Abstract

This document describes the security and encryption mechanisms available in HPE Gen10 servers and embedded firmware. This document is intended for individuals who are responsible for the secure configuration and operation of HPE servers for their organization.
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.


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

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

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.

UNIX® is a registered trademark of The Open Group.
Contents

Introduction......................................................................................................................... 10
  The importance of security.................................................................................................................. 10
  HPE Gen10 platform security features and licensing........................................................................ 10
  HPE Gen10 product security features............................................................................................... 11
  HPE iLO 5 Security Features.................................................................................................. 11
  Unauthorized access prevention.................................................................................. 12
  Phlashing protection.................................................................................................... 12
  Protected Management ROM...................................................................................... 13
  Protected PCI bus........................................................................................................13
  Host Access Configuration Lock..................................................................................13
  Network and management ports..................................................................................13
  Security Override switch.............................................................................................. 14
  Trusted Platform Module and Trusted Modules........................................................... 14
  Operating iLO servers in the DMZ............................................................................... 15
  Communication between iLO and server blades or Synergy systems......................... 17
  Security audits............................................................................................................. 17
  Firmware verification....................................................................................................19
  HPE Gen10 UEFI security features........................................................................................21
  Intelligent Provisioning Security Features...............................................................................22
  Intelligent Provisioning.................................................................................................22
  Intelligent Provisioning security through iLO................................................................22
  Intelligent Provisioning security through UEFI............................................................. 23
  iLO Amplifier Pack security features.......................................................................................23

HPE Gen10 recommended security settings.................................................................................. 24

Hardware security........................................................................................................................................ 30
  HPE Gen10 Server hardware security.............................................................................................. 30

HPE Gen10 security best practices................................................................................................. 32
  Physical access security.................................................................................................................. 32
  The HPE ProLiant Gen10 System Maintenance switch.......................................................... 32
  iLO security with the system maintenance switch........................................................................ 33
  HPE ProLiant Gen10 system intrusion detection........................................................................ 34
    Enabling or disabling system intrusion detection........................................................................ 34
  iLO Service Port.......................................................................................................................... 34
    Configuring the iLO Service Port settings................................................................................. 35
    iLO Service Port supported devices......................................................................................... 35
  Configuration security.................................................................................................................. 36
    iLO settings for configuration security....................................................................................... 36
      Preparing to set up iLO.................................................................................................................. 37
      IPMI/DCMI settings...................................................................................................................... 41
      iLO security............................................................................................................................... 42
      iLO user accounts...................................................................................................................... 44
      iLO directory groups.................................................................................................................... 49
      Administering SSH keys........................................................................................................... 52
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>UEFI settings for configuration security</td>
</tr>
<tr>
<td>65</td>
<td>Using the iLO 5 Configuration Utility</td>
</tr>
<tr>
<td>72</td>
<td>iLO Amplifier Pack configuration security</td>
</tr>
<tr>
<td>72</td>
<td>Managed Servers Alerts</td>
</tr>
<tr>
<td>74</td>
<td>Activity Logs and Alerts</td>
</tr>
<tr>
<td>74</td>
<td>Recovery Management</td>
</tr>
<tr>
<td>88</td>
<td>Remote management security</td>
</tr>
<tr>
<td>90</td>
<td>HPE ProLiant Gen10 security states</td>
</tr>
<tr>
<td>91</td>
<td>iLO security states</td>
</tr>
<tr>
<td>92</td>
<td>Configuring encryption settings</td>
</tr>
<tr>
<td>94</td>
<td>Connecting to iLO when using higher security states</td>
</tr>
<tr>
<td>95</td>
<td>Configuring a FIPS-validated environment with iLO</td>
</tr>
<tr>
<td>95</td>
<td>Disabling FIPS mode</td>
</tr>
<tr>
<td>96</td>
<td>SSL cipher and MAC support</td>
</tr>
<tr>
<td>99</td>
<td>Configuring schema-free directory settings in iLO</td>
</tr>
<tr>
<td>98</td>
<td>Prerequisites for configuring authentication and directory server settings</td>
</tr>
<tr>
<td>100</td>
<td>Configuring HPE Extended Schema directory settings in iLO</td>
</tr>
<tr>
<td>101</td>
<td>Directory user contexts</td>
</tr>
<tr>
<td>102</td>
<td>Directory Server CA Certificate</td>
</tr>
<tr>
<td>102</td>
<td>Local user accounts with Kerberos authentication and directory integration</td>
</tr>
<tr>
<td>102</td>
<td>Running directory tests</td>
</tr>
<tr>
<td>105</td>
<td>CAC Smartcard Authentication</td>
</tr>
<tr>
<td>109</td>
<td>Kerberos authentication with iLO</td>
</tr>
<tr>
<td>111</td>
<td>Configuring the iLO hostname and domain name for Kerberos authentication</td>
</tr>
<tr>
<td>112</td>
<td>Preparing the domain controller for Kerberos support</td>
</tr>
<tr>
<td>112</td>
<td>Generating a keytab file for iLO in a Windows environment</td>
</tr>
<tr>
<td>114</td>
<td>Verifying that your environment meets the Kerberos authentication time requirement</td>
</tr>
<tr>
<td>115</td>
<td>Configuring Kerberos support in iLO</td>
</tr>
<tr>
<td>115</td>
<td>Configuring supported browsers for single sign-on</td>
</tr>
<tr>
<td>117</td>
<td>Directory integration</td>
</tr>
<tr>
<td>117</td>
<td>Choosing a directory configuration to use with iLO</td>
</tr>
<tr>
<td>118</td>
<td>Schema-free directory authentication</td>
</tr>
<tr>
<td>119</td>
<td>Prerequisites for using schema-free directory integration</td>
</tr>
<tr>
<td>119</td>
<td>Process overview: Configuring iLO for schema-free directory integration</td>
</tr>
<tr>
<td>120</td>
<td>Schema-free nested groups (Active Directory only)</td>
</tr>
<tr>
<td>120</td>
<td>Process overview: Configuring the HPE Extended Schema with Active Directory</td>
</tr>
<tr>
<td>121</td>
<td>Prerequisites for configuring Active Directory with the HPE Extended Schema configuration</td>
</tr>
</tbody>
</table>
Lifecycle security

Updates and patches

Intelligent Provisioning, UEFI, and server boot security

Operating system security provisioning

Directory services support
Installing the iLO directory support software
Running the Schema Extender
Directory services objects
Directory-enabled remote management (HPE Extended Schema configuration)
Roles based on organizational structure
How role access restrictions are enforced
User access restrictions
Role access restrictions
Tools for configuring multiple iLO systems at a time
UEFI, passwords, and the Trusted Platform Module
Server Security options
Setting the power-on password
Setting an administrator password
Secure Boot
Enabling or disabling Secure Boot
Configuring Trusted Platform Module options
Advanced Secure Boot Options
Viewing Advanced Secure Boot Options settings
Enrolling a Secure Boot certificate key or database signature
Deleting a Secure Boot certificate key or database signature
Deleting all keys
Exporting a Secure Boot certificate key or database signature
Exporting all Secure Boot certificate keys
Resetting a Secure Boot certificate key or database signature to platform defaults
Resetting all Secure Boot certificate keys to platform defaults
TLS (HTTPS) Options
Viewing TLS certificate details
Enrolling a TLS certificate
Deleting a TLS certificate
Deleting all TLS certificates
Exporting a TLS certificate
Exporting all TLS certificates
Resetting all TLS settings to platform defaults
Configuring advanced TLS security settings
Enabling or disabling Intel TXT support
Enabling or disabling the One-Time Boot Menu F11 prompt
Enabling or disabling processor AES-NI support
Enabling or disabling backup ROM image authentication
Managing firmware, OS software, and language packs
Firmware updates
Online firmware update
Online firmware update methods
Offline firmware update
Offline firmware update methods
HPE OneView 4.0 for HPE Synergy security

