Senior technologists have complete access rights to the appliance. The access rights assigned to the Corporate IT administrators are not restricted by scope.

The corporate IT users are granted the following permissions:

Department	Function	Permission Role	Permission Scope
Corporate IT	Senior technologists	Infrastructure administrator	All resources
Corporate IT	Server administrators	Server administrator	All resources
Corporate IT	Network administrators	Network administrator	All resources
Corporate IT	Storage administrators	Storage Administrator	All resources

The VM Cloud IT administrators have experience managing the HPE OneView resources. As with Corporate IT, the VM Cloud IT Server administrator and Network administrator functions align well with the rights defined in the similarly named HPE OneView roles. Rights assigned to the Cloud IT administrators are restricted to resources assigned to the VM Cloud.

Corporate IT identified a few additional considerations:

- Data centers, racks, power delivery devices and unmanaged devices are not restricted by scope. The Server administrator role grants **Create**, **Read**, **Update** and **Delete** rights to each of the above resources categories. For this pilot, neither the power delivery devices nor unmanaged devices are managed by HPE OneView. Changes to

data center and rack resources are considered low impact. Corporate IT discussed this with VM Cloud IT management. They agreed to take responsibility for ensuring that their users do not modify the data center or rack resources.

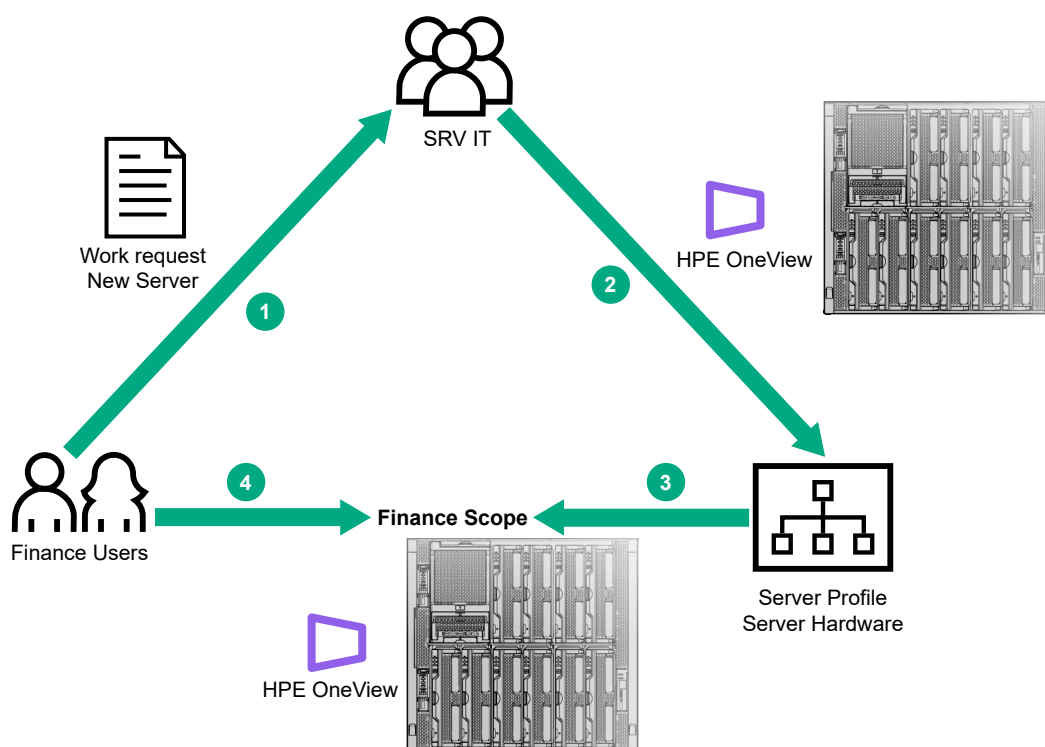
- SAN managers, SANs, and storage systems are considered shared resources and managed exclusively by the Corporate IT. The VM Cloud IT users must not be granted Storage administrator rights.
- The VM Cloud IT administrators are only allowed to create volumes using volume templates created by the Corporate IT. This requirement can be enforced using scopes. When creating a volume, the user must select either a volume template or storage pool. As the VM Cloud IT permissions are restricted by scope, the `Use` check only allows the selection of volume templates and storage pools in the VM Cloud scope. Only approved volume templates are placed in the VM Cloud scope. No storage pools are assigned to the VM Cloud scope.

The VM Cloud IT users are granted the following permissions:

Department	Function	Permission Role	Permission Scope
VM Cloud IT	Server administrators	Server administrator	VM Cloud
VM Cloud IT	Network administrators	Network administrator	VM Cloud

The SRV Cloud IT administrators have less experience with HPE OneView. As a result, Corporate IT retains responsibility for managing the SRV Cloud enclosures. However, SRV Cloud IT is responsible for the SRV Cloud provisioning and reservation process.

A high-level overview of the SRV Cloud reservation process is shown here.



The illustration depicts the following:

1. A department (for example, Finance) user submits a request to the SRV Cloud IT for a new server.
2. A member of SRV IT uses HPE OneView to create a server profile using an available server assigned to the SRV Cloud scope.

3. A member of SRV IT assigns the server profile and physical server to the department requesting the server.

4. The department user is now allowed to use HPE OneView to manage the server.

As depicted in the flow, SRV Cloud IT needs `Create`, `Delete` and `Update` rights to the server profiles. They have also requested the right to create, delete and update server profile templates. For this pilot, SRV Cloud servers only use local storage. They should not be allowed to create volumes.

Corporate IT analyzed the HPE OneView role definitions and determined that the Server profile architect role was the best fit. The Server profile architect role grants the following rights:

Category	Rights	Analysis
Labels	Create, Read, Update, Delete	Allows SRV IT users to assign labels to any resource in a category granted <code>Update</code> rights by the role (for example, assign a label to any server hardware). As labels are not used to control IT, VM IT Cloud or SRV IT Cloud operations, granting users this right was not viewed as an issue.
Network Sets	Create, Read, Update, Delete	Allows SRV IT to create network sets in the SRV Cloud scope.
Server Hardware	Read, Update	Aligned with desired privileges.
Server Profile Templates	Create, Read, Update, Delete	Aligned with desired privileges.
Server Profiles	Create, Read, Update, Delete	Aligned with desired privileges.
Volumes	Create, Read, Update, Delete	Scope can be used to prevent SRV IT from managing volumes. For SRV IT to create a volume, either a volume template or storage pool must be assigned to the SRV Cloud scope. To update or delete a volume, the volume must be assigned to the SRV Cloud scope.

SRV Cloud IT also needs to assign the SRV Cloud resources to the Human Resources and Finance scopes. The Scope operator role grants users the rights to assign resources to scopes. This right must be restricted to the SRV Cloud resources. SRV Cloud IT users are granted both permissions.

Department	Function	Permission Role	Permission Scope
SRV Cloud IT	Server Cloud administrators	Server profile architect	SRV Cloud
SRV Cloud IT	Server Cloud administrators	Scope operator	SRV Cloud

Finance and Human Resources users are only allowed to update the servers and server profiles assigned to their department.

Server profile operator rights align well with the desired Finance and Human Resources rights. The following table describes the results of an analysis performed by Corporate IT.

Category	Rights	Analysis
Labels	Create, Read, Update, Delete	Operations on labels are not restricted by scope. The ability to add or remove labels to resources that are not in the user's authorized scope is not viewed as a risk.
Server Hardware	Read, Update	Aligned with desired privileges.
Server Profiles	Read, Update	Aligned with desired privileges.

Human Resources and Finance users are granted the following permissions:

Department	Function	Permission Role	Permission Scope
Finance	OS/Application administrators	Server profile operator	Finance
Human Resources	OS/Application administrators	Server profile operator	Human Resources

Example: Define permission scopes

In the **previous** step, Corporate IT identified ten permissions. Six permissions are restricted by four distinct scopes. Corporate IT needs to create four scopes: VM Cloud, SRV Cloud, Human Resources and Finance.

Department	Function	Permission Role	Permission Scope
Corporate IT	Senior technologists	Infrastructure administrator	All resources
Corporate IT	Server administrators	Server administrator	All resources
Corporate IT	Network administrators	Network administrator	All resources
Corporate IT	Storage administrators	Storage administrator	All resources
Finance	OS/Application administrators	Server profile operator	Finance
Human Resources	OS/Application administrators	Server profile operator	Human Resources
SRV Cloud IT	Server Cloud administrators	Server profile architect	SRV Cloud
SRV Cloud IT	Server Cloud administrators	Scope operator	SRV Cloud
VM Cloud IT	Server administrators	Server administrator	VM Cloud
VM Cloud IT	Network administrators	Network administrator	VM Cloud

VM Cloud IT is responsible for managing their enclosures. The following table summarizes the results of the analysis performed by Corporate IT to determine the resources that must be assigned to the VM Cloud scope.

Operation	Analysis
Create networks	Created by VM Cloud IT and automatically added to the VM Cloud scope. SANs are considered as shared resources and not restricted by scope. VM Cloud IT is allowed to assign SANs to Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) networks.
Create network sets	Created by VM Cloud IT and automatically added to the VM Cloud scope. VM Cloud IT is only allowed to assign networks created by VM Cloud IT to the VM Cloud network sets.
Create logical interconnect groups	Created by VM Cloud IT and automatically added to the VM Cloud scope. VM Cloud IT is only allowed to assign networks created by VM Cloud to the uplink sets.

Table Continued

Operation	Analysis
Create enclosure groups	Created by VM Cloud IT and automatically added to the VM Cloud scope. VM Cloud IT is only allowed to assign logical interconnect groups created by VM Cloud IT to enclosure groups.
Create logical enclosures	Created by VM Cloud IT and automatically added to the VM Cloud scope. The logical interconnects created during this operation are automatically added to the VM Cloud scope. VM Cloud IT needs access to the enclosures assigned to the VM Cloud pilot. Corporate IT must assign the three enclosures to the VM Cloud scope. As the firmware bundles are restricted by scope, VM Cloud IT needs access to approved firmware bundles. Corporate IT must assign the authorized firmware bundles to the VM Cloud scope.
Power on/off/Refresh interconnects	To allow VM Cloud IT to manage the VM Cloud interconnects, Corporate IT must assign the interconnects in the VM Cloud enclosures to the VM Cloud scope.
Power on/off/Refresh drive enclosures	To allow VM Cloud IT to manage the drive enclosures in the VM Cloud enclosures, Corporate IT must assign the drive enclosures to the VM Cloud scope.
Launch console/Power on/off/Reset/Refresh server hardware	Corporate IT must assign the blades in the VM Cloud enclosures to the VM Cloud scope.
Create server profile templates	Created by VM Cloud IT and automatically added to the VM Cloud scope. In order to assign resources to the server profile templates, VM Cloud IT needs access to firmware bundles, networks, network sets and volume templates. Corporate IT must assign the authorized volume templates to the VM Cloud scope. Image Streamer is not configured for this pilot. Therefore, access to the OS deployment plans is not required.
Create server profiles	Created by VM Cloud IT and automatically added to the VM Cloud scope. In addition to rights granted above, VM Cloud IT needs access to the server hardware.

Corporate IT performed a similar analysis for the SRV Cloud scope. SRV Cloud IT users are only allowed to perform server-related operations. The following table summarizes the results:

Operation	Analysis
Launch console/Power on/off/Reset/Refresh server hardware	Corporate IT needs to assign the blades in the SRV Cloud enclosures to the SRV Cloud scope.
Create server profile templates	Created by SRV Cloud IT and automatically added to the SRV Cloud scope. In order to assign resources to server profile templates, SRV Cloud IT needs access to firmware bundles, networks and network sets. Corporate IT must assign firmware bundles, networks and network sets to the SRV Cloud scope.

Table Continued

Operation	Analysis
Create server profiles	Created by SRV Cloud IT and automatically added to the SRV Cloud scope. In addition to rights granted above, SRV Cloud IT needs access to server hardware.
Assign SRV Cloud resources to Human Resources and Finance scopes	Both an <code>Update</code> and <code>Use</code> authorization check are performed when assigning a resource to a scope. For example, to assign a blade to the Human Resources scope, SRV Cloud IT needs <code>Update</code> rights on the Human Resources scope and <code>Use</code> rights on the server hardware. Additionally, both the Human Resources scope and the blade must be assigned to the SRV Cloud scope. SRV Cloud IT is only allowed to update the Human Resources and Finance scopes. When assigning a resource to a scope there is no concept of a hierarchy. Assigning a scope to a scope restricts operations that can be performed on the scope; it does not affect access to resources assigned to either scope. Corporate IT must assign the Human Resources and Finance scope instances to the SRV Cloud scope.

Finally, Corporate IT completes the analysis of the Human Resources and Finance scopes.

Operation	Analysis
Launch console/Power on/off/Reset/Refresh server hardware	SRV Cloud IT is responsible for assigning SRV Cloud server hardware to the Human Resources and Finance scopes.
Update server profiles	SRV Cloud IT is responsible for assigning SRV Cloud server profiles to the Human Resources and Finance scopes. SRV Cloud IT is also allowed to assign SRV Cloud firmware bundles to the Human Resources and Finance scopes. SRV Cloud IT is still debating on whether or not Human Resources and Finance users are allowed to update server firmware.