Best practices for maintaining a secure appliance ................................................. 224
Understanding the security features of HPE OneView ........................................... 227
About certificate validation ................................................................................... 228
About complex passwords .................................................................................... 228
About directory service authentication ................................................................. 229
About emergency local login ............................................................................... 231
About permissions ................................................................................................ 231
About scopes ......................................................................................................... 232
About trusting certificates .................................................................................... 232
About user accounts ............................................................................................. 232
About user roles .................................................................................................... 233
Action privileges for user roles ............................................................................ 236
Scope-enabled resource categories ..................................................................... 248
Security-hardened appliance ............................................................................... 249
Creating a login session ....................................................................................... 251
Authentication for appliance access .................................................................... 251
Two-factor Authentication ..................................................................................... 252
Certificate owner - Subject alternative name attributes ...................................... 253
Certificate owner - Subject attributes .................................................................. 254
Directory domain .................................................................................................. 255
Requirements to validate the certificate ............................................................... 256
Controlling access for authorized users .............................................................. 256
Specifying user accounts and roles ................................................................….. 256
Mapping of SSO roles for iLO ............................................................................ 256
Mapping appliance interactions with iLO and IPDU .......................................... 257

Contents

Algorithms for securing the appliance ................................................................. 196
Files you can download from the appliance ....................................................... 201
Modeling scope-based access control in HPE OneView ................................. 202
About scope-based access control ..................................................................... 202
Scope-based access control authorization semantics ...................................... 202
Scope-based access control facts ...................................................................... 204
Scope-based access control implementation process ...................................... 206
Design the authorization model ........................................................................ 206
Configure the authorization model .................................................................... 208
Scope-based access control example: Scenario overview ................................. 208
Example: Identify users and groups ................................................................. 209
Example: Determine the best fit HPE OneView role ........................................ 210
Example: Define permission scopes ................................................................. 212
Certificate management....................................................................................... 216
Establishing trust between a web browser and HPE OneView ......................... 216
Establishing trust between HPE OneView and remote devices ....................... 217
Certificate authority or public key infrastructure-based trust ........................... 217
Using scripts to enable PKI or CA-based trust ..................................................... 218
User-verified initial trust ..................................................................................... 218
Automatic initial trust ......................................................................................... 218
Certificates in HPE OneView ............................................................................. 220
Certificate Revocation Lists ............................................................................... 221
Certificate status checks ..................................................................................... 222
Expiry checks for self-signed certificates of devices ............................................ 222
Device-specific certificate handling .................................................................... 222
Integrated Lights-Out certificates ....................................................................... 222
Onboard Administrator Certificates .................................................................... 222
Enabling and disabling certificate validation .................................................... 223
Mapping appliance interactions with iLO and IPDU ......................................... 257
Secure Shell access........................................................................................................ 258
Protecting credentials................................................................................................. 258
Understanding the audit log....................................................................................... 258
Choosing a policy for the audit log............................................................................. 260
Appliance access over TLS ....................................................................................... 260
Managing certificates from a browser........................................................................ 260
Self-signed certificate........................................................................................................ 261
Use a certificate authority............................................................................................. 261
Create an appliance certificate signing request......................................................... 262
Create an appliance self-signed certificate................................................................. 262
Create a CA-signed client certificate for SCMB......................................................... 263
Import an appliance certificate..................................................................................... 264
View the Certificate settings.......................................................................................... 265
Download a self-signed certificate................................................................................ 265
Verify a certificate.......................................................................................................... 266
Trusting a certificate....................................................................................................... 266
Nonbrowser clients........................................................................................................ 267
Passwords....................................................................................................................... 267
TLS connection.............................................................................................................. 267
SSH connection............................................................................................................. 267
Ports required for HPE OneView.................................................................................. 267
Controlling access to the appliance console.............................................................. 269
Enable or disable authorized services access............................................................... 269
Algorithms for securing the appliance........................................................................... 270
Files you can download from the appliance ............................................................... 274
Modeling scope-based access control in HPE OneView .............................................. 275
About scope-based access control............................................................................. 275
Scope-based access control authorization semantics................................................. 276
Scope-based access control facts.................................................................................. 277
Scope-based access control implementation process................................................. 279
Design the authorization model.................................................................................... 279
Configure the authorization model............................................................................... 281
Scope-based access control example: Scenario overview............................................. 281
Example: Identify users and groups............................................................................ 282
Example: Determine the best fit HPE OneView role.................................................... 283
Example: Define permission scopes............................................................................. 285
Certificate management.................................................................................................. 289
Establishing trust between a web browser and HPE OneView..................................... 289
Establishing trust between HPE OneView and remote devices................................... 290
Certificate authority or public key infrastructure-based trust....................................... 290
Using scripts to enable PKI or CA-based trust............................................................. 291
User-verified initial trust............................................................................................... 291
Automatic initial trust................................................................................................... 291
Certificates in HPE OneView....................................................................................... 293
Certificate Revocation Lists......................................................................................... 294
Certificate status checks.............................................................................................. 295
Expiry checks for self-signed certificates of devices..................................................... 295
Device-specific certificate handling.............................................................................. 295
Integrated Lights-Out certificates.................................................................................. 295
Enabling and disabling certificate validation............................................................... 295

Support and other resources......................................................................................... 297
Accessing Hewlett Packard Enterprise Support.......................................................... 297
Accessing updates......................................................................................................... 297
Customer self repair...................................................................................................... 298
Remote support........................................................................................................................................ 298
Warranty information............................................................................................................................. 298
Regulatory information.......................................................................................................................... 299
Documentation feedback....................................................................................................................... 299

Frequently asked questions.................................................................................................................... 300
Introduction

The importance of security

As threats move from network security to the hardware and firmware layers, HPE Gen10 security features help protect your hardware, firmware, and network components from unauthorized access and unapproved use. HPE offers an array of embedded and optional software and firmware for HPE Gen10 that enables you to institute the best mix of remote access and control for your network and data center.

HPE Gen10 servers are offered with the following security aware components:

• HPE iLO 5
  The HPE iLO subsystem, a standard component of HPE ProLiant servers, simplifies server setup, health monitoring, power and thermal optimization, and remote server administration. With an intelligent microprocessor, secure memory, and dedicated network interface, iLO offers varying degrees of encryption and security. Ranging from a standard open level (Production) up to the Federal Information Processing Standard (FIPS) and the Commercial National Security Algorithm (SuiteB/CNSA) security, iLO offers administrators a reliable way to integrate HPE ProLiant servers into existing security environments.

• Intelligent Provisioning
  Intelligent Provisioning is a single-server deployment tool embedded in ProLiant Gen10 servers and HPE Synergy compute modules that simplifies server setup, providing a reliable way to deploy servers.