To summarize, the authentication model for the pilot defines four permission scopes and nine directory group accounts with associated permissions.

Permission Scope	Resources explicitly assigned to the scope by Corporate IT
Finance	None
Human Resources	None
SRV Cloud	<p>The blades contained in the two enclosures dedicated to the SRV Cloud pilot.</p> <p>The firmware bundles approved for use by SRV Cloud IT.</p> <p>The networks approved for use by SRV Cloud IT.</p> <p>The Finance and Human Resources scope resource instance. This is required to allow SRV Cloud IT to assign SRV Cloud resources to the Finance and Human Resources scopes.</p>
VM Cloud	<p>The three enclosures dedicated to the VM Cloud pilot.</p> <p>The blades contained in the three enclosures.</p> <p>The interconnects contained in the three enclosures.</p> <p>The drive enclosures contained in the three enclosures.</p> <p>The firmware bundles approved for use by VM Cloud IT.</p> <p>The volume templates approved for use by VM Cloud IT.</p>

Directory Group	Permissions
CorpIT-FULL	(Infrastructure administrator, All resources)
CorpIT-NA	(Network administrator, All resources)
CorpIT-SA	(Server administrator, All resources)
CorpIT-StA	(Storage administrator, All resources)
Finance-Admins	(Server profile operator, Finance)
HR-Admins	(Server profile operator, Human Resources)
SRVCloudIT-Admins	(Server profile architect, SRV Cloud); (Scope operator, SRV Cloud)
VMCloudIT-SA	(Server administrator, VM Cloud)
VMCloudIT-NA	(Network administrator, VM Cloud)

Certificate management

HPE OneView uses HTTPS to communicate with managed devices and remote servers. HTTPS is based on Transport Layer Security (TLS). HTTPS and TLS offer the following benefits:

- Confidentiality: Data is encrypted on the wire using symmetric key cryptography.
- Message integrity: Secure hash functions guarantee integrity.
- Authentication: HPE OneView authenticates the remote end point of the HTTPS connection. Public key cryptography is used to authenticate HTTPS and TLS.

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

Public key cryptography uses public and private key pairs to encrypt and decrypt data. In a public key system, digital certificates certify the ownership of the public key. Digital certificates also certify the allowed usage of that key (for example, digital signatures, certificate signing, encryption).

HPE OneView supports the use of both self-signed certificates and certificate authority-issued (CA) certificates in a formal public key infrastructure (PKI).

The security model for each differs and is described in the following sections:

- **Establishing trust between a web browser and HPE OneView**
- **Establishing trust between HPE OneView and remote devices**
- **Certificate Revocation Lists**
- **Device-specific certificate handling**
- **Enabling and disabling certificate validation**
- **Managing servers with iLO configured for two-factor authentication**

HPE OneView appliance certificate

The default HPE OneView appliance certificate in a VM appliance is a FIPS-compliant SHA-256 certificate with 2048-bit key length.

Establishing trust between a web browser and HPE OneView

When you log into an HPE OneView appliance, the browser might display security warnings that the appliance certificate is not present in the browser trust store. Depending on whether an appliance uses a self-signed certificate or a certificate authority-signed (CA) certificate, follow these steps to validate the certificate:

- **Self-signed-certificate**

1. View the appliance certificate fingerprint using HPE OneView **Settings > Security > Certificate** screen from the appliance console.
2. Validate that the fingerprint matches the one displayed by the browser when connecting to HPE OneView. If the fingerprints match, store the HPE OneView certificate in browser trust store.

NOTE: To view the appliance self-signed certificate without using HTTPS, use the hypervisor user interface to connect to the console interface.

- **CA-signed certificate**

Add the CA-root and any appropriate intermediates that has signed the HPE OneView certificate to the browser trust store.

NOTE: HPE OneView requires that the root and any intermediate certificates that form the full chain of the appliance CA-signed certificate are also imported into HPE OneView when the CA-signed appliance certificate is imported to the appliance.

Establishing trust between HPE OneView and remote devices

A session between an HTTPS or TLS client and an HTTPS server is considered secure only when the client and server can exchange the appropriate certificates. For example, if HPE OneView is communicating with the server iLO, HPE OneView is the client and iLO is the server. To ensure a secure connection, HPE OneView must have the appropriate iLO certificates (which can be the iLO self-signed certificate, or a CA-root certificate and any intermediate certificates used to sign the iLO certificate in a PKI environment) in the local trust store.

NOTE: HPE OneView requires that the root and any intermediate certificates that form the full chain of the appliance CA-signed certificate are also imported into HPE OneView when the CA-signed appliance certificate is imported to the appliance.

More information

Certificate authority or public key infrastructure-based trust

Using scripting to enable PKI or CA-based trust

User-verified initial trust

Automatic initial trust

Certificate authority or public key infrastructure-based trust

The certificate authority (CA) or public key infrastructure-based trust approach assumes that the organization has an established public key infrastructure (PKI). A PKI is a set of roles, policies, and procedures required to create, manage, distribute, use, store, revoke digital certificates and manage public-key encryption.

For secure communication between HPE OneView and the devices based on a common root of trust, before HPE OneView communicates with the device, the administrator must:

- Upload any CA-issued root and intermediate certificates required by the PKI of an organization into HPE OneView. These certificates form the root of trust for all certificates issued by a CA. The administrator must also upload any applicable Certificate Revocation Lists (CRL) along with the CA root and intermediate certificates.
- Securely connect to each of the remote devices. This is typically accomplished by connecting to the device before it is connected to the management LAN (for example, when the device is isolated on a private network segment).
- Obtain a certificate signing request (CSR) for each device.

For information on the support for various devices, see the *HPE OneView Support Matrix* on the **Hewlett Packard Enterprise Information Library**.

- Get the CSRs signed by the certificate authority.
- Upload the resultant certificate to each device.

All communications between HPE OneView and the device are now secure due to the common root of trust. Typically, the CA-signed leaf certification for a device does not need to be added to the HPE OneView trust store. The root and any intermediate certificates are all that is required to validate trust for the device. However, if a discovered device uses CA-signed certificates and communications with the device occur before the user adds the CA root certificate and appropriate

intermediate certificates to the HPE OneView trust store, the CA-signed leaf certificate for the device is automatically added to the trust store and is treated as a self-signed certificate.

Trusting a root CA certificate - “iLO/iLO 3/iLO 4/iLO 5 Default Issuer (do not trust)” certificate

When you trust an iLO self-signed certificate using the **Settings > Security > Manage Certificates > Add Certificate** screen and select **Fetch from IP address or hostname**, always enable the **Force trust leaf certificate** option, that ensures only the iLO leaf certificate is added to the trust store. If you forget to use this option, the iLO **Default Issuer (do not trust)** certificate is sometimes added to the trust store. In that case, delete the **Default Issuer (do not trust)** certificate. Never place these certificates into the trust store as they can cause errors when present.

Using scripts to enable PKI or CA-based trust

When you work in an environment which uses self-signed certificates, use the HPE OneView REST APIs to facilitate a scripting-based migration to CA-signed certificates.

For example, enclosures and the appliance all provide REST APIs for generating CSRs and uploading the resulting CA-signed certificates and CRLs.

User-verified initial trust

The user-verified initial trust approach applies to devices that use self-signed certificates. HPE OneView displays the certificate for the device, including the certificate fingerprint. You can compare the fingerprint to one you have obtained from the device in a secure, out-of-band manner. If the device fingerprint displayed by HPE OneView matches the fingerprint obtained by the out-of-band approach, you are assured that the device is trusted and the self-signed certificate is safe to add to the HPE OneView trust store.

The key to this security model is to securely obtain the certificate fingerprint for the device. **Automatic initial trust** provides instructions.

Automatic initial trust

The automatic initial trust approach applies to devices such as server hardware and onboard administrators (OA) that use self-signed certificates and are added to HPE OneView using a discovery process.

During the setup of the initial HTTPS connection with the device, HPE OneView automatically adds the self-signed certificate of the device to the HPE OneView trust store. For this approach to be secure from man-in-the-middle attacks, the initial discovery has to be done in an isolated network segment. If not, you must validate the authenticity of the device certificates after the fact and out-of-band. The ease with which the authenticity is validated depends on the device. This approach only works for devices that allow you to securely view the certificate fingerprint for the device.

NOTE: The automatic initial trust approach is used when HPE OneView first communicates with a device. Once the device is discovered or managed, if the self-signed certificate changes, HPE OneView is unable to communicate with the device. An alert is generated asking the administrator to add the new certificate for the device to the HPE OneView trust store.

To securely validate the certificate fingerprint and import the self-signed certificate for key HPE OneView devices, follow these steps:

- Securely obtain the certificate fingerprint for the device using one of the prescribed methods in the following sections.
- Compare the fingerprint you have obtained to the one from the device's certificate stored in the HPE OneView trust store after HPE OneView has discovered or added the device. Use the **Settings > Security > Manage Certificates** screen to view the certificates in the HPE OneView trust store.
- If the fingerprints match, communications between HPE OneView and the device are secure.
- If the fingerprints do not match, either the device certificate was changed after the initial communication session with HPE OneView or there is a possible man-in-the-middle-attack.

Cited below are a few examples:

- **Server iLOs**

- **For a Gen10 rack mount server**

- Connect a serial cable and the terminal to the server. Use the following command on the iLO to identify the certificate fingerprint of the iLO's self-signed certificate:

- ```
cd /map1/sslcert1/hpiLO
show
```

- If a serial connection is not available and the SSH host fingerprint has not been previously verified, disconnect the iLO from the management network and connect directly from another trusted device on an isolated, protected network. You can securely establish an SSH connection on an isolated network. Ensure that you note down the SSH host fingerprint of the iLO for use later by other administrators when the iLO is placed back on the management network.

- **For Gen9 and earlier rack mount servers**

- For Gen9 and earlier rack mount servers, the iLO command line interface (CLI) is not available. Instead, disconnect the iLO from the management network, and set it up temporarily on an isolated network with another client device operating a web browser. Use the web browser to connect to the iLO and note down the certificate fingerprint.

- **For BladeSystem blade servers**

- Establish trust with the onboard administrator (OA) and use the OA user interface to connect securely to each of the iLOs and view the certificate fingerprint using a web browser.

- **BladeSystem Onboard Administrators**

- The onboard administrator (OA) supports serial connection and the **show oa certificate** command. The OA also has a dedicated, secure, network service port for connecting to a laptop. You can use a browser from the laptop to display the user interface of the OA and the associated certificate fingerprint. You can now establish trust between a browser on the management network and the OA. From the OA, you can securely connect to each iLO and determine certificate fingerprint for it using the browser.

## Certificates in HPE OneView

The **Manage Certificates** option under the **Settings > Security** screen displays the following types of certificates:

- **Trusted certificates:** All certificates shown on the **Manage Certificates** screen are trusted by HPE OneView. All certificates trusted by HPE OneView can communicate securely with devices and servers that are associated with a certificate trusted by HPE OneView or a certificate signed by a CA (root or intermediate CA) certificate trusted by HPE OneView.

The certificates shown as trusted comprise:

- Root CA certificates: These certificates are either prebundled with HPE OneView or imported by users. You must upload a CRL for root CA certificates to do revocation checking on certificates signed by the root CA.
- Intermediate CA certificates: These certificates are either pre-bundled with HPE OneView or imported by users. You must upload a CRL for Intermediate CA certificates to do revocation checking on certificates signed by an Intermediate CA.
- Leaf-level certificates
  - Self-signed certificates: These are device certificates that get added to the appliance trust store during automated blind trust. These certificates can also be directly imported by the user or added during a device configuration. Unlike CA signed certificates, self-signed certificates are not subject to host name verification or revocation checks.
  - CA-signed certificates: CA-signed leaf certificates are normally not stored in the appliance trust store. However, they may get stored during automated blind trust or when a user uses the force trust option to forcefully add the leaf certificate to the trust store. Such CA-signed leaf certificate in the appliance trust store



is treated similar to self-signed certificates if the CA that signed these certificates are not present in the appliance. Such blindly or forcefully trusted CA-signed certificates are not subject to host name verification or revocation checks.

These certificates can be pre-bundled with HPE OneView, imported as part of the automatic initial trust done by HPE OneView (system) when a hardware gets discovered and managed by HPE OneView or imported by users.

- **Pre-bundled Certificates:** HPE OneView pre-bundles the following types of certificates:
  - Internal root CA - Infrastructure Management Certificate Authority: The root CA is bundled with HPE OneView 4.0 out-of-the-box. It is required for the internal functioning of the RabbitMQ message bus server within HPE OneView. This root CA is internally used to sign the RabbitMQ server and RabbitMQ client certificate. The internal root CA and the RabbitMQ client certificate must be imported to any external client using AMQP to communicate with HPE OneView. The internal root CA or the RabbitMQ certificates are not displayed in the **Manage Certificates** screen, but are available using REST APIs.

---

**NOTE:** Starting with HPE OneView 4.0, users can use external CA-signed certificates for RabbitMQ server certificate and RabbitMQ client certificate.