  Intelligent Provisioning prepares the system for installing original, licensed vendor media and Hewlett Packard Enterprise-branded versions of OS software, and integrates optimized server support software from the Service Pack for ProLiant (SPP). Intelligent Provisioning also provides an alternative method of configuring HPE iLO 5, including the range of security settings iLO offers.

• Smart Update Manager (SUM)
  SUM is a tool for firmware and driver maintenance which provides a browser-based GUI or a command-line scriptable interface for increased flexibility and adaptability for your needs. SUM includes a discovery engine that finds the installed hardware and current versions of firmware and software in use on target nodes. SUM identifies associated targets you can update at the same time to avoid interdependency issues. SUM deploys updates in the correct order and ensures that all dependencies are met before deploying an update. If SUM finds version-based dependencies it cannot resolve, SUM prevents deployment.

• UEFI System Utilities
  The UEFI System Utilities is embedded in the system ROM. Unified Extensible Firmware Interface (UEFI) defines the interface between the operating system and platform firmware during the boot, or start-up process. UEFI supports advanced pre-boot user interfaces and extended security control. Features such as Secure Boot enable platform vendors to implement an OS-agnostic approach to securing systems in the pre-boot environment. The ROM-Based Setup Utility (RBSU) functionality is available from the UEFI System Utilities along with additional configuration options.

HPE Gen10 platform security features and licensing

HPE iLO licensing

iLO is available at three license levels, each offering increasingly sophisticated capabilities.
• iLO Standard—The default no-cost license available for all installations of iLO includes industry standard security features. Servers are also protected by the new hardware root of trust, standard on all Gen10 servers that use iLO.

• iLO Advanced—This license offers advanced security features, with secure remote management. Also includes directory integration, common access card support (also known as CAC, or smartcard support), and Kerberos authentication to a directory service.

• iLO Advanced Premium Security Edition—This license includes high security capabilities, such as automatic firmware recovery, runtime firmware verification, and support for the Commercial National Security Algorithm Suite (CNSA suite). The CNSA is a suite of algorithms defined by NIST and approved by the NSA.

For more information, see the HPE iLO Licensing Guide at http://www.hpe.com/support/iLOLicenseGuide-en or visit http://www.hpe.com/servers/iloadvanced.

HPE Gen10 product security features

Hewlett Packard Enterprise security features are designed to meet challenges such as attacks on firmware by continually improving the hardware and firmware security of Gen10 platforms and related hardware environments—ensuring that every link in the chain of security provides effective security protections.

HPE focused on increasing the level of security in the three critical pillars of the security environment—protect, detect, and recover—so you can be confident that your server hardware infrastructure is secure from threats, and that any potential vulnerabilities will be addressed quickly.

The HPE ProLiant Gen10 servers with the iLO 5 and its silicon root of trust undergo a server boot process that authenticates from the hardware itself and undergoes a series of trusted handshakes before fully initializing the UEFI and the OS. The silicon root of trust enables the detection of previously undetectable compromised firmware or malware. The advanced capabilities of iLO 5 enable daily automatic scanning of firmware and automatic recovery to authentic good states. Combining the Gen10 security features with selected server options allows you to design a resilient and hardened industry-standard server infrastructure.

HPE iLO 5 Security Features

HPE iLO 5 includes the following security features:

• Unauthorized access prevention
• Phlashing protection
• Protected Management ROM
• Protected PCI bus
• Host Access Configuration Lock
• Network and management port control
• Security override switch
• Trusted Platform Module and Trusted Modules
• Compliant with DMZ zones
• Secure communication between iLO and server blades
• Extensive logging to enable efficient security audits
Unauthorized access prevention

Access through an iLO portal involves a multi-layer security process that includes authentication, authorization, data integrity, and security keys. iLO firmware is digitally signed with a private key that prohibits unauthorized firmware from executing.

Authentication

Determines who is at the other end of the network connection using identity verification methods such as Kerberos. Authentication can be performed locally, or through directory services using authentication methods such as Active Directory, SSO, and Smartcard.

Authorization

Determines whether the user attempting to perform a specific action has the right to do it. Using local accounts, you can define separate iLO users and vary their server access rights. Using directory services, you maintain network user accounts and security policies in a central, scalable database that supports thousands of users and system management roles.

Data integrity

Verifies that no one has altered incoming commands or data. iLO uses digital signatures and trusted .NET, Java, and iLO mobile applets available for iOS and Android.

Security keys

Manages confidentiality of sensitive data and transactions. iLO protects privacy through TLS encryption of web pages and the AES encryption of remote console and virtual serial port data. iLO can be configured to allow only the highest cryptographic methods (like AES) to be used. iLO uses layers of security and industry-standard methods to secure access to the server. For example, iLO cryptographic keys use a minimum key length of 128 bits and conform to industry standards. When high encryption modes are not used, iLO may negotiate weaker keys or algorithms.

Phlashing protection

Phlashing is a permanent denial of service (PDOS) attack. A PDOS attack could theoretically take advantage of vulnerabilities during updates of network-based firmware. Rogue firmware installed through a PDOS attack could lead to unauthorized server access or permanent hardware damage.

iLO offers following protections:

• Authorized firmware updates – iLO firmware images are digitally signed with a 4096-bit private key. The boot block checks the digital signature every time iLO is reset. iLO checks the digital signature before allowing a firmware update to proceed. Remote flashing requires login authentication and authorization, including optional two-factor authentication.

• Unencrypted ports – iLO clearly defines the port encryption status. You can disable access to any non-encrypted ports (such as IPMI). Access to iLO requires a password unless you decide to disable the password.

• Authentication and audit trails – iLO creates a log of authentication failures and successes across every interface. SSH-key authentication makes successful brute force attacks even less likely. For additional protection, iLO 5 uses 2048-bit DSA or RSA keys and, in SuiteB security state, iLO requires ECDSA 384-bit keys.
• Unsuccessful Login delays – iLO captures all login activity. It uses a progressive timed delay during unsuccessful login attempts to impede brute force and dictionary attacks.

• Restricted access and modification of critical security parameters – iLO logs many security parameter changes such as user accounts, log changes, and certificates. This allows tracing potential unauthorized information access attempts.

Protected Management ROM

There are two types of signature checking of the iLO firmware image. There is the validation of a new image before it is programmed into iLO’s flash device and there is the integrity check of this image as iLO boots.

Image Validation

The entire image is hashed with SHA512 and signed using Hewlett Packard Enterprise’s RSA 4096-bit private key. This signature block is pre-pended to the firmware binary image.

When performing a firmware update, the hash is decrypted by the currently executing iLO firmware with Hewlett Packard Enterprise’s public key. This hash is compared with a hash of the entire image. If they match, the firmware update is allowed to proceed. The signature block is discarded.

Boot-Time Integrity Check

At boot time, each piece has its signature validated before it is allowed to execute. Subsequent pieces are checked by the previous ones until iLO is fully booted.

If an image becomes corrupt to the point that it will not boot, iLO automatically recovers from a backup image in the system recovery set.

Individual parts, such as the kernel, of the iLO firmware image are also signed. These integrity signatures are not discarded during the flash process.

Protected PCI bus

iLO shields keys and data stored in memory and firmware, and does not allow direct access to keys via the PCI bus.

Host Access Configuration Lock

When the iLO 5 security state is set to HighSecurity or better, iLO access from the host operating system prevents configuration changes with a Host Access Configuration Lock.