---

- CA certificates required by Remote Support in HPE OneView: When you use the remote support capability within HPE OneView, communication is established from HPE OneView to one or more remote support servers hosted by HPE (<https://api-support.hpe.com>). The remote support servers hosted by HPE are associated with server certificates that are signed by Symantec intermediate CA and a Verisign Root CA. HPE OneView pre-bundles the following root and intermediate CA certificates that are required for the secure and trusted communication with the remote support server:
  - Verisign Root CA - VeriSign Class 3 Public Primary Certification Authority - G5
  - Symantec Intermediate CA - Symantec Class 3 Secure Server CA - G4
  - Verisign Root CA - VeriSign Universal Root Certification Authority
  - Symantec Intermediate CA - Symantec Class 3 Secure Server SHA256 SSL CA
  - DigiCert Root CA - DigiCert Global Root G2
  - DigiCert Intermediate CA - DigiCert Global CA G2

**x509 v1 certificates:** HPE OneView supports older x509 v1 certificates as well. These v1 certificates do not have enough information in them to determine whether it is a CA certificate or not. When such a V1 certificate is imported into the appliance, it is treated as a CA certificate.

However, if any v1 certificate already exists in the appliance prior to an appliance upgrade, that v1 certificate is considered a leaf certificate. If such a pre-upgrade v1 certificate is meant to be a root certificate, you must delete and re-add it to consider it as a root certificate.

Hewlett Packard Enterprise recommends that you replace any such x509 v1 leaf-level certificates with x509 v3 leaf-level certificates. It is hard to replace x509 v1 root CA certificates, and therefore this recommendation is limited to leaf-level certificates alone.

See **Certificate validation criteria** for additional details.

## Certificate Revocation Lists

A certificate authority-signed (CA) certificate can be revoked under the following conditions:

- When the CA issues an improper certificate
- If the private key of the certificate is compromised

Information about revoked certificates is published by a CA as a Certificate Revocation List (CRL). A CRL for the certificate is specified in the CRL Distribution Points (CRL DP) field of the certificate. CRLs are accessible using HTTP and are digitally signed by the issuing CA.

HPE OneView enables users to import CRLs downloaded from a CA to the appliance. HPE OneView then validates all certificates signed by the CA against this CRL. CRLs have an expiration date and must be uploaded into the appliance before their expiration.

---

**ⓘ IMPORTANT:** HPE OneView does not support delta CRLs. Do not upload a delta CRL into the appliance. A delta CRL contains all certificates that have been revoked since the last base CRL was published.

---

Certificate revocation checking is enabled by default. A revoked certificate cannot be imported into the appliance. TLS communication with a device or external server having a revoked certificate is not allowed by HPE OneView.

However, if the CA-issued CRL for the certificate is not imported into HPE OneView or if the imported CRL has expired, certificate revocation check is skipped by default. You can disable these default behaviors and enable strict revocation checking from the **Settings > Security** screen. The security best practice is to enable strict revocation checking.

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

When two-factor authentication is enabled, the CRLs for HPE OneView appliance certificate and client certificates of the users must be current.

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

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

*Locate CRL Distribution Points* in the *HPE OneView Online Help* provides details on how to locate the CRL DPs for these certificates.

#### **More Information**

##### **Two-factor Authentication.**

See "CRL Distribution Points" in the online help for information about uploading CRLs.

## **Certificate status checks**

HPE OneView performs periodic status checks on certificates. A scheduled job runs every hour at the top of the hour within HPE OneView. The job checks the status (Expired, About to expire, Revoked or Untrusted) of all certificates within the HPE OneView trust stores.

Alerts are raised and displayed in the **Settings > Security** screen of the appliance for users to take required action on the certificates.

# About certificate validation

HPE OneView performs certificate validation for all Transport Layer Security (TLS) communications between the appliance and external servers or devices. These checks guarantee confidentiality, integrity, and authentication with the remote end-point.

In production environments, Hewlett Packard Enterprise strongly recommends that certificate validation be enabled. In environments where security is not a concern, such as a testing environment, certificate validation can optionally be disabled.

If certificate validation is disabled, any sensitive data such as credentials are transmitted insecurely. Make sure to use only local user accounts and not enterprise directory-based accounts to avoid transmitting enterprise login credentials over the network when certificate validation is disabled.

---

**NOTE:** When upgrading from earlier releases, the certificates in use by the currently monitored or managed devices are imported into the HPE OneView trust store and alerts are generated for issues such as expired certificates. These automatically added certificates are either a device's self-signed certificate or the leaf certificate for a certificate authority (CA) signed certificate. Using CA-signed certificates can simplify the device **trust process**.

Certificate checking is enabled by default, but some of the stricter validation checks are relaxed to maintain communications with all devices, even those with certificate issues. The relaxed checking gives the administrator time to address any expired certificates, to upload trusted CA root and intermediate certificates, and upload the appropriate CRLs.

---

**NOTE:** During communication from the appliance to managed devices or external servers, when the certificate is presented, expiration check is not performed on the following types of leaf certificates:

- Self-signed certificates: See **Certificate management** for additional information on self-signed certificates.
- Pinned CA-signed certificates: A pinned certificate refers to the copy of a CA-signed leaf certificate that belongs to a managed device or external server saved to the appliance trust store.

---

Hewlett Packard Enterprise strongly recommends that you enable strict certificate validation checks after completing an update as appropriate for your enterprise security policies. See Manage certificates screen details in the online help for additional information on certificate management.

---

HPE OneView supports devices using self-signed certificates and devices using formal CA-signed certificates. CA-signed certificates offer benefits such as revocation checking and overall simplified management.

HPE OneView enables users to import a CA CRL file and to perform the appropriate revocation checking on existing certificates in the trust store and for certificates received during communication with a managed device or external server.

**More information:**

- "Manage certificates" in the online help
- "Certificate screen details" in the online help

## Certificate validation criteria

Certificates can be classified into the following types:

- **Device or server certificate (external to the appliance)**
- **CA certificate (Root or intermediate CA)**
- **Appliance certificate**
- **Client certificate used in two-factor authentication**

### Device or server certificate (external to the appliance)

A device's certificate is considered valid when:

- it is in X509 format, v1 or v3. X509 v3 is the preferred and recommended format for the device leaf-level certificates.
- it has not expired. The validity period is indicated by the **valid from** and **valid to** fields.

Expired and future-dated certificates are not considered as valid and you cannot import such certificates to the appliance.

- it has an optional **Key Usage** extension.

If the certificate contains a **Key Usage** extension, it must contain `Digital signature` and must not contain `Certificate signing` as one of the values.

For self-signed certificates, this field is not validated.

For CA-signed certificates, this field is validated.

- it has an optional **Extended Key Usage** extension.

If the certificate contains an **Extended Key Usage** extension, it must contain `Server Authentication` as one of the values.

- it has an optional **Basic Constraints** extension.

If the certificate contains a **Basic Constraints** extension, it must contain **Subject Type** set to `End Entity` and **Path Length Constraint** set to `None`.

- it is signed by a signature algorithm, specified as supported by the appliance for external devices and servers. For example, an MD5 certificate is considered invalid.
- it has a public key length, specified as supported by the appliance for external devices and servers. For example, 512-bit public key is invalid.
- for external repository servers:
  - it has a **Subject Alternative Name** (SAN) field containing the key `IP Address` of the repository server, along with the required values. For example, `IP Address=172.20.3.173`.

### CA certificate (root or intermediate CA)

A CA certificate (root or intermediate) is considered valid when

- it is of X509 format, v1 or v3.
- it has not expired. The validity period is indicated by the **valid from** and **valid to** fields.

Expired and future-dated certificates are not considered as valid and you cannot import such certificates to the appliance.

- it has an optional **Key Usage** extension. If the certificate contains a **Key Usage** extension, it must contain `Certificate signing` as one of the values.
- it has an optional **Extended Key Usage** extension. If the certificate contains an **Extended Key Usage** extension, it is ignored.
- it has an optional **Basic Constraints** extension. If the certificate contains a **Basic Constraints** extension, the *Subject Type* must be set to **CA**.

Optionally, the certificate may contain a *Path Length Constraint*.

- it is signed by a signature algorithm, specified as supported by the appliance for CA certificates. For example, an MD5 or an SHA-1 CA certificate are invalid.
- it has a public key length, specified as supported by the appliance for CA certificates.

### Appliance certificate

Appliance certificate is considered valid when

- it is of X509 format, v1 or v3.
- it has not expired. The validity period is indicated by the **valid from** and **valid to** fields.

Expired and future-dated certificates are not considered as valid and you cannot import such certificates to the appliance.

- it has an optional **Key Usage** extension.

If the certificate contains a **Key Usage** extension, it must contain `Digital Signature` as one of the values.

- it has an optional **Extended Key Usage** extension.

If the certificate contains an **Extended Key Usage** extension, it must contain `Server Authentication` and `Client Authentication` as the values.

- it has an optional **Basic Constraints** extension. If the certificate contains the **Basic Constraints** extension, the values of *Subject Type* and *Path Length Constraint* must be set to **End Entity** and **None**, respectively.
- it is signed by a signature algorithm, specified as supported by the appliance for the appliance certificate. For example, an MD5 or an SHA-1 certificates are invalid.
- it has a public key length that is specified as supported by the appliance for the appliance certificate.

### Client certificate used in two-factor authentication

A two-factor authentication client certificate is considered valid when

- it is of X509 v3 format.
- it has not expired. The validity period is indicated by the **valid from** and **valid to** fields.

Expired and future-dated certificates are not considered as valid and you cannot import such certificates to the appliance.

- it has an optional key usage extension.

If the certificate contains a key usage extension, it must contain `Digital Signature` as one of the values.

- it has an optional **Extended Key Usage** extension.

If the certificate contains an **Extended Key Usage** extension, it must contain `Client Authentication` and `Smart Card Logon` as the values.

- it has an optional **Basic Constraints** extension. If the certificate contains the **Basic Constraints** extension, the values of *Subject Type* and *Path Length Constraint* must be set to **End Entity** and **None**, respectively.
- it has a **Subject Alternative Name (SAN)** field that has `Other name: Principal Name` set to the User Principal Name (UPN) of the user logging in with two-factor authentication. An example of a UPN is **firstname.lastname@example.com**.

Alternatively, the certificate has the SAN field, with either an email address of the user logging in or the common name.

The domain component (base DN of directory) is part of either the Issuer or the Subject field (for example, `dc=example,dc=com`).

- it is signed by a signature algorithm that is specified as supported by the appliance for external devices and servers. For example, an SHA-1 certificate is considered invalid.
- it has a public key length that is specified as supported by the appliance for external devices and servers.

**More information:**

- [\*\*Algorithms, cipher suites, and protocols for securing the appliance\*\*](#)
- [\*\*Two-factor Authentication\*\*](#)

## Expiry checks for self-signed certificates of devices

By default, HPE OneView has disabled expiry check of self-signed certificates during communication with the managed devices. [\*\*Device-specific certificate handling\*\*](#) provides details. Once you have taken appropriate actions to correct the device certificates, you can enable expiry checks of self-signed certificates from the **Settings > Security** screen.

## Device-specific certificate handling

Some of the devices that HPE OneView needs to securely communicate with require device-specific certificate management procedures.

### [\*\*Integrated Lights-Out certificates\*\*](#)

### [\*\*Managing servers with iLO configured for two-factor authentication\*\*](#)

### [\*\*Onboard Administrator Certificates\*\*](#)

---

**NOTE:** The maximum number of certificates that can be present in the certificate chain is nine. The appliance fails to connect to any device or server if it has a certificate chain depth higher than the maximum limit. The maximum certificate chain depth is set by default on the appliance, and cannot be customized by the user.

---

## iLO certificates

HPE OneView treats the default certificate for HPE-Integrated Lights-Out (iLO) as a self-signed certificate. This certificate is added to the HPE OneView trust store and treated as a leaf certificate. The iLO certificate is signed by a certificate authority internal to Hewlett Packard Enterprise, namely, 'iLO Default Issuer (Do not trust)'. This warns the users to the danger of trusting self-signed certificates and encourages them to move to use PKI-based certificates.

The iLO has limited space for storing certificates. When using CA-signed certificates, the iLO does not present HPE OneView with a chain of intermediate certificates during the TLS handshake. To establish proper HTTPS connections, the intermediates must be present in the HPE OneView trust store, along with the CA root.

iLO 3 and iLO 4 have a Customer Advisory for an issue where the default self-signed certificate is expired by default. In this case, the `Valid from` date of the certificate is later than the `Valid to` date. The advisory describes the steps required to upgrade the iLO firmware and fix the certificate.

The **Security > Certificates** screen allows the administrator to control whether to skip expiration check for self-signed certificates. This option allows the administrator to manage iLOs securely while working to address the expiration issues.

The issue can occur on iLO versions mentioned in this [\*\*advisory\*\*](#).

---

**NOTE:** When the system boots up for the first time, the iLO creates a default self-signed certificate. This certificate does not change unless you change the iLO hostname or loads a CA-signed certificate.

---

## Managing servers with iLO configured for two-factor authentication

As iLO 5 supports two-factor authentication, HPE OneView is able to import and manage servers when iLO 5 is configured for two-factor authentication. When you configure iLO 5 with **CAC/Smart Card Authentication** enabled, no specific

configurations are required for HPE OneView to manage the server. HPE OneView authenticates to the iLO using its own credentials to manage the server.