When using RIBCL or IPMI, the system will respond with an insufficient privilege level error for commands while the lock is enabled (note that for IPMI, any commands require a session login and it is possible to set the maximum privilege level that can be accepted when the lock is enabled.)

Network and management ports

iLO’s firewall and bridge logic prevent any connection between the iLO management port and the server Ethernet port. Even by using the shared network port (SNP), iLO cannot bridge traffic between its 10/100/1000 Ethernet port and the server Ethernet port. Therefore, attacks on the server network cannot compromise iLO and vice-versa.

Shared network port

Most ProLiant ML and DL servers with iLO support SNP. Consult the server documentation to determine whether your ProLiant server supports SNP. Hewlett Packard Enterprise does not support SNP on HPE BladeSystem server blades or Synergy systems.

The SNP lets iLO management traffic use a sideband connection on the server NIC rather than dedicating a second port to iLO management traffic. Although the iLO traffic shares a port with the server OS traffic, both iLO and the server NIC have their own MAC and IP address. This ensures that other devices can
independently address iLO. This is an advantage if you want to install and maintain a single network infrastructure for handling both management and productivity traffic.

![Diagram of traffic paths of shared and dedicated networks]

**Figure 1: Traffic paths of shared and dedicated networks**

**Shared network port with Virtual LAN**

Implementing Virtual LAN (VLAN) tags enhances iLO SNP security. When you enable VLAN Tags, the iLO SNP becomes part of a Virtual LAN. The VLAN is a logical network that isolates network traffic to segments. It increases security because established rules keep traffic on one segment from entering another segment. All network devices with the same Virtual LAN tag appear to be on a separate LAN even if they are physically connected to the same LAN. The SNP NIC checks the Ethernet frame for a VLAN ID and compares it against its configured value. If they match, then the SNP strips the frame of the VLAN tag and forwards it to iLO. If they do not match, the SNP forwards the frame to the server. The SNP NIC inserts a VLAN tag into any outgoing Ethernet frames.

**Security Override switch**

You can disable all of iLO’s security authorization checks by turning on the Security Override switch. This gives you access to the following tasks:

- Reconfigure iLO through ROM-Based Setup (RBSU) even if RBSU is disabled
- Log into iLO without credentials

⚠️ **IMPORTANT:**

The Security Override switch does not allow login to iLO without credentials when the iLO is in HighSecurity mode or above.

**Trusted Platform Module and Trusted Modules**

Trusted Platform Modules and Trusted Modules are computer chips that securely store artifacts used to authenticate the platform. The iLO Overview page displays the following **TPM Status** or **TM Status** information:
• **Not Supported**—A TPM or TM is not supported.

• **Not Present**—A TPM or TM is not installed.

• **Present-Enabled**—A TPM is installed and enabled.

If a TPM or TM module is present on the server, **Module Type** is added to the display. Module Type displays one of the following statuses, indicating whether a TPM is installed or supported, or indicating the version for supported modules:

• **TPM 1.2**

• **TPM 2.0**

• **TM 1.0**

• **Not Specified**

• **Not Supported**

**Operating iLO servers in the DMZ**

An Internet-connected architecture typically has a more secure, de-militarized zone (DMZ). The DMZ zone lies between the corporate servers and the Internet. The DMZ zone usually has a firewall that restricts traffic flow between the corporate/Internet areas. You may access servers that provide publicly available Internet services through a firewall. However, you cannot access these services on the internal network. This more secure zone provides an area isolated from the internal network and hardened against external attack. The security challenges of a DMZ require a balance between critical security requirements, and the need for effective management and system maintenance.
Figure 2: Example configuration of a DMZ

iLO can exist on a separate, secondary network parallel to the primary or production network. This dual-network architecture segregates management traffic from production network traffic. The segregation allows group server management activities, including servers inside the DMZ. Maximum security is maintained by limiting access to the production network.

The image shows a packet-filtering router that acts as an initial line of defense. Behind this router is a firewall. There is no direct connection from the Internet or the external router to the internal network. All traffic to or from the internal network must pass through the firewall. An additional router filters packets destined for the public services in the DMZ and protects the internal network from public access.

The firewall is a server that you can configure to evaluate traffic according to different rules based on the traffic source and destination:

- From the Internet to the DMZ
- From the DMZ to the Internet
- From the Internet to the internal network
- From the internal network to the Internet
- From the DMZ to the internal network
- From the internal network to the DMZ

Servers inside the DMZ and on the internal network can use iLO processors. Data cannot flow between the DMZ network and the iLO network. The network connection to iLO is completely isolated from the network ports on the server. Even if the DMZ network were compromised, the iLO network would remain secure. This isolation lets you use iLO on servers located in the DMZ or in the internal network without compromising...
sensitive data. Administrators create this separation by using a dedicated NIC or the SNP with its VLAN (see the section "Shared network port" on page 13).

Communication between iLO and server blades or Synergy systems

The HPE BladeSystem architecture uses a single enclosure to hold multiple servers. A separate power subsystem provides power to all servers in that enclosure. ProLiant c-Class server blades and Synergy systems use iLO to send alerts and management information throughout the server blade infrastructure.

There is a strict communication hierarchy among server or system components. The Onboard Administrator (OA) management module (or FLM - Frame Link Module for Synergy) communicates with the iLO processor on each server blade or Synergy system. The OA module or FLM provides independent IP addresses. The iLO device also maintains an independent IP address. The iLO firmware exclusively controls any communication from iLO to the OA module or FLM. There is no connection from the iLO processor or OA module/FLM to the server NICs. The iLO processor only has information about the presence of other server blades/systems in the infrastructure and whether enough amperage is available from the power subsystem to boot. A single, physical port on the rear of the enclosure provides access to the iLO network connections on the server blade or Synergy system. This simplifies and reduces cabling.

Security audits

A company's policy may mandate periodic security audits. iLO maintains an event log containing date- and time-stamped information pertaining to events that occurred in the iLO configuration and operation. You can manually access this log through the System Status tab of the iLO browser interface. You can also use the HPE RESTful API and RESTful commands to set up an automated examination and extraction process that parses the event log by date/time and by authenticated user for accessing information about security events.

Security vulnerability scanners and iLO

Security vulnerability scanners are tools commonly used in server environments to probe for weaknesses that need to be investigated and addressed. The iLO team uses security vulnerability scanners in our quality labs for every release of iLO firmware. There are known issues and best practices associated with the use of security vulnerability scanners. If the business requirements of your organization require vulnerability scans, remember that setting the iLO 5 security state to HighSecurity or better is a security best practice.

A best practice is to test new versions of security vulnerability scanners in a lab environment before deploying to a production environment. By definition the security vulnerability scanner is probing interfaces for known or suspected vulnerabilities. In effect, the scanner is attempting to hack the interface being tested. This operation may have a negative impact on the stability of the system being scanned. Therefore, it makes sense to start on a small scale and then move to a wider scale and production environment.

There are some known issues that most security vulnerability scanners will identify. These items are listed in the following sections, and include remediation recommendations. Many of the issues shown are resolved by setting the iLO 5 security state to HighSecurity or better.


Documentation for the iLO RESTful API can be found at [https://hewlettpackard.github.io/ilo-rest-api-docs/](https://hewlettpackard.github.io/ilo-rest-api-docs/). Documentation for the RESTful Interface Tool can be found at [https://hewlettpackard.github.io/python-redfish-utility/](https://hewlettpackard.github.io/python-redfish-utility/).