However, when you configure iLO 5 with both **CAC/Smart Card Authentication** and **CAC Strict Mode** enabled, HPE OneView authenticates to the iLO using its digital certificate. Ensure that the following configurations are present on both the iLO and HPE OneView for the appliance to successfully import and manage the server when the iLO is in this mode:

- HPE OneView and the iLO are set up with a CA-signed certificate.
- The HPE OneView certificate has Extended Key Usage (EKU) of 'Client Authentication' in addition to 'Server Authentication.'
- Make sure the CA root certificate and any appropriate certificate chains are present in the iLO and HPE OneView trust stores.
- If **Local user accounts** is enabled in the iLO, ensure that these prerequisites are met:
  - An account for HPE OneView is created in the iLO with full administrator privileges.
  - The HPE OneView certificate is imported into the iLO and mapped to this iLO user and account.

---

**NOTE:** You can use the HPE OneView self-signed certificate instead of a CA-signed certificate.

---

- If **Local user accounts** is disabled in the iLO and the iLO is configured for directory authentication and authorization, ensure that:
  - You have created a user account for HPE OneView in the directory server.
  - The account name matches the name specified in the **Subject Alternative Name (SAN) DNS Name=** or in the **Subject CN=** field in the certificate. In general, this field takes the hostname of the HPE OneView appliance as the value.
  - The user account created in the directory is associated with a directory group that has 'Administrator' privileges in the iLO.

---

**NOTE:** You must manually perform these configurations for each iLO that has **CAC Strict Mode** enabled.

---

## Onboard Administrator Certificates

By default, the HPE Onboard Administrator (OA) generates self-signed certificates. These certificates do not contain the following:

- Subject field with a fully qualified domain name, that is a common name (CN) field
- Subject Alternate Name (SAN) field

The default certificate does not offer adequate security as you cannot bind the certificate to a specific device identity of HPE OneView. Instead, you must opt to use the PKI CA-signed certificates, or, if self-signed must be used, create a new OA self-signed certificate and manually specify the following:

- A fully qualified domain name (FQDN) for the CN field of the certificates.
- The same FQDN in addition to the IP addresses of the OA in the Subject Alternative Name field. Make sure to include all the valid OA IPs that are used in your management environment (IPv4, IPv6 and IPv6 link local).

The Onboard Administrator online help provides details on how to properly specify the values for the SAN field.

## Enabling and disabling certificate validation

You can enable or disable certificate validation from the **Security > Settings** screen.

Hewlett Packard Enterprise recommends that you disable certificate checking only in test environments where certificate checking is not required. When disabling certificate checking, use only the local user account and not enterprise directory accounts. No checking is performed on the connection to the directory server, which can compromise a user's directory credentials. If certificate validation is disabled, the appliance is subject to MITM (man-in-the-middle) security attacks. Hence, use the **Certificate validation** option with utmost caution.



# Appliance Management

The chapters in this part describe tasks performed outside of HPE OneView to help manage the appliance. This part also includes best practices for managing the appliance and troubleshooting.

# Managing the appliance

This chapter describes tasks performed outside of HPE OneView to help manage the appliance and how to restore the appliance. For tasks performed in HPE OneView to manage the appliance, see the online help.

- **How the appliance handles an unexpected shutdown**
- **About restoring the appliance**
- **Best practices for restoring an appliance**
- **Restore an appliance from a backup file using the HPE OneView GUI**

## How the appliance handles an unexpected shutdown

The appliance has features to help you with unexpected shutdowns, allowing managed resources to continue to operate while the appliance is offline. For example:

- Setting up automatic backups
- Setting up automatic recovery

Hewlett Packard Enterprise recommends that you use the hypervisor high-availability to reduce down-time and backup features to ensure that the appliance is backed up daily, and when you make significant configuration changes.

### **Appliance recovery operations**

When the appliance restarts, it performs the following operations:

- Detects tasks that were in progress and resumes those tasks, if it is safe to do so. If the appliance cannot complete a task, it notifies you that the task has been interrupted or is in some other error state.
- Attempts to detect differences between the current environment and the environment at the time the appliance shut down, and then refreshes its database with the detected changes.

If you determine that the appliance data does not match the current environment, you can request that the appliance refresh the data for certain resources, such as enclosures.

### **Appliance recovery during a firmware update of a managed resource**

If the appliance shuts down during a firmware update of a managed resource, when the appliance restarts, it detects the failed update and marks the firmware update tasks as being in an error state. To update the firmware for this resource, you must re-initiate the firmware update task.

### **What to do when an appliance restarts**


The online help provides information about using the user interface or the REST APIs to:

- Check for critical alerts or failed tasks and follow the provided resolution instructions
- Manually refresh a resource if the resource information displayed appears to be incorrect or inconsistent
- Create a support dump (recommended for unexpected shutdowns to help support personnel to troubleshoot the problem)
- Update firmware for a resource, if a firmware update task was in progress when the appliance shutdown.


# About restoring the appliance

Restoring an appliance from a backup file replaces all management data and most configuration settings with the data and settings in the backup file, including user names and passwords, audit logs, cryptography mode, but does not include the appliance network settings (appliance IP address, hostname and DNS server).

The appliance is not operational during the restore operation and it can take several hours to perform; the larger the configuration HPE OneView is managing, the longer the restore will take. A restore operation cannot be canceled or undone after it has started. The appliance blocks login requests while a restore operation is in progress.

 **IMPORTANT:** A restore operation must be used to recover from catastrophic failures, not to fix minor problems that can be resolved in other ways.

The backup file must have the same version of HPE OneView as the appliance you want to restore. You can restore onto the same appliance or a new installation of the appliance.

| Actions during the restore operation                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Validates the resource inventory</b>             | During a restore operation, the appliance firmware validates the resource inventory (enclosures, servers, interconnects, switches) and reconciles the data in the backup file with the current state of the managed environment. The state of the managed environment is likely to be different from the state of the environment at the time the backup file was created. After the restore operation, the appliance uses alerts to report any discrepancies that it cannot resolve automatically.                                                                                                                                                                                                                            |
| <b>Rediscovered enclosures to validate contents</b> | During the restore operation, the appliance rediscovers each enclosure or fabric to validate its contents—especially to ensure that the appliance can still claim them and that the given instance of HPE OneView is the manager of the enclosure.<br><br>Then the appliance rediscovers each server and refreshes all rack servers.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Clears virtual IDs</b>                           | To prevent duplicate identifiers on the network, the appliance clears server hardware configurations if an associated server profile is not in the backup. These servers most likely had a profile assigned after the last backup was made.<br><br> <b>IMPORTANT:</b> During a restore operation, the appliance reconciles the data in the backup file with the current state of the managed environment. There are some discrepancies that the restore operation cannot resolve automatically. They are presented as alerts. After the restore operation, the appliance administrator must manually resolve any remaining inconsistencies. |

See also [Post-restoration tasks](#).

You can use the UI to **upload a backup file and restore the appliance from it**. You can also use REST APIs for this purpose.

# About the support dump file

The support dump contains data that might be considered customer sensitive such as hostnames, IP addresses, and the appliance audit log. Unless you specify otherwise, all data in the support dump file is encrypted so that only an authorized technical support person can access it.

You can choose not to encrypt the support dump file if you are an Infrastructure administrator. This can be useful if you have an onsite, authorized technical support person or if your environment prohibits outside connections. You can also

validate the contents of the support dump file and verify that it does not contain data considered sensitive in your environment.


Some error messages recommend that you create a support dump of the appliance and send it to authorized technical support for analysis. The support dump process performs the following functions:

- Deletes any previous support dump file
- Gathers logs and other information required for debugging
- Creates a compressed file with a name in the following format:

*hostname-identifier-timestamp.sdmp*

Where, for support dump files created from the UI, *identifier* is either `CI` (indicating an appliance support dump) or `LE` (indicating a logical enclosure support dump).

---

 **IMPORTANT:** If the appliance is in an error state, a special **Appliance error screen** is displayed. Anyone can create an encrypted support dump file from that screen without the need for logging in or other authentication.

---

The support dump file contains the following:

- Operating system logs
- Product logs
- The results of certain operating system and product-related commands

Items logged in the support dump file are recorded according to UTC time.

#### **About support dump created from a clustered appliance**

##### **About logical enclosure support dumps**

You can create a logical enclosure support dump, which, by default, includes the appliance support dump. The logical enclosure support dump file includes content from each member logical interconnect. After the logical enclosure support dump is created, it is incorporated into the appliance support dump and the entire bundle of files is compressed into a zip file and encrypted for downloading.

---

**NOTE:** To create a logical enclosure support dump that does not contain the appliance support dump, you must use the logical enclosure REST APIs.

---

# Best practices for restoring an appliance


| Topic            | Best Practice                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Before you begin | <p><b>1.</b> Note the passwords you use.</p> <p>Maintain a list of the current user accounts on the appliance.</p> <p>The restore operation resets the user names and passwords to those that were in effect when the backup file was created.</p>                                                                                                                                                                                                      |
|                  | <p><b>2.</b> Take a support dump before the restore operation, if you are restoring onto the same appliance where you have taken the backup. Taking a support dump helps the support representative to troubleshoot problems that might have existed before the restore operation.</p>                                                                                                                                                                  |
|                  | <p><b>NOTE:</b> Ensure to download any backup taken, before creating a support dump, as the backup gets deleted during the support dump operation. The create support dump operation also deletes an uploaded backup file.</p>                                                                                                                                                                                                                          |
|                  | <p><b>3.</b> Download the existing audit logs, and store them for safekeeping.</p> <p>The restore operation restores the audit logs from the backup file, overwriting the existing logs.</p>                                                                                                                                                                                                                                                            |
|                  | <p><b>4.</b> Stop all automatically scheduled backups.</p> <p>If HPE OneView is configured for automatic backups, backups resume after the appliance is restored.</p>                                                                                                                                                                                                                                                                                   |
|                  | <p><b>5.</b> Make the backup file accessible to the appliance you wish to restore. If you are using an enterprise backup product to archive backup files, follow any steps required by your backup product to prepare for the restore operation.</p>                                                                                                                                                                                                    |
|                  | <p> <b>WARNING:</b> The current backup file stored on the appliance will be deleted during the restore process. Download the backup file and store it in a safe, off-appliance location for future restorations.</p>                                                                                                                                                 |
|                  | <p><b>6.</b> If you added hardware to the appliance after the backup file was created, that hardware is not in the appliance database when the restore process completes. Then, if you restore from the backup file, you must add that hardware to the appliance and then repeat any other configuration changes (such as assigning server profiles) that were made between the time the backup file was created and the restore process completed.</p> |
| Inform users     | <p>Make sure that all users logged in to the appliance log out. Users who are logged in when the restore operation begins are automatically logged out, losing whatever work was in progress. All users are blocked from logging in during the restore operation.</p>                                                                                                                                                                                   |

Table Continued

| Topic                            | Best Practice                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use the right backup file</b> | <ul style="list-style-type: none"> <li>Use the latest backup file to restore the appliance. The backup file will not include any changes made after the backup file was created.</li> <li>Make sure the appliance IP addresses are the ones you want the appliance to use after the restore operation. Appliance IP addresses are not restored from the backup file.</li> <li>Ensure that the appliance being restored and the appliance on which the backup file was created have the same appliance firmware version; otherwise, the restore operation fails.</li> </ul> <p>The platform type, hardware model, and the major and minor numbers of the appliance firmware must match to restore a backup. The revision and build numbers do not need to match. The format of the appliance firmware version is:</p> <p><i>majornumber.minornumber.revisionnumber-buildnumber</i></p> <p>If the backup file is incompatible with the firmware on the appliance, the upload returns an error and the restore operation stops. You will need to update the firmware or select a different backup file.</p> <ul style="list-style-type: none"> <li>If it is necessary to restore a backup to a new appliance and the old appliance is still functioning (the hardware has not failed), delete the old appliance. Removing the appliance ensures that it no longer manages the devices it was managing when the backup file was created. Serious errors can occur if multiple appliances attempt to manage the same devices.</li> </ul> |
| <b>Upload firmware bundles</b>   | <p>Upload the firmware bundles used by your server profiles, enclosures, and logical interconnects. These were not saved as part of the backup file. Refer to each profile's <code>Firmware baseline</code> setting to determine the file name for the required baseline.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Restore an appliance from a backup file using the HPE OneView GUI

### Prerequisites

Restoring an appliance from a backup file replaces all management data and most configuration settings on the appliance. You are directed to re-enter unresolved data, if applicable.



**CAUTION:** If restoring the backup to a new appliance, ensure to first shutdown the old appliance to prevent both the appliances from managing the environment. A conflict occurs and the appliance you were attempting to restore is not restored.

- Privileges: Infrastructure administrator.
- You have completed all the **best practices for restoring an appliance**.
- You have the original network configuration information available to enter.

### Procedure

1. Install HPE OneView on the new or replacement appliance.
2. Configure the new appliance with the same network settings as the appliance on which the backup file was created and use the network to upload the backup file to the new appliance. See "Change the Appliance network settings" in the online help.
3. When the new appliance network is configured, continue the restore operation based on one of the following scenarios:

- Select a backup file to immediately start the restoration process.
- Select a backup file to start the restoration process later.

#### More information

- **About restoring the appliance**
- *HPE OneView Installation Guide* at <http://www.hpe.com/info/oneview/docs>

## Scenario: Select a backup file and start the restoration immediately

### Prerequisites

- Minimum required privileges: Infrastructure administrator.
- HPE OneView is installed on a new or replacement appliance.

### Procedure

1. From the main menu, select **Settings**, and then select **Backup**.
2. Select **Actions** > **Restore from backup**.  
A dialog box opens.
3. Read the onscreen notification and select **Select a backup file**.
4. Do one of the following:

- Drag the backup file and drop it into the indicated text box.
- Click **Browse**, and then select the backup file to upload.

---

**NOTE:** Not all browsers and browser versions offer the ability to drag and drop files onto applications.

---

5. Click **Upload and restore**.

Wait until the restore process is complete. A status page indicates progress.

When the restore process completes, you are returned to the login page where you can log in to the restored appliance.

6. Upload the firmware bundles used by your server profiles, enclosures, and logical interconnects. These were not saved as part of the backup file. Refer to each profile's `Firmware baseline` setting to determine the file name for the required baseline.
7. If you used HPE OneView to create a custom SPP, recreate the custom SPP after the base SPP and the hotfixes are uploaded to the repository using one of the following methods:
  - Use the `CMDLET Restore-HPOVCustomBaseline`. For more information, see <https://github.com/HewlettPackard/POSH-HPOneView/wiki/Restore-HPOVCustomBaseline>.
  - Use the UI to recreate the custom SPP.
8. Verify that the restore operation was successful by logging in to the appliance and successfully resolving any discrepancies that the restore operation cannot resolve automatically.

**Next step:**

**Post-restoration tasks**

## Backup and restore the appliance

### Prerequisites

- Privileges: Infrastructure administrator.
- HPE OneView is installed on a new or replacement appliance.

### Procedure

1. From the main menu, select **Settings**, and then select **Backup**.
2. Select **Actions** > **Restore from backup**.  
A dialog box opens.
3. Read the onscreen notification and select **Select a backup file**.
4. Do one of the following:

- Drag the backup file to the indicated text box.
- Click **Browse**, and then select the backup file to upload.

---

**NOTE:** Not all browsers and browser versions offer the ability to drag and drop files onto applications.

---

5. Click **Upload**.

Wait until the upload process is complete. A progress bar appears. The file name, creation date, and version are displayed when the file upload is complete.

6. When you are ready to restore the appliance from the backup file, return to the dialog box and verify that the backup file is correct and uploaded.
7. Select **Restore from a backup**.
8. Click **Restore**.

---

**NOTE:** During the restore process the appliance may get restarted, and you may lose access to the maintenance console. Reconnect to the maintenance console after 5 minutes to monitor the progress of the restore process.

---

Wait until the restore process is complete. A status page indicates progress.

When the restore process completes, you are returned to the login page where you can log in to the restored appliance.

9. Download the current Service Pack for ProLiant (SPP) at <https://www.hpe.com/servers/spp/download>.
10. If you used HPE OneView to create a custom SPP, recreate the custom SPP after the base SPP and the hotfixes are uploaded to the repository using one of the following methods:



- Use the CMDLET `Restore-HPOVCustomBaseline`. For more information, see <https://github.com/HewlettPackard/POSH-HPOneView/wiki/Restore-HPOVCustomBaseline>.
- Use the UI to recreate the custom SPP.

11. Verify that the restore operation was successful by logging in to the appliance and successfully resolving any discrepancies that the restore operation cannot resolve automatically.

**Next step:**

**Post-restoration tasks**

## Post-restoration tasks

During a restore operation, the appliance reconciles the data in the backup file with the current state of the managed environment. There are some discrepancies that a restore operation cannot resolve automatically; for example, if servers were added after the backup file was created. The network configuration on these servers is unknown to the appliance after a restore and could result in duplicate MAC addresses and World-Wide Names (WWNs), as a result.

After a restore operation completes, you must manually resolve any remaining alerts and add these servers back into the appliance to eliminate the risk of duplicate IDs. You must also perform manual cleanup of hardware (servers, interconnects, and enclosures) if server profiles are forcibly unassigned or the hardware is forcibly removed without first being unconfigured.

**Procedure**

1. After a restore operation is complete, readd any enclosure or server hardware added since the selected backup.

---

**NOTE:** For any enclosures added since the last backup that you decide **not** to readd after the restore, avoid duplicate IDs by running the Onboard Administrator SSH command `clear vcmode` on these enclosures. Running this command ensures the virtual MACs and WWNs on the server blades in the enclosure have been cleared.

---

2. For any server profile alerts about the profile not matching the server hardware:
  - a. Identify all server profiles with a mismatch-type of error message. Make a list of these server profiles and the assigned server hardware.
  - b. Power off the server, and then unassign all the server profiles individually. From the **Server Profiles** screen, select **Actions > Edit**, and then select **Unassign** from the server hardware drop-down selector. Click **OK**.
  - c. Select **Actions > Edit** again, and then reassign all the documented profiles to the documented server hardware.
3. For any alerts about ID ranges, the Network administrator should examine the address and identifier ranges and edit them, if needed.
4. Recreate any profiles for the servers in any enclosures that were added in step 1.
5. For HPE Composable Fabric, log into the HPE Composable Fabric Manager, and re-enter the HPE OneView credentials. Perform a refresh and reapply the configuration on the fabric resource.

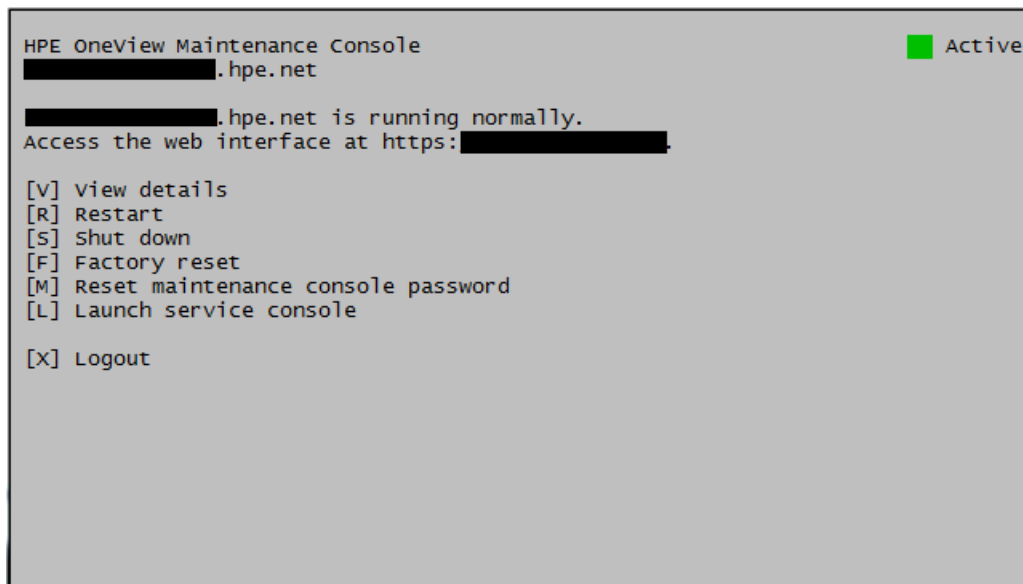
# Appliance maintenance console

- **About the appliance maintenance console** on page 178
- **Access the appliance maintenance console** on page 180
- **About the factory reset operation** on page 180
- **About the appliance maintenance console password** on page 180
- **Log in to the appliance maintenance console** on page 181
- **Appliance maintenance console main menu screen details** on page 182
- **Appliance maintenance console details screen details** on page 182
- **Appliance maintenance console appliance states** on page 183
- **Perform a factory reset using the appliance maintenance console** on page 184
- **Reset the administrator password with the appliance maintenance console** on page 185
- **Reset the appliance maintenance console password** on page 186
- **Restart the appliance using the appliance maintenance console** on page 187
- **Shut down the appliance using the appliance maintenance console** on page 187
- **View the appliance details** on page 187

## About the appliance maintenance console

The appliance maintenance console is an important tool for troubleshooting appliance issues when the HPE OneView UI is not available.

The appliance maintenance console, shown in the example, provides a limited set of administrative commands that might be required when you cannot access the web user interface (UI) of the appliance.



**Figure 2: Example of the appliance maintenance console main menu**

In the upper left of most appliance maintenance console screens, the local appliance is identified by its host name.

The appliance maintenance console displays an icon and a message about the state of the appliance indicating few actions such as:

- Normal operation.
- Appliance is offline.
- Appliance is being updated.
- Appliance is starting up, shutting down, restarting, or temporarily unavailable.
- Appliance is being restored from a backup file.
- Appliance is being reset to factory default settings.

### Commands

The body of the main menu contains commands that can be used:

- To view the appliance details.
- To restart the local appliance.
- To shut down the appliance.
- To reset the administrator password.
- To perform a factory reset of the appliance.
- To launch a service console, which an authorized technical support representative can use to diagnose or repair a problem.
- To configure appliance networking.
- To log out of the Maintenance console.

---

**NOTE:** The commands displayed by the appliance maintenance console depend on the current state of the appliance and how the appliance maintenance console was accessed.

---

### Navigation

- Use the tab and arrow keys to navigate within the appliance maintenance console screen.
- Commands are displayed with corresponding hot keys. These keys are shown within brackets in **Figure 2: Example of the appliance maintenance console main menu** on page 178. Pressing a hot key selects the command.
- You can use the **Enter** key to invoke a selection. That is, after you make a selection, pressing **Enter** runs the command.

### More information

- **Access the appliance maintenance console** on page 180
- **Log in to the appliance maintenance console** on page 181
- **View the appliance details** on page 187

## About the appliance maintenance console password


The appliance maintenance console has no initial password. To set it, see **Reset the appliance maintenance console password** on page 186.

Appliance maintenance console passwords must meet the following minimum requirements:

- Fourteen (14) characters long
- One uppercase alpha character
- One lowercase alpha character
- One numeric character
- One special character

Backup operations do not back up the appliance maintenance console password. Ensure that you can remember or retrieve the appliance maintenance console password in some other way.


---

 **IMPORTANT:** You can only reset the password by resetting the appliance to its original factory settings, which reverts the appliance maintenance console password to its initial setting, none.

---

## About the factory reset operation

A factory reset restores the appliance to the original factory settings, but does not change the installed firmware version.

 **CAUTION:** By default, the factory reset operation erases appliance data, including logs, network settings, and managed device settings in HPE OneView. You have the option of explicitly preserving network settings and logs. The preserve network settings option also preserves the cryptography mode.

Preserving network settings is the safest option when trying to recover an appliance from an error because the appliance remains accessible from the network.

Ensure that you have a recent backup file before performing this operation.

---

The factory reset operation can be performed from the UI or from the appliance maintenance console.

Use the factory reset operation for either of these reasons:

- To decommission the appliance so that you can migrate the hardware.
- To return the appliance to a known state for reuse (for example, to restore the appliance from a backup file).

## Access the appliance maintenance console

Access the appliance maintenance console through the virtual console or through an SSH connection.

---

**NOTE:** Use the credentials of a local user with the Infrastructure administrator role when prompted. You can **reset the administrator password** from the appliance maintenance console.

---

**Access the appliance maintenance console through an SSH connection.**

## Access the appliance maintenance console through an SSH connection

---

**NOTE:** Hewlett Packard Enterprise recommends the use of these tools for accessing the appliance maintenance console through an SSH connection:

- PuTTY
  - MTPuTTY
  - vSphere/vCenter Console
- 

### Procedure

1. Invoke one of the recommended tools on your local computer.
2. Access the appliance by specifying its fully qualified domain name or its IP address.
3. Enter the user name `maintenance` at the login prompt.
4. **Log in to the appliance maintenance console** on page 181.

## Access the appliance maintenance console from the virtual console

### Procedure

1. Access the virtual appliance console.
2. Enter the user name `maintenance` at the login prompt.
3. **Log in to the appliance maintenance console** on page 181.

## Log in to the appliance maintenance console

When you access the appliance console, you are presented with either a login screen or the appliance maintenance console main menu:

### Procedure

1. Access through the appliance console presents the appliance maintenance console main menu immediately.

After you enter your first command and before it runs, the login screen is presented.

---

**NOTE:** The **Reset password** option requires a challenge/response authorization.

---

2. Access through SSH presents the login screen immediately.
  3. Enter the user name and password of a local Infrastructure administrator account on this appliance.
- 

**NOTE:** You cannot log in using an Infrastructure administrator account that is authenticated by an authentication directory service.

---

The appliance maintenance console login remains valid for one hour. After one hour of inactivity, you must reenter the password. The appliance maintenance console session closes after 24 hours of inactivity.