X.509 Certificate Subject CN Does Not Match the Entity Name

Replace the default, self-signed SSL certificate with a certificate signed by a Certificate Authority. When iLO left the factory, the customer, DNS name/IP address of the server is unknown. Therefore, iLO uses a self-signed certificate. iLO firmware provides the capability to create a Certificate Signing Request (CSR) that you can use to request/create a signed certificate that matches their system. This signed certificate can then be imported back into the iLO.

This is documented in the HPE iLO 5 user guide.
The CSR process can also be executed using iLO’s XML scripting or by using the RESTful Interface Tool with the iLO RESTful API. The specific XML scripting commands are in the iLO scripting and command line user guide, while the documentation for the RESTful Interface Tool and the iLO RESTful API is available on the github sites.

**IPMI 2.0 RAKP RMCP+ Authentication HMAC Password Hash Exposure**

The IPMI handshake that is required in the IPMI specification should be more secure. IPMI is disabled by default in iLO 5. For customers who are not actively using IPMI, Hewlett Packard Enterprise recommends leaving the IPMI over LAN interface disabled. Instead, HPE recommends that you use the iLO RESTful API - a programmatic interface - and the industry-standard “Redfish” as a replacement for IPMI over LAN capabilities.

- Enabling/Disabling IPMI is documented in the iLO 5 User Guide.
- Enabling/Disabling IPMI can also be executed using iLO’s XML scripting and is documented in the iLO Scripting and Command Line user guide.

If you require the use of IPMI, re-enabling it will expose this issue. For more information about the iLO RESTful API and the RESTful Interface Tool, see [http://www.hpe.com/info/redfish](http://www.hpe.com/info/redfish) or the GitHub repositories.

**Untrusted TLS/SSL server X.509 certificate**

Replace the default, self-signed SSL certificate with a certificate signed by a Certificate Authority. When iLO left the factory, the customer, DNS name/IP address of the server is unknown. Therefore, iLO uses a self-signed certificate. iLO firmware provides the capability to create a Certificate Signing Request (CSR) that you can use to request/create a signed certificate that matches their system. This signed certificate can then be imported back into the iLO.

The CSR process can also be executed using the RESTful Interface Tool and iLO RESTful API, or by using iLO’s XML scripting.

**IPMI 1.5 GetChannelAuth Response Information Disclosure**

This is an assumed vulnerability based on HPE support of the IPMI protocol. iLO itself is not susceptible to this vulnerability. This vulnerability report can be suppressed by disabling IPMI as described in the RAKP vulnerability.

**TCP Sequence Number Approximation Vulnerability**

iLO uses TCP sequence number randomization and is resistant to TCP sequence number approximation attacks. iLO is not susceptible to this vulnerability.

**IPMI 2.0 RAKP RMCP+ Authentication Username Disclosure**

The IPMI specification enables a pre-authenticated client to confirm the existence of a configured username. HPE recommends changing the default username. Additionally, when not actively using IPMI, HPE recommends disabling the interface as described in the RAKP vulnerability.

**Weak Cryptographic Key**

This vulnerability may be addressed by setting the iLO 5 security state to **HighSecurity**. This will require iLO to use the higher grade ciphers.

This vulnerability will also be reported if the default SSL certificate is used. This is addressed, as documented above, by creating a Certificate Signing Request and importing a CA-signed certificate.

The CSR process can also be executed using the RESTful Interface Tool and iLO RESTful API, or by using iLO’s XML scripting.
TCP timestamp response

This is a standard TCP behavior. The theory is that this can be used to estimate the uptime of the system, which could then be used for further attacks. This has a very low CVE vulnerability rating of 1.

Firmware verification

The Firmware Verification page allows you to run an on-demand scan or implement scheduled scans. To respond to detected issues, choose between logging the results or logging the results and initiating a repair action that uses a recovery install set.

Depending on the scan results, information is logged in the Active Health System Log and the Integrated Management Log.

The following firmware types are supported:

- iLO Firmware
- System ROM (BIOS)
- System Programmable Logic Device (CPLD)
- Server Platform Services (SPS) Firmware
- Innovation Engine (IE) Firmware

When a firmware verification scan is in progress, you cannot install firmware updates or upload firmware to the iLO Repository.

If a supported management tool is configured to listen for system recovery events, you can send a recovery event from this page.

Running a firmware verification scan

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: http://www.hpe.com/support/ilo-docs.

Procedure

1. Navigate to the Administration page, and then click the Firmware Verification tab.
2. Click Run Scan.

When a firmware verification scan is in progress, you cannot install firmware updates or upload firmware to the iLO Repository.

The scan results are displayed at the top of the page.

If a failure occurred, the firmware state on the Firmware Verification page changes to Failed/Offline, the System Health status changes to Critical, and an event is recorded in the IML. If the firmware verification scan feature is configured to Log and Repair Automatically, the failed firmware is flashed. If successful, the firmware state and System Health status are updated, and the IML event changes to Repaired status.

If automatic repair is not configured, you must complete the repair manually. For more information, see the iLO user guide.
Configuring the firmware verification settings

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: http://www.hpe.com/support/ilo-docs.

Procedure

1. Navigate to the Administration page, and then click the Firmware Verification tab.
2. Click the Scan Settings icon.
3. Set Enable Background Scan to enabled or disabled status.
4. Select an Integrity Failure Action.
5. Set the Scan Interval in days. Valid values are from 1 to 365 days.
6. Click Submit.

Firmware Verification scan options

- **Enable Background Scan**—Enables or disables Firmware Verification scanning. When enabled, iLO scans the supported installed firmware for file corruption.
- **Integrity Failure Action**—Determines the action iLO takes when a problem is found during a Firmware Verification scan.
  - To log the results, select Log Only.
  - To log the results and initiate a repair action, select Log and Repair Automatically.
    - If a problem is detected for a supported firmware type, iLO checks for the affected firmware type in a protected install set. By default, this set is the Recovery Set. If a firmware image is available, iLO flashes that firmware image to complete the repair.
- **Scan Interval (in days)**—Sets the background scan frequency in days. Valid values are from 1 to 365.

Viewing firmware health status

Prerequisites

A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: http://www.hpe.com/support/ilo-docs.
Procedure

Navigate to the **Administration** page, and then click the **Firmware Verification** tab.

**Firmware health status details**

The following information is displayed for each supported firmware type.

**Firmware Name**

The name of the installed firmware.

**Firmware Version**

The firmware version.

**Health**

The firmware health status.

**State**

The firmware status. The possible values follow:

- **Enabled**—The firmware is verified and enabled.
- **Scanning**—A firmware verification scan is in progress or is about to start.
- **Flashing**—A firmware update is in progress.
- **Failed/Offline**—The firmware could not be verified and was not repaired.

**Recovery Set Version**

The version of the firmware in the System Recovery Set.

If this firmware type is not in the System Recovery Set, or there is no System Recovery set, **Not present** is displayed.

**HPE Gen10 UEFI security features**

The following features are present in HPE Gen10 servers:

- Power On Password
- Admin Password
- Secure Boot and Advanced Secure Boot (including PK, KEK, DB/DBX options)
- TLS (HTTPS) Boot
- TPM 1.2 and 2.0
- Intel® TXT Support
- One-Time Boot
- Intelligent Provisioning (F10 prompt) disable
- Processor AES-NI Support
- Other UEFI security related options include:
  - Secure Start
  - No-Execute Protection
Intelligent Provisioning Security Features

Intelligent Provisioning

Intelligent Provisioning is a single-server deployment tool embedded in ProLiant servers and HPE Synergy compute modules. Intelligent Provisioning simplifies server setup, providing a reliable and consistent way to deploy servers.