# Appliance maintenance console main menu screen details

| Screen component     | Description                                                                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title                | Identifies the appliance maintenance console.                                                                                                                                                                                  |
| Appliance identifier | Identifies an appliance by its host name.<br><br>Is located directly beneath the Title.                                                                                                                                        |
| Icon                 | Indicates the general state of the appliance. The icon is located in the upper right of the console screen.                                                                                                                    |
| State text           | Displays one to three lines of additional text to elaborate on the state indicated by the icon.<br>Example states include:<br><br>Restoring from backup<br>Starting                                                            |
| Notification banner  | Notifies or warns of a situation regarding the appliance.<br><br>The Notification banner spans the width of the appliance maintenance console.<br><br>If no notification is pending, the Notification banner does not display. |
| Commands             | Lists the available commands that are appropriate to the state of the appliance. Examples include:<br><br>View details<br>Restart<br>Shut down<br>Reset password<br>Factory reset<br>Launch service console                    |

## More information

- **[About the appliance maintenance console](#)**
- **[Access the appliance maintenance console through an SSH connection](#)** on page 181
- **[Log in to the appliance maintenance console](#)** on page 181
- **[View the appliance details](#)** on page 187
- **[Restart the appliance using the appliance maintenance console](#)** on page 187
- **[Shut down the appliance using the appliance maintenance console](#)** on page 187
- **[Reset the administrator password with the appliance maintenance console](#)** on page 185
- **[Perform a factory reset using the appliance maintenance console](#)** on page 184

# Appliance maintenance console details screen details

The View Details command displays this screen.

| Screen component     | Description                                                                                                                                                                                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title                | Identifies the appliance maintenance console.                                                                                                                                                                                                       |
| Appliance identifier | Identifies an appliance by its host name.<br>Located directly beneath the Title.                                                                                                                                                                    |
| Icon                 | Indicates the general status of the appliance in the upper right.                                                                                                                                                                                   |
| State text           | Displays one to three lines of additional text to elaborate on the icon state. State text examples include:<br><code>Restoring from backup</code><br><code>Starting</code><br><code>Active</code>                                                   |
| Notification banner  | Notifies or warns of a situation regarding the appliance or appliance cluster.<br><br>The Notification banner spans the width of the appliance maintenance console.<br><br>If no notification is pending, the Notification banner does not display. |
| <b>Host name</b>     | Displays the host name of the appliance.                                                                                                                                                                                                            |
| <b>IP address</b>    | Displays the IP address of the appliance.                                                                                                                                                                                                           |
| <b>Model</b>         | The model number of the appliance running HPE OneView.                                                                                                                                                                                              |
| <b>Firmware</b>      | The version number of the firmware running on the HPE OneView appliance and the date the firmware was last updated.                                                                                                                                 |
| <b>Serial number</b> | The serial number of the appliance.                                                                                                                                                                                                                 |

## Appliance maintenance console appliance states

| State                          | Situation                                                 | Action                                                                                        |
|--------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Active                         | The appliance is running normally.                        |                                                                                               |
| Offline<br>Unrecoverable error | The appliance failed with an unrecoverable error.         | For information on resolving this issue, see the "Appliance error screen" in the online help. |
| Resetting                      | The appliance is being reset to factory default settings. |                                                                                               |

*Table Continued*

| State                   | Situation                                                          | Action |
|-------------------------|--------------------------------------------------------------------|--------|
| Restarting              | The appliance is restarting and will be available shortly.         |        |
| Restoring from backup   | The appliance will be restarted after the restoration completes.   |        |
| Starting                | The appliance is starting up and will be available shortly.        |        |
| Shutting down           | The local appliance is shutting down.                              |        |
| Temporarily unavailable | The local appliance is in a transition, and its state will change. |        |
| Updating                | The local appliance is undergoing a software update.               |        |

## Perform a factory reset using the appliance maintenance console

### Prerequisites

- Ensure that all users are logged out and all ongoing work is completed.
- Back up all user files.
- Create an unencrypted support dump file and save it to an external location for safekeeping.

### Procedure

1. Access the appliance maintenance console main menu.
2. Select **Factory reset** in the main menu.
3. In the subsequent dialog box, do one of the following:
  - a. Enter **Y** to continue the factory reset operation.



**CAUTION:** This option erases the network settings and logs. Use this option to decommission an appliance.

- b. Enter **P** to continue with the factory reset operation, but preserve the network settings and logs.  
Use this option if you want to restore an appliance from a backup file or if you want to apply a new configuration.
  - c. Enter **N** to cancel the factory reset operation and return to the main menu.
4. Confirm that you want to perform the factory reset in the subsequent dialog boxes.
  5. In the next dialog box, do one of the following:



- a. Enter **Y** to continue the factory reset operation.
  - b. Enter **N** to cancel the factory reset operation and return to the main menu.
6. Verify by observing the operation.

---

**NOTE:** You can **view details** to see the progress in the top right corner of the screen. `Reset successful` displays when the reset has completed.

---

## Reset the administrator password with the appliance maintenance console

- ❗ **IMPORTANT:** The **request code** is valid only while you are on the **Password reset** screen of the appliance maintenance console. If you return to the main menu or end the appliance maintenance console session, the request code will be invalid. You will need to start this procedure over again to acquire a new request code.

You will need to contact your support specialist, who will send an **authorization code** (also known as a response code) after verifying your information.

You must enter the **authorization code** within one hour or it becomes invalid.

---

**NOTE:**

- This operation resets the password for a local administrator account on the appliance. It does not apply to administrator accounts authenticated by a directory service.
- This operation allows you to set a single-use password for the `local administrator account`.

Use that single-use password the next time you log in to the UI with this account. You will be prompted to set a new password.

---

### Prerequisites

If you lose or forget the local administrator password and can access the appliance maintenance console through the virtual console, use the following procedure to reset it. This operation provides a unique request code that you use when contacting your support specialist.

---

**NOTE:** If you accessed the appliance maintenance console through SSH, use the User interface (UI) to reset the administrator password.

---

You have access to the appliance console.

### Procedure

1. **Access the appliance maintenance console** on page 180.

2. Select **Reset password**.

The appliance maintenance console displays a request code.

3. Telephone your support specialist and provide that person with the following information:

- The name of the person requesting the password to be reset.
- The name of the company that owns the appliance.
- The request code from the appliance maintenance console.

The support specialist verifies the information and then sends a message to the authorized email address on file. This message contains the authorization code. An ISO image, which is also the authorization code, is attached to the message.

**4.** Do one of the following to enter the authorization code in the response field:

- If you are able to paste information into the appliance maintenance console, copy the authorization code from the email message and paste it into the response field of the appliance maintenance console.
- Read the authorization code from the ISO image:
  - a. Save the ISO image attached to the email message.
  - b. Mount the ISO image as a virtual media mount (a virtual CD).
  - c. Select **Read from ISO** in the appliance maintenance console.
  - d. The appliance maintenance console reads the ISO image and, after a moment, automatically fills in the response field with the authorization code.
- Enter the authorization code into the response field manually.

**5.** Determine a single-use administrator password.

**6.** When prompted, enter and re-enter the new password.

**7.** Select **OK** to set the single-use password.

**8.** Verify by logging out and then log in to this account with the new password.

## Reset the appliance maintenance console password

### Prerequisites

- Create a new password that fulfills the **password requirements**.
- If the current appliance maintenance console password is forgotten, perform and download a backup and then perform a **factory reset of the appliance**.

### Procedure

1. Access the appliance maintenance console main menu.
2. Log in with the user name `maintenance` and password (if set) at the login prompt.
3. Select **Reset maintenance console password**.
4. Enter the current password and the new password twice, once for verification.
5. Select **OK**.

## Restart the appliance using the appliance maintenance console

This procedure describes how to use the appliance maintenance console to shut down and then restart the appliance.

### Prerequisites

Ensure that all users are logged out and all ongoing work is completed.

### Procedure

1. Access the appliance maintenance console main menu.
2. Select **Restart**.
3. Confirm that you want to restart the appliance.
4. Verify by observing the restart.

## Shut down the appliance using the appliance maintenance console

This procedure describes how to use the appliance maintenance console to perform a graceful shutdown of the appliance.

### Prerequisites

Ensure that all users are logged out and all ongoing work is completed.

### Procedure

1. Access the appliance maintenance console main menu.
2. Select **Shut down** in the main menu.
3. Confirm that you want to shut down the appliance.
4. Verify by observing the shutdown.

## View the appliance details

Use this procedure to display appliance details such as state, host name, IP address, model, and firmware.

### Procedure

1. Access the appliance maintenance console main menu.
2. Select **View details**.

The appliance maintenance console details screen is displayed.

# Troubleshooting the appliance

The following topics provide troubleshooting information to handle issues that require action outside of HPE OneView.

## Tasks fail when appliance is in IPv6 mode

### Symptom

The appliance initially allows you to enter an IPv4 address in HPE OneView but tasks fail with error messages.

### Cause

HPE OneView, when configured for IPv6, cannot send or receive communications to or from devices on an IPv4 network.

### Action

Ensure that you are using IPv6 addresses with managed resources when the appliance is configured only for IPv6.

### More information

## Appliance is offline, unrecoverable error

### Symptom

The appliance is offline with an unrecoverable error. HPE OneView displays an Appliance Error screen.

### Cause

An internal error in HPE OneView occurred.

The appliance error screen provides details about the error, if known, and recommends actions to take based on the error detection.

You might be directed to do one or more of the following actions:

### Action

1. Restart the appliance.
2. If prompted, create a support dump file and contact your authorized support representative.
3. Shutdown the appliance and restore a backup onto a new appliance with the same version of HPE OneView.
4. Do not delete the old appliance until HPE OneView has been recovered onto the new appliance. Contact your authorized support representative if the appliance in the error state must be recovered.

### More information

#### About restoring the appliance

## Appliance performance is slow

### Symptom

The appliance operates, but its performance is slow.

### Cause

The appliance configuration is not set for optimum performance.

### Action

1. Ensure that the physical components satisfy the requirements described in the **HPE OneView Support Matrix**.
  - VM host with ProLiant G7-class CPUs or later
  - VM with two 2 GHz or greater virtual CPUs
2. Ensure proper network connection between the appliance and managed devices.
3. Ensure power management is not enabled.
4. Ensure the hypervisor is not overloaded.
5. Ensure the available storage is acceptable.
6. Ensure the host is not overloaded.
  - a. Examine the virtual machine's performance data (performance counters). If the hypervisor host is running at 100% utilization, consider:
    - Restarting the VM host
    - Moving the appliance to a VM host with more resources, especially one that is not as busy
    - Using reservations or shares on the hypervisor host
7. From the local computer, use the `ping` command to determine if the round-trip time of the ping is acceptable. Long times can indicate browser problems.
8. Determine that the browser settings are correct.
9. Consider bypassing the proxy server.
10. Ensure the scale limits are not exceeded. See the **HPE OneView Support Matrix**.
11. Create a support dump file and **contact your authorized technical support**.

## Appliance rejects your login for HPE OneView

### Symptom

There is a login screen, but the appliance rejects your login.

### Solution 1

### Cause

Authentication for the local user account is invalid.

### **Action**

1. Retype your login name and password in case you made an error.
2. Verify your login name and role settings with the Infrastructure administrator. If the appliance was reset to its original factory settings, the Infrastructure administrator might need to reinstate you.
3. As Infrastructure administrator, do the following:
  - a. Verify the account name and ensure that a role is assigned to the user.
  - b. Restart the appliance and try again.

### **Solution 2**

#### **Cause**

Authentication for the Authentication directory service is invalid.

#### **Action**

1. Retype your login name and password, and choose the correct authentication directory in case you made an error.
2. Verify your login name and your group and role settings with the Infrastructure administrator. If the appliance was reset to its original factory settings, the Infrastructure administrator might need to reinstate you.
3. As Infrastructure administrator, do the following:
  - a. Verify the account name and ensure that the user is a member of the group in the directory service.
  - b. Verify that the authentication directory service is configured properly.
  - c. Verify that the directory service server is operational. See "Directory service not available" in the online help.
  - d. Verify that the directory service host certificate is valid. If not, reacquire a certificate and install it.
  - e. Contact the directory service provider to ensure that the credentials are accurate.
  - f. Restart the appliance and try again.

## **Cannot log in to HPE OneView after a factory reset action**

#### **Symptom**

Log in not accepted following a factory reset operation.

#### **Cause**

The authentication was deleted by the factory reset.

### **Action**

Log in to the appliance with the default credentials that you used when you logged in for the first time.

## **Cannot restart the appliance after a shutdown**

### **Symptom**

The restart action resulted in a shutdown, but not a restart.

### **Cause**

An internal server error might have occurred.

### **Action**

Required privileges: Infrastructure administrator

1. Log in as the Infrastructure administrator.
2. Retry the restart action.
3. Retry the restart action from the hypervisor.
4. If the problem persists, create a support dump.
5. Contact your Authorized technical support and provide them with the support dump.

## **Browser does not display the HPE OneView user interface**

### **Symptom**

The browser does not display the HPE OneView user interface.

### **Solution 1**

#### **Cause**

The browser is not supported.

#### **Action**

Use a supported browser. See the [\*\*HPE OneView Support Matrix\*\*](#).

### **Solution 2**

#### **Cause**

The browser cache is full.

#### **Action**

1. Clear the browser cache and try again.
2. Refresh or reload the browser.

### **Solution 3**

#### **Cause**

JavaScript is not enabled.

#### **Action**

Enable JavaScript on the browser.

### **Solution 4**

#### **Cause**

There is a connectivity issue with the appliance.

#### **Action**

1. Verify that the browser proxy setting is accurate.
2. Refresh or reload the browser.
3. Verify that the appliance can access the network.

### **Solution 5**

#### **Cause**

HPE OneView encountered an error that prevents it from responding to browser requests.

#### **Action**

1. **Log in to the appliance maintenance console** on page 181.
2. Determine the state of the appliance.
3. Use the appropriate action as noted in **Appliance maintenance console appliance states** on page 183.

## **Login screen is not displayed in HPE OneView**

#### **Symptom**

There is no login screen.

#### **Cause**

The appliance has not yet started or the browser is not behaving correctly

#### **Action**

1. Wait for the appliance to start completely.
2. Refresh your browser and try again.
3. Open a new browser and try again.
4. As Infrastructure administrator, use the REST APIs to restart the appliance.



# Reinstall the remote console for proper iLO operation

## Symptom

When running Firefox or Chrome on a Windows client, the first-time installation of the iLO remote console prevents the installation dialog box from being displayed again. If you need to reinstall the console software, you must reset the installation dialog box. Installation dialog box is not displayed.

## Cause

If you installed the iLO remote console software using one browser (Firefox or Chrome), but are using another browser, the dialog box that prompts you to install the software is displayed, even if the software is already installed.

## Action

1. To reinstall the console, press the **Shift** key and select **Actions > Launch console**.
2. To reinstall the software, click **Install software** and close all of the dialog boxes for installing the application.
3. Click **My installation is complete — Launch console** to launch the console after it is installed.

# Restore action was unsuccessful for HPE OneView

## Symptom

The restore and factory reset operations failed, and the appliance could not restart.

## Solution 1

### Cause

The backup file is incompatible.

### Action

1. Log in as Infrastructure administrator.
2. Retry the restore operation with a recent backup file that fulfills this criteria:  
The appliance being restored has the same HPE OneView major and minor version numbers as the appliance on which the backup file was created. The Settings screen displays the version number in this format:

Version major.minor.nn-nnnnn month-day-year

3. Reconcile any discrepancies that the restore operation could not resolve automatically.

## Solution 2

### Cause

A serious error occurred.

### Action

1. Log in as Infrastructure administrator.
2. Create a support dump file, in case you might need to contact an authorized support representative.

**3.** If possible, reset the appliance to factory settings.

**4.** Retry the restore operation.

### **Solution 3**

#### **Cause**

Restore operation failed.

#### **Action**

**1.** Log in as Infrastructure administrator.

**2.** Create a support dump file, in case you might need to contact an authorized support representative.

**3.** Do one or both of the following:

- Retry the restore operation, specifying the most recent backup file.
- Try the restore operation with another backup file that is compatible with the appliance.

**4.** If the problem persists, contact your authorized support representative.

### **Solution 4**

#### **Cause**

The status of the restore operation is IN PROGRESS but the percentage of change does not change for 2.5 hours or more.

#### **Action**

**1.** Log in as Infrastructure administrator.

**2.** Restart the appliance.

**3.** Do one or both of the following:

- Retry the restore operation, specifying the most recent backup file.
- Try the restore operation with another backup file that is compatible with the appliance.

# Managing and Monitoring in HPE OneView

HPE OneView makes it possible to easily monitor, configure, and manage physical and logical server, network, and storage resources. The tasks for managing and monitoring the physical and logical resources are provided in the HPE OneView online help at [\*\*http://www.hpe.com/info/oneview/docs\*\*](http://www.hpe.com/info/oneview/docs).

The **online help** provides conceptual and task information covering each resource of HPE OneView.

# 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.

# Websites

## General websites

Hewlett Packard Enterprise Information Library

[www.hpe.com/info/EIL](http://www.hpe.com/info/EIL)

HPE OneView documentation

[www.hpe.com/info/oneview/docs](http://www.hpe.com/info/oneview/docs)

Subscription Service/Support Alerts

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

HPE Insight Remote Support

[www.hpe.com/info/insightremotesupport/docs](http://www.hpe.com/info/insightremotesupport/docs)

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

[www.hpe.com/storage/spock](http://www.hpe.com/storage/spock)

Storage white papers and analyst reports

[www.hpe.com/storage/whitepapers](http://www.hpe.com/storage/whitepapers)

For additional general support websites, see [Support and other resources](#).

## Product websites

HPE Virtual Connect user guides and command line references

[www.hpe.com/info/virtualconnect/docs](http://www.hpe.com/info/virtualconnect/docs)

HPE 3PAR StoreServ and HPE StoreVirtual

[www.hpe.com/info/storage](http://www.hpe.com/info/storage)

HPE Integrated Lights-Out

[www.hpe.com/info/ilo](http://www.hpe.com/info/ilo)

HPE BladeSystem enclosures

[www.hpe.com/info/bladesystem](http://www.hpe.com/info/bladesystem)

HPE ProLiant server hardware

General information: [www.hpe.com/info/servers](http://www.hpe.com/info/servers)

BL series server blades: [www.hpe.com/info/blades](http://www.hpe.com/info/blades)

DL series rack mount servers: [www.hpe.com/servers/dl](http://www.hpe.com/servers/dl)

HPE Integrity Superdome X

[www.hpe.com/info/superdome](http://www.hpe.com/info/superdome)

HPE Superdome Flex Server

[www.hpe.com/info/superdome](http://www.hpe.com/info/superdome)

HPE Composable Cloud for ProLiant DL

[www.hpe.com/info/composablecloud-docs](http://www.hpe.com/info/composablecloud-docs)

# HPE OneView product feedback

## **Provide feedback to Hewlett Packard Enterprise**

Hewlett Packard Enterprise is always interested in hearing your feedback on any Hewlett Packard Enterprise product. To provide feedback directly to Hewlett Packard Enterprise, access <https://www.hpe.com/us/en/contact-hpe> and click **Submit Feedback**.

## **Provide feedback to Gartner Peer Insights**

Hewlett Packard Enterprise has partnered with several third-party sites as another option to provide your candid feedback. Our first partnership is with Gartner, a leading research and advisory firms for information technology insights. Hewlett Packard Enterprise has partnered with Gartner to set up a Gartner Peer Insights survey where you can review HPE OneView and provide your feedback within 15 minutes. If you are interested in providing your feedback to others interested in HPE OneView and becoming a trusted advisor, follow this link: <http://gtnr.it/2jgx9Ju>

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

### Hewlett Packard Enterprise Support Center: Software downloads

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

### Software Depot

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

- To subscribe to eNewsletters and alerts:  
[www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:  
[www.hpe.com/support/AccessToSupportMaterials](http://www.hpe.com/support/AccessToSupportMaterials)



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

## Customer self repair

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

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

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

## Remote support

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

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

### **Remote support and Proactive Care information**

#### **HPE Get Connected**

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

#### **HPE Proactive Care services**

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

#### **HPE Datacenter Care services**

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

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

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

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

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

### **Proactive Care customer information**

#### **Proactive Care central**

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

#### **Proactive Care service activation**

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

## Warranty information

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

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

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

#### **HPE Enterprise and Cloudline Servers**

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



#### **HPE Storage Products**

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

#### **HPE Networking Products**

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

## Regulatory information

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

**[www.hpe.com/support/Safety-Compliance-EnterpriseProducts](http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts)**

#### **Additional regulatory information**

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

**[www.hpe.com/info/reach](http://www.hpe.com/info/reach)**

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

**[www.hpe.com/info/ecodata](http://www.hpe.com/info/ecodata)**

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

**[www.hpe.com/info/environment](http://www.hpe.com/info/environment)**

## Documentation feedback

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

# Install and configure a web-based external firmware repository on Microsoft Windows

An externally managed HTTP/HTTPS web server can be added to the appliance as a firmware repository. It is a user-maintained HTTP/HTTPS web server. You can upload firmware bundles in a specific virtual directory and then register the HTTP/HTTPS server with HPE OneView. A virtual directory is a directory name that you specify in Internet Information Services (IIS) and map to a physical directory on a local or remote server. The directory name then becomes part of URL of the application, and you can request the URL from a web browser to access content in the physical directory, such as a webpage or a list of additional directories and files. This functionality is supported for Linux and Windows systems.

---

**NOTE:**

- An external web server configured with both the IPv4 and IPv6 address can be added to HPE OneView. For IPv6 addresses, you can configure using either static or DHCP address types.

**Examples:**

- IPv4 address: 192.168.12.0
  - IPv6 address: [2001:db8::]
- Only when HPE OneView communicates with the IP address of an external repository using HTTP/HTTPS protocol, the appliance and external firmware repository can be part of different subnets. Ensure that the connection does not have a high latency.

---

## Install IIS Web Server on Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012

**Prerequisites**

Windows Server 2008, Windows Server 2008 R2 or Windows Server 2012 has been installed on the system.

**Procedure**

1. From the operating system **Start** menu, choose **Server Manager**.
2. In the navigation pane, choose **Dashboard**, and click **Add Roles and Features**.
3. Read **Before you begin** page and click **OK**.
4. In the **Installation type** page, select **Role-based or feature-based installation**, and click **Next**.
5. In the **Server selection** page, select your server, and click **OK**.
6. In the **Server Roles** window, select **Web Server (IIS)**, **Add Roles and Feature Wizard** displays.
7. Click **Add Features**.
8. In the **Web Server Role (IIS)** page, click **Next**.
9. In the **Role services** page, click **Next**.

---

**NOTE:** Do not change the default settings on the **Role services** page.

---

10. In the **Confirm installation selections** page, click **Install**.
11. In the **Installation Progress** page, confirm that your installation completed successfully, and click **Close**.
12. To verify that the web server has been installed correctly, start your browser, and then in the address, enter the IP address of the web server and prepend **http://** to it.

## Install IIS Manager on Windows 8 and Windows 10

### Prerequisites

Windows 8 or Windows 10 has been installed.

### Procedure

1. Click operating system **Start** menu, and then select **Control Panel**.
2. Click **programs** and then click **Turn Windows feature on or off**.
3. Select **Internet Information Services** and expand **World Wide Web Services** in the **Windows Feature** window.
4. Expand **Common HTTP Features** and select the **Static Content Feature**.
5. Select **Internet Information Service (IIS) Manager**, under **Internet Information Services**, expand **Web Management Tools** and select **IIS Management Console**.
6. Click **OK**.
7. To verify that the web server has been installed correctly, start your browser, and then in the address, enter the IP address of the web server and prepend **http://** to it.

## Open IIS Manager

Now that you have installed the IIS Manager, open it for configuration and use.

### Procedure

1. From the operating system **Start** menu, select **Control Panel**.
2. Do one of the following:
  - If you are using Windows Vista® or Windows Server® 2008, click **System and Maintenance** and select **Administrative Tools**.
  - If you are using Windows® 8, Windows 10, or Windows Server® 2008 R2, click **System and Security** and select **Administrative Tools**.
3. In the **Administrative Tools** window, double-click **Internet Information Services (IIS) Manager** to open the **IIS manager**.

## Configure IIS web server on Windows

### Procedure

1. Open IIS Manager
2. Right-click **Default Website**, and select **Add Virtual Directory**.

3. Enter the **Alias** and the **physical path** of the virtual directory and click **OK**.

---

**NOTE:** If the name of the virtual directory consists of special characters, while editing the properties of the directory in HPE OneView, you might see that a few extra characters added to the name of the virtual directory.

---

4. Double-click **Directory Browsing** and click the **Enable** tab on the **Actions** pane.

To view the contents of the virtual directory, enable directory browsing. After enabling the **directory browsing**, you can view the contents by opening the browser and entering **http://{IP of the web server}/{Name of the virtual directory}**.

## Configure Authentication

### Procedure

1. If you are using Microsoft Windows 2008 Server, Windows 2012 Server or Windows 2012 r2 Server, perform the following steps:
  - a. From the operating system **Start** menu, click **Server Manager**.
  - b. In the navigation pane, select **Dashboard** and click **Add Roles and Features**.
  - c. In the select **Server Roles** window, select and expand **Web Server (IIS)** and select **Web Server**.
  - d. Under **Web Server**, expand **Security** and select **Basic Authentication**.
  - e. Click **Next**.
  - f. Click **Next** on the **Select Features** page.
  - g. Click **Install**.
2. If you are using Microsoft Windows 8 or 10, perform the following steps:
  - a. From the operating system **Start** menu, select **Control Panel**.
  - b. Click **programs** and then click **Turn Windows feature on or off**.
  - c. Select **Internet information services** and then expand **World Wide Web Services** in the **Windows Feature** window.
  - d. Select and expand **Security** and select **Basic Authentication**.
  - e. Click **OK**.
3. To enable the Basic Authentication for the web server, perform the following steps:
  - a. **Open IIS Manager**.
  - b. Double-click the **Authentication** tab in the **Features** view of your virtual directory.
  - c. Click **Anonymous Authentication** in the **Authentication** screen.
  - d. To disable **Anonymous Authentication**, click **Disable** in the **Actions** pane.

By Default **Anonymous Authentication** will be **Enabled**.
  - e. Click **Basic Authentication** in the **Authentication** page.
  - f. To enable **Basic Authentication**, click **Enable** in the **Actions** pane.

By Default **Basic Authentication** will be **disabled**.

g. Restart IIS manager.

4. To enable the Anonymous Authentication for the web server, perform the following steps:

Any other authentication mechanism mentioned above must be disabled before enabling Anonymous Authentication.

a. Double-click **WebDav Authoring Rules**.

b. Click **WebDav Setting** in the **Actions** pane.

c. In the **Property Behavior** section, do the following:

- Set the **Allow Anonymous Property Queries** to **True**.
- Set the **Allow Property Queries with Infinite Depth** to **True**.