Intelligent Provisioning prepares the system for installing original, licensed vendor media and Hewlett Packard Enterprise-branded versions of OS software. Intelligent Provisioning also prepares the system to integrate optimized server support software from the Service Pack for ProLiant (SPP). SPP is a comprehensive systems software and firmware solution for ProLiant servers, server blades, their enclosures, and HPE Synergy compute modules. These components are preloaded with a basic set of firmware and OS components that are installed along with Intelligent Provisioning.

IMPORTANT:

HPE ProLiant XL servers do not support operating system installation with Intelligent Provisioning, but they do support the maintenance features. For more information, see “Performing Maintenance” in the Intelligent Provisioning User Guide and online help.

After the server is running, you can update the firmware to install additional components. You can also update any components that have been outdated since the server was manufactured.

To access Intelligent Provisioning:

- Press F10 from the POST screen.
- From the iLO web browser user interface using Always On. Always On allows you to access Intelligent Provisioning without rebooting your server.

Intelligent Provisioning security through iLO

Intelligent Provisioning security features depend on iLO security settings. Accessing Intelligent Provisioning requires rebooting a server and pressing the correct key during the boot process, or by using the Always On Intelligent Provisioning feature through iLO 5.

- Remote access is controlled by iLO, through required credentials and variable levels of configurable encryption. Users must have the iLO privileges Host BIOS and Remote Console to launch Always On Intelligent Provisioning.
- Physical access to the server is a function of your organization’s physical security mechanisms.

Intelligent Provisioning supports the security modes available through HPE iLO, including FIPS mode, and adheres to TPM requirements.
Intelligent Provisioning security through UEFI

Access to Intelligent Provisioning can be removed through UEFI/BIOS settings. An option available in the Server Security portion of the available settings allows you to disable the F10 key during the boot process. For more information, see UEFI configuration security.

iLO Amplifier Pack security features

The iLO Amplifier Pack is an advanced server inventory and firmware and driver update solution that enables rapid discovery, detailed inventory reporting, and firmware and driver updates by leveraging iLO advanced functionality. The iLO Amplifier Pack performs rapid server discovery and inventory for thousands of supported servers for the purpose of updating firmware and drivers at scale.

The iLO Amplifier Pack includes detailed server alerting capabilities to help keep servers secure, and powerful automated recovery to mitigate firmware corruption.

Note that iLO Amplifier Pack does not support iLO security states greater than Production. The evolving nature of HPE security capabilities means that some functions are still in development. Future releases will have more capabilities.
HPE Gen10 recommended security settings

Refer to the following tables for the paths and recommended settings for security related functions in Gen10 embedded applications.

When determining the level of security to implement, organizations must find a balance between the security settings for iLO and associated applications, versus the adoption of unnecessarily restrictive security settings that hinder system usage. Weigh the need to protect the data in your environment against the need for authorized users to readily access that data. Enabling every possible suggested security setting may not be the best approach for your organization.

### iLO 5 settings

<table>
<thead>
<tr>
<th>Feature or function</th>
<th>Path</th>
<th>Setting</th>
<th>Suggested setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPM or TM status</td>
<td>Information &gt; Overview</td>
<td>TPM Status</td>
<td>Read only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Module Type</td>
<td>Read only (displays only when a TPM or TM is present)</td>
</tr>
<tr>
<td>Local user account controls</td>
<td>Administration &gt; User Administration</td>
<td>Add, edit, and delete local users</td>
<td>Up to 12 local accounts, with a range of individual user privilege settings to support the security principle of least access.</td>
</tr>
<tr>
<td>Directory group account controls</td>
<td>Administration &gt; Directory Groups</td>
<td>Add, edit, and delete directory groups</td>
<td></td>
</tr>
<tr>
<td>iLO service settings</td>
<td>Security &gt; Access Settings</td>
<td>Secure Shell (SSH)</td>
<td>Enabled (also must set port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web Server</td>
<td>Enabled (also must set Non-SSL and SSL ports)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Console</td>
<td>Enabled (also must set port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virtual Media</td>
<td>Enabled (also must set port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMP</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPMI/DCMI over LAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>iLO access options</td>
<td>Security &gt; Access Settings</td>
<td>iLO Functionality</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iLO Web Interface</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iLO RIBCL Interface</td>
<td>Enabled (although HPE recommends using the iLO RESTful API)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iLO ROM-Based Setup Utility</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Require Login for iLO RBSU</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Feature or function</th>
<th>Path</th>
<th>Setting</th>
<th>Suggested setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show iLO IP during POST</td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Virtual Serial Port Log</td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>XML Reply</td>
<td></td>
<td>Disabled (Enable to have the iLO discoverable on your network)</td>
<td></td>
</tr>
<tr>
<td>Serial Command Line Interface</td>
<td></td>
<td>Enabled-Authentication Required</td>
<td>(Also must set speed)</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td></td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Server Name</td>
<td></td>
<td>Leave blank and let host OS assign</td>
<td></td>
</tr>
<tr>
<td>Server FQDN/IP Address</td>
<td></td>
<td>Leave blank and let host OS assign</td>
<td></td>
</tr>
<tr>
<td>Authentication Failure Logging</td>
<td></td>
<td>Enabled-Every Failure</td>
<td></td>
</tr>
<tr>
<td>Authentication Failure Delay</td>
<td></td>
<td>10 seconds</td>
<td></td>
</tr>
<tr>
<td>Authentication Failures Before Delay</td>
<td></td>
<td>1 Failure causes no delay</td>
<td></td>
</tr>
<tr>
<td>iLO Service Port</td>
<td>Security &gt; iLO Service Port</td>
<td>iLO Service Port</td>
<td>Enabled</td>
</tr>
<tr>
<td>USB flash drives</td>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Require authentication</td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>USB Ethernet adapters</td>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>SSH key administration</td>
<td>Security &gt; Secure Shell Key</td>
<td>Keys must be 2048-bit DSA or RSA (or ECDSA 384-bit keys in SuiteB security state)</td>
<td>Using SSH keys provides better security than simple password authorization.</td>
</tr>
<tr>
<td>Certificate to user mapping</td>
<td>Security &gt; Certificate Mappings</td>
<td>Each local user account must have an associated certificate.</td>
<td>Using a Smartcard with certificates provides better security than simple password authentication</td>
</tr>
<tr>
<td>Smartcards</td>
<td>Security &gt; CAC/Smartcard</td>
<td>CAC Smartcard Authentication</td>
<td>Enabled (Requires an iLO Advanced license)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CAC Strict Mode</td>
<td>(Optional) Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import Trusted CA Certificates and revocation list</td>
<td>At least one trusted CA certificated must be installed, along with revocation list.</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Feature or function</th>
<th>Path</th>
<th>Setting</th>
<th>Suggested setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL certificate administration</td>
<td>Security &gt; SSL Certificate</td>
<td>Customize Certificate</td>
<td>Create a trusted SSL certificate for each iLO. Default self-signed certificates are not secure.</td>
</tr>
<tr>
<td>Directory-based authentication</td>
<td>Security &gt; Directory</td>
<td>LDAP Directory Authentication</td>
<td>Use HPE Extended Schema (requires Active Directory) or use Directory Default Schema (Also must set all Directory Server Settings on page, according to your environment)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local User Accounts</td>
<td>Depending on environment, enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kerberos Authentication</td>
<td>Enabled (Also must set Realm, Server Address, Server Port, and Keytab file)</td>
</tr>
<tr>
<td>Encryption</td>
<td>Security &gt; Encryption</td>
<td>Security State</td>
<td>HighSecurity</td>
</tr>
<tr>
<td>HPE SSO</td>
<td>Security &gt; HPE SSO</td>
<td>Single Sign-On Trust Mode</td>
<td>Trust by Certificate²</td>
</tr>
<tr>
<td>Login security banner</td>
<td>Security &gt; Login Security Banner</td>
<td>Enable Login Security Banner</td>
<td>Enabled (Also must set a security message)</td>
</tr>
</tbody>
</table>