By Default, **Allow Anonymous Property Queries** and **Allow Property Queries with Infinite Depth fields** are set to **False**.

## Install and enable WebDAV

### Prerequisites

The WebDAV Redirector must be installed for Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012. The WebDAV Redirector is already installed on Windows Vista, Windows 8, and Windows 10.

### Procedure

1. **If you are using Microsoft Windows 2008 Server, Windows 2012 Server or Windows 2012 r2 Server, perform the following steps:**

- a. From the operating system **Start** menu, click **Server Manager**.
- b. In the navigation pane, select **Dashboard** and click **Add Roles and Features**.
- c. In the select **Server Roles** window, select and expand **Web Server (IIS)**.
- d. Select and expand **Web Server** and choose **Common HTTP Features**, and then select **WebDAV Publishing**.
- e. Click **Next**, and then click **Install**.

2. **If you are using Microsoft Windows 8 or 10, perform the following steps:**

- a. From the operating system **Start** menu, select **Control Panel**.
- b. Click **programs** and click **Turn Windows feature on or off**.
- c. Select **Internet information services** and expand **World Wide Web Services** in the **Windows Feature** window.
- d. Select and expand **Common HTTP Features** and select **WebDAV Publishing**.
- e. Click **OK**.

3. **Open IIS Manager**.

4. Select your virtual directory and in the features view, double-click **WebDAV Authoring Rules**.
5. In the virtual directory features view, click **Enable WebDAV**.
6. Click **WebDAV Settings**.
7. If you have anonymous access enabled, select **True** for **Allow Anonymous Property Queries**, and click **Apply**.
8. Select the **Directory or Virtual Directory** to which you want to allow **WebDAV** access, and double-click **WebDAV Authoring Rules**.
9. Click **Add Authoring Rule** and set the following conditions.
  - a. Click **All content** to specify that the rule applies to all the content types.
  - b. Select **All users** or **Specified users** and type "**administrator**" as the user name.
  - c. Select **Read**, **Source**, and **Write** in the permissions section.
  - d. Click **Ok**.

You can add the web server to HPE OneView after installing and configuring WebDAV on IIS Manager. Enter the complete WebDAV mounted path as the web server address in HPE OneView. For more information on adding, editing, or removing external repository from HPE OneView, see section "*Settings: Repository*" in the HPE OneView help.

## Set up HTTPS Binding

### Procedure

1. **Open IIS Manager.**
2. To generate a Self-Signed Certificate on IIS, perform the following steps:
  - a. On the home page of the Internet Information services (IIS) Manager, double-click **Server Certificate** and in the **Actions** pane, select **Create Self-Sign Certificate**.
  - b. Enter a friendly **name** for the certificate, and click **OK**.
  - c. Select **Default web site** from the connections panel, and in the **Actions** pane, select **Bindings**.
  - d. Click **Add** and from the **Type** drop down list, select **https**. The default port assigned is **443**.
  - e. From **SSL Certificate**, select **self-signed certificate** and click **ok**.
  - f. To test **HTTPS binding**, select **Default Web Site** and select **Browse \*:443(https)** from the right panel.

The IIS home page opens in a web browser.
  - g. If you used a self-signed certificate, you will see a certificate error in the browser. To proceed, accept the certificate exception.

If you have a self-signed certificate, you will not see a certificate error. You will see the IIS home page with HTTPS in the web address.

---

**NOTE:** After you generate the certificate, ensure to **validate the certificate**.

---

# Set up MIME type

## Procedure

1. **Open IIS Manager.**
2. In the virtual directory Features view, double-click **MIME Types**.
3. In the **Actions** pane, click **Add**.
4. In the add **MIME Type dialog box**, type **.iso** in the File name extension text box.
5. Type **application/octet-stream** as the **MIME type** in the **MIME type** text box.
6. Click **OK**.
7. Click **Restart** from the **Actions** pane to restart the IIS manager.

# Configure size header

## Procedure

1. **Open IIS Manager.**
2. In the virtual directory Features view, double-click **HTTP Response Headers**.
3. In the **Actions** pane, click **Add**.
4. Enter **MaxRepoSize** as the **Name** and **100G** as the **Value** in the **Add Custom HTTP Response Header** window.
5. Click **OK**.
6. Click **Restart** from the **Actions** pane to restart the IIS manager.

---

**NOTE:** Important considerations for setting up an external repository

- Do not delete the firmware bundle from the external repository while the update process is in progress. Deleting the bundle will result in the failure of the update process.
- If two or more firmware bundles have the same name, the update process will continue for both the firmware bundles, but only one firmware bundle will be visible in HPE OneView.

---

Now that you have installed and configured the IIS Manager, you can add the web server to HPE OneView with the provided credentials and HTTP. HPE OneView will discover all the valid bundles. For more information on adding, editing or removing external repository from HPE OneView, see section "Settings: Repository" in the HPE OneView help.

# Install and configure a web-based external firmware repository on Linux

An externally managed HTTP/HTTPS web server can be added to the appliance as a firmware repository. It is a user-maintained HTTP/HTTPS web server. You can upload firmware bundles in a specific virtual directory and then register the HTTP/HTTPS server with HPE OneView. A virtual directory is a directory name that you specify in Linux Apache web server. You map this directory name to a physical directory on either a local or remote server. The directory name then becomes part of the application's URL. You can request the URL from a web browser to access content in the physical directory. For example, a webpage or a list of additional directories and files. This functionality is supported for Linux and Windows systems.

---

**NOTE:** An external web server configured with both the IPv4 and IPv6 address can be added to HPE OneView. For IPv6 addresses, you can configure using either static or DHCP address types.

**Examples:**

- IPv4 address: 192.168.12.0
- IPv6 address: [2001:db8::]

---

This chapter describes the procedures to install and configure an Apache web server on a Linux operating system.

## Configure Apache web server on Linux

**Procedure**

1. Update the **yum** package.

```
yum -y update
```

2. Install **Apache** on the **Linux** OS.

```
yum -y install httpd
```

3. Start the Apache service.

```
systemctl start httpd
```

Restart the Apache service if there was configuration changes.

```
systemctl restart httpd
```

4. To verify that the web server has been installed correctly, open the Apache server using a web browser with IP (http) address.

## Configure HTTPS using OpenSSL

**Procedure**

1. Obtain OpenSSL, mod\_ssl, and Apache's interface to OpenSSL.

```
yum install mod_ssl openssl
```

2. Add the **Subject Alternative Name** (SAN) field with the IP address of the Linux external repository in the section titled [v3\_req], in /etc/pki/tls/openssl.cnf.

```
subjectAltName = IP:172.20.5.55
```



[v3\_req] should look like the following example:

```
[v3_req]
```

```
Extensions to add to a certificate request
```

```
basicConstraints = CA:FALSE
```

```
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

```
subjectAltName = IP:172.20.5.55
```

**3. Generate the key and certificate with the required values for the attributes.**

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -nodes -
days 3650 -subj '/CN=<repo hostname or
IP>,C=<Country>,ST=<State>,L=<City>,O=<Customer>,OU=<IT>' -extensions
v3_req
```

**4. Copy the generated certificate and key to the correct location.**

```
cp cert.pem /etc/pki/tls/certs/localhost.crt
```

```
cp key.pem /etc/pki/tls/private/localhost.key
```

**5. Set the protocol by uncommenting the following line in /etc/httpd/conf.d/ssl.conf:**

```
SSLProtocol -all +TLSv1.2
```

**6. Set up the cipher suites by performing the following steps:**

**a. Comment the following existing lines in /etc/httpd/conf.d/ssl.conf:**

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA
```

```
#SSLCipherSuite ECDHE-ECDSA-AES256-SHA:HIGH:MEDIUM:!aNULL:!MD5
```

SSL Cipher Suite details in the ssl.conf file should look like the following example:

```
SSL Cipher Suite:
List the ciphers that the client is permitted to negotiate.
See the mod_ssl documentation for a complete list.
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA
#SSLCipherSuite ECDHE-ECDSA-AES256-SHA:HIGH:MEDIUM:!aNULL:!MD5
```

**b. Add cipher suites.**

```
SSLCipherSuite ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-ECDSA-AES256-GCM-SHA384:4:ECDH-RSA-
AES256-SHA384:ECDH-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-
AES256-GCM-SHA384:AES256-SHA256:AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RS#A-AES128-SHA256:ECDHE-RSA-
AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDH-ECDSA-
AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-
SHA256:ECDH-RSA-AES128-SHA256:ECDH-R#SA-AES128-GCM-SHA256:AES128-
SHA256:AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-DSS-AES128-GCM-
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:AES256-SHA:AES128-SHA:ECDH-
RSA-AES128-SHA:ECDHE-ECDSA#-AES256-SHA:ECDH-ECDSA-AES256-SHA:ECDH-RSA-
AES256-SHA:ECDHE-ECDSA-AES128-SHA:ECDH-ECDSA-AES128-SHA:ECDH-ECDSA-DES-
CBC3-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:ECDH-RSA-DES-
CBC3-SHA
```

7. Save the changes and exit the text editor.

8. Restart Apache.

```
service httpd restart
```

## Enable WebDAV and set up Basic Authentication

### Procedure

1. Determine if the WebDAV module is running.

```
sudo httpd -M | grep fs
```

If WebDAV is already enabled, you will see the following output:

```
dav_fs_module (shared)
```

By default, the WebDAV module is included and enabled with the Apache installations.

2. Create a WebDAV directory under the Apache web root directory.

```
sudo mkdir /var/www/html/webdav
```

3. Change the ownership and permission of the WebDAV directory.

```
sudo chown -R apache:apache /var/www/html/webdav
```

```
sudo chmod -R 755 /var/www/html/webdav
```

4. To set up a password authentication for the WebDAV directory by creating a **.htpasswd file**, perform the following steps:

a. Create a **.htpasswd file**.

```
sudo htpasswd -c /etc/httpd/.htpasswd {User Name}
```

b. Assign group ownership to the Apache user and lock down permissions for other users.

```
sudo chown root:apache /etc/httpd/.htpasswd
```

```
sudo chmod 640 /etc/httpd/.htpasswd
```

5. Create a **virtual host file** for the WebDAV directory:

a. Create a **site configuration file** called **webdav.conf**.

```
vi /etc/httpd/conf.d/webdav.conf
```

b. Enter the following code block:

```
DavLockDB /var/www/html/DavLock
<VirtualHost *:80>
 ServerAdmin webmaster@localhost
 DocumentRoot /var/www/html/webdav/
 ErrorLog /var/log/httpd/error.log
 CustomLog /var/log/httpd/access.log combined
 Alias /webdav /var/www/html/webdav
 <Directory /var/www/html/webdav>
 DAV On
```

```
AuthType Basic
AuthName "webdav"
AuthUserFile /etc/httpd/.htpasswd
Require valid-user
</Directory>
</VirtualHost>
```

---

**NOTE:** The **AuthName** must be same as the user name specified in step 4.

---

6. Save the file and restart Apache.

```
service httpd restart
```

After restarting the Web Server, login details are requested.

---

**NOTE:** Only Basic Authentication and OpenSSL certificate are supported for https in HPE OneView.

---

7. You can add the web server to HPE OneView with the provided credentials and HTTP. HPE OneView will discover all the valid bundles.

For more information on adding an external repository to HPE OneView, see the *Add external repository* topic in the HPE OneView online help.

8. To add the web server as an external repository using **HTTPS**, perform the following steps.

- a. Navigate to the **/etc/httpd/conf** path and edit the **httpd.conf**.

```
vi httpd.conf
```

- b. Search for the following line of code in the .conf file.

```
DocumentRoot "/var/www/html/"
#
Relax access to content within /var/www.
#
```

- c. Search for the directory path and change the path from **<Directory "/var/www/html/>** to **<Directory "/var/www/html/webdav">**.

- d. Add the following code in the **<Directory>** block.

```
DAV On
AuthType Basic
AuthName "webdav"
AuthUserFile /etc/httpd/.htpasswd
Require valid-user

All access controls and authentication are disabled
in this directory
#AuthType None
#Satisfy all
#Allow from all
#AllowOverride None
Header set MaxRepoSize 100G
AllowOverride AuthConfig
#Require all granted
```

---

**NOTE:** The code line, `Header set MaxRepoSize 100G` configures the size of the web server.

---

- e. Save the file and restart Apache.

```
service httpd restart
```

- 9. To add the web server to HPE OneView without requiring a password, perform the following steps:

- a. Navigate to `/etc/httpd/conf` and edit `httpd.conf`.

```
vi httpd.conf
```

- b. Remove # from the following lines:

```
#AuthType None
#Satisfy all
#Allow from all
#AllowOverride None
#Require all granted
```

- c. Add # to the following code line:

```
AllowOverride AuthConfig
```

- d. Save the file and restart Apache.

```
service httpd restart
```

Now that you have installed and configured the Linux Apache web server, you can add the web server to HPE OneView and copy the firmware bundles to the external repository.

---

**NOTE:** Hewlett Packard Enterprise recommends downloading the new file to another folder in the Linux repository in the same mount point. This prevents Linux from keeping a partial download in the repository path. You can then move the file to the folder which is registered in the Linux repository. For example, in this use case, move the file to `/var/www/html/webdav`.

---

For more information on adding, editing, or removing an external repository from HPE OneView, see the *Add external repository* topic in the HPE OneView online help.