1 If disabled, access is removed for RIBCL, iLO RESTful API, remote console, iLO Federation, and the iLO web interface.
2 Some HPE applications may not successfully use SSO when the iLO 5 security state is set to HighSecurity and above. See your application's documentation for more information.

**UEFI settings**

<table>
<thead>
<tr>
<th>Feature or function</th>
<th>Path</th>
<th>Setting</th>
<th>Suggested setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Settings</td>
<td>System Configuration &gt; BIOS/Platform</td>
<td>Set Power On Password</td>
<td>Password compliant with strong security standards.</td>
</tr>
<tr>
<td></td>
<td>Configuration (RBSU) &gt; Server Security</td>
<td>Set Admin Password</td>
<td>Set a password that is compliant with strong security standards.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intel TXT Support</td>
<td>Enabled, if available on your system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>One-Time Boot Menu (F11 Prompt)</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intelligent Provisioning (F10 Prompt)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Feature or function</th>
<th>Path</th>
<th>Setting</th>
<th>Suggested setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Processor AES-NI Support</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup ROM Image Authentication</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System Intrusion Detection</td>
<td>Enabled</td>
</tr>
<tr>
<td>Secure Boot Settings</td>
<td>System Configuration &gt; BIOS/Platform Configuration (RBSU) &gt; Server Security &gt; Secure Boot Settings</td>
<td>Attempt Secure Boot</td>
<td>Enabled¹</td>
</tr>
<tr>
<td>Advanced Secure Boot Options</td>
<td>System Configuration &gt; BIOS/Platform Configuration (RBSU) &gt; Server Security &gt; Secure Boot Settings &gt; Advanced Secure Boot Options</td>
<td>Settings for PK, KEK, DB, DBX, and DBT. Also includes controls for deleting all keys, exporting all keys, or resetting all to defaults.</td>
<td>See the UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy</td>
</tr>
<tr>
<td>TLS (HTTPS) Options</td>
<td>System Configuration &gt; BIOS/Platform Configuration (RBSU) &gt; Server Security &gt; TLS (HTTPS) Options</td>
<td>Settings for viewing, enrolling, deleting, and exporting certificates. Also includes controls for deleting, exporting, or resetting all certificates.</td>
<td>See the UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy</td>
</tr>
<tr>
<td>Advanced Security Settings</td>
<td>System Configuration &gt; BIOS/Platform Configuration (RBSU) &gt; Server Security &gt; TLS (HTTPS) Options &gt; Advanced Security Settings</td>
<td>Cipher suites allowed for TLS connections</td>
<td>Select the allowed ciphers for TLS connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certificate validation for every TLS connection</td>
<td>Peer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strict Hostname checking</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TLS Protocol Version Support</td>
<td>Auto</td>
</tr>
<tr>
<td>Trusted Platform Module Options</td>
<td>System Configuration &gt; BIOS/Platform Configuration (RBSU) &gt; Server Security &gt; Trusted Platform Module Options</td>
<td>Chipset-TPM</td>
<td>Enable²</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current TPM Type</td>
<td>(Read only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current TPM State</td>
<td>(Read only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TPM 2.0 Operation</td>
<td>No Action</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TPM Mode Switch</td>
<td>TPM 2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TPM 2.0 Visibility</td>
<td>Visible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TPM UEFI Option ROM Measurement</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Feature or function</th>
<th>Path</th>
<th>Setting</th>
<th>Suggested setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SATA Secure erase</td>
<td><strong>System Configuration</strong> &gt; BIOS/Platform Configuration (RBSU) &gt; Storage Options &gt; SATA Controller Options</td>
<td>Embedded SATA Configuration</td>
<td>To support secure erase, this option must be set to SATA AHCI Support and the SATA drives installed must support the Secure Erase command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SATA Secure Erase</td>
<td>Enable this to allow SATA secure erase functions to work. This control does not start the secure erase function.</td>
</tr>
</tbody>
</table>

**UEFI iLO 5 Configuration Utility**

<table>
<thead>
<tr>
<th>iLO 5 configuration options</th>
<th><strong>System Utilities</strong> &gt; System Configuration &gt; iLO 5 Configuration Utility</th>
<th>iLO 5 Functionality</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iLO 5 Configuration Utility</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Require user login and configuration privilege for iLO 5 Configuration</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Show iLO 5 IP Address during POST</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Local Users</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial CLI Status</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial CLI Speed (bits/second)</td>
<td>As appropriate for your environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iLO Web Interface</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 Secure Boot requires UEFI boot mode.
2 If you have a discrete TPM to install, such as the HPE TPM 2.0 Gen10 Kit, set this to disabled before installation. Consult your operating system documentation to stop any TPM usage before disabling this setting, or data loss can occur.
3 TPM 2.0 Operation, and the following three options only display when a TPM module is installed.

**Intelligent Provisioning settings (server decommissioning)**

<table>
<thead>
<tr>
<th>Feature or function</th>
<th>Path</th>
<th>Setting</th>
<th>Suggested setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase devices</td>
<td>Press F10 during POST, or from iLO 5, click Intelligent Provisioning &gt; Always On. Then click Perform Maintenance &gt; System Erase and Reset</td>
<td>Erase all hard drives</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure erase of non-volatile storage</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clear Intelligent Provisioning preferences</td>
<td>Enable</td>
</tr>
<tr>
<td>Feature or function</td>
<td>Path</td>
<td>Setting</td>
<td>Suggested setting value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------</td>
<td>---------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>iLO security bypass</td>
<td>Remove the chassis cover</td>
<td>Position 1</td>
<td>Off</td>
</tr>
<tr>
<td>System configuration lock</td>
<td></td>
<td>Position 2</td>
<td>On (after configuration is complete)</td>
</tr>
<tr>
<td>Power-on password control</td>
<td></td>
<td>Position 5</td>
<td>On (most secure)</td>
</tr>
<tr>
<td>Restore defaults</td>
<td></td>
<td>Position 6</td>
<td>Off</td>
</tr>
</tbody>
</table>
Hardware security

HPE Gen10 Server hardware security

Introduction

Hewlett Packard Enterprise (HPE) is committed to constantly improving its security stance to meet challenges such as attacks on firmware by continually improving the hardware and firmware security of ProLiant server platforms and related hardware environments—ensuring that every link in the chain of security provides the most effective cyber security protections possible. Enhanced security capabilities are incorporated throughout the HPE Gen10 platforms, including ProLiant, BladeSystem C-Class, Apollo, and Synergy. The first and broadest implementations available will be with the HPE ProLiant Gen10 servers, making it the ideal server platform, as of this writing, to build the industry’s most secure server environment.

Silicon root of trust

With HPE Gen10 Servers, HPE offers the first industry-standard servers to include a silicon root of trust built in to the hardware. The silicon root of trust provides a series of trusted handshakes from lowest level firmware to BIOS and software to ensure a known good state. From this silicon root of trust—server design to specific networking and storage options, HPE has built in security features that help you prevent, detect, and recover from cyber attacks.

The iLO 5 chipset provides an unprecedented level of hardware security with its silicon root of trust. The silicon root of trust:

- Is based in the silicon chip hardware itself
- Is virtually impossible to alter
- Enables firmware to be authenticated as far back as the supply chain
- Provides a secure startup process

The iLO 5 chipset acts as a silicon root of trust and includes an encrypted hash embedded in silicon hardware at the chip fabrication facility. This makes it virtually impossible to insert any malware, virus, or compromised code that would corrupt the boot process. Rather than the iLO firmware checking the integrity of the firmware every time it boots, the iLO 5 hardware determines whether to execute the iLO firmware, based on whether it matches the encryption hash that is permanently stored in the iLO chipset silicon. These improvements help ensure that, if iLO 5 is running, your server is trusted.

The System Maintenance switch

HPE Gen10 Servers are equipped with a hardware System Maintenance switch which controls different aspects of server security, including:

- iLO security—This switch controls whether a password is required to access iLO.

NOTE:

The security switch does NOT disable password requirements for logging in to iLO when iLO is set to higher security modes (any mode other than production mode.)

- System configuration lock—While off, this switch allows changes to the system configuration. When on, the system configuration is locked.
- Power-on password control—This switch controls whether the server requires a password whenever it is cold booted. When off (the default), a power-on password is required whenever power is shut off to the
system (cold booted). When on, the power-on password is disabled. Set the password in the UEFI System Utilities.

- Restore defaults—When the switch is in the on position (the default is off), all manufacturing defaults are restored. However, if Secure Boot is enabled in UEFI, the following items are not reset to factory defaults:
  - Secure Boot is not disabled and remains enabled.
  - The boot mode remains in UEFI boot mode, even if the boot mode is set to Legacy.
  - The Secure Boot Database is not restored to its default state.
  - iSCSI Software Initiator configuration settings are not restored to defaults.

See the hardware guide for your server for specifics on the System Maintenance switch.

**Disable USB ports**

Hewlett Packard Enterprise provides external USB support to enable local connection of USB devices for administration, configuration, and diagnostic procedures. A special iLO-only USB port called the iLO Service port provides direct iLO access.

For more security, external USB functionality can be disabled through USB options in UEFI System Utilities. Additionally, the iLO Service Port must be disabled using the iLO 5 web interface or the HPE RESTful API.

**Trusted Platform Module (TPM)**

The TPM is a hardware-based system security feature that can securely store information, such as passwords and encryption keys, which can be used to authenticate the platform. Trusted Platform Modules securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM to store platform measurements to make sure that the platform remains trustworthy. For servers configured with a Trusted Platform Module, TPM enables the firmware and operating system to take measurements of all phases of the boot process. For information on installing and enabling the TPM module option, see the user documentation for your server model.

TPM (1.2) works with Microsoft Windows BitLocker, which is a data protection feature available in Microsoft Windows Server 2008 R2 SP1 and later operating systems. BitLocker helps protect user data and helps ensure that a server running Windows Server has not been tampered with while the system was offline.

HPE Gen10 and later hardware supports TPM 2.0 only with Windows Server 2016. To prevent possible damage to the TPM or to the system board, the TPM cannot be removed from the board once it has been installed.

**System intrusion detection**

All HPE ProLiant Gen10 servers can optionally add a system intrusion detection switch to the chassis access cover. After installation, whenever the chassis access cover is physically opened or removed an event is recorded in the iLO Integrated Management Log (IML). An alert is also sent to the BIOS whenever a chassis intrusion is detected. The switch and the iLO reporting occur as long as the server is plugged in, regardless of whether the server is powered on or off. You can enable or disable system intrusion detection in UEFI settings.

**Chassis tag**

HPE Servers have an informational tag attached to the chassis during manufacture, which lists pertinent default access information for the server. Some chassis can have more than one, such as a sticker on the underside of the chassis or on a special pull tab on the front. Consult your server’s hardware manual for the exact location.
HPE Gen10 security best practices

HPE Gen10 Servers include many features in embedded software and firmware which keep server deployment secure. Gen10 Server deployment security includes the following areas:

- **Physical access**
- **Configuration**
- **Remote management**
- **Configurable security modes**
- **Protocols, directory integration, access control, and auditing**
- **UEFI, passwords, and TPM**
- **Firmware updates**

Physical access security

The first area of security in any organization is securing physical access to servers. HPE Gen10 servers include the following options to secure physical server access:

- **System Maintenance switch**
- **Chassis intrusion detection**
- **External USB port controls**

The HPE ProLiant Gen10 System Maintenance switch

HPE ProLiant Gen10 Servers are equipped with hardware System Maintenance switches, which control different aspects of server security, including:

- iLO security (position 1)—This switch controls whether a password is required to access iLO.

  **NOTE:**
  This switch does NOT disable password requirements for logging in to iLO when iLO is set to higher security modes (anything other than production mode.)

- System configuration lock (position 2)—While off, this switch allows changes to the system configuration. When on, the system configuration is locked.

- Power-on password control (position 5)—This switch controls whether the server requires a password whenever it is cold booted. When off (the default), a power-on password is required whenever power is shut off to the system (cold booted). When on, the power-on password is disabled. Set the password in the UEFI System Utilities.

- Restore defaults (position 6)—When the switch is in the on position (the default is off), all manufacturing defaults are restored. However, if secure boot is enabled in UEFI, the following items are not reset to factory defaults:
  - Secure Boot is not disabled and remains enabled.
  - The boot mode remains in UEFI boot mode, even if the boot mode is set to Legacy.
- The Secure Boot Database is not restored to its default state.
- iSCSI Software Initiator configuration settings are not restored to defaults.

See the hardware guide for your server for specifics on the System Maintenance switch.

**iLO security with the system maintenance switch**

The iLO security setting on the system maintenance switch provides emergency access to an administrator who has physical control over the server system board. If iLO is configured to use the **Production** security state, disabling security allows login access with all privileges, without a user ID and password.

The system maintenance switch is inside the server and cannot be accessed without opening the server enclosure. When you work with the system maintenance switch, ensure that the server is powered off and disconnected from the power source. Set the switch to enable or disable iLO security, and then power on the server. For detailed information about enabling and disabling iLO security with the system maintenance switch, see the server maintenance and service guide.

The system maintenance switch position that controls iLO security is sometimes called the iLO Security Override switch.

**Reasons to disable iLO security**

- All user accounts that have the Administer User Accounts privilege are locked out.
- An invalid configuration prevents iLO from being displayed on the network, and the ROM-based configuration utility is disabled.
- The iLO NIC is turned off, and it is not possible or convenient to run the ROM-based configuration utility to turn it back on.
- Only one user name is configured, and the password is forgotten.

**Effects of disabling iLO security**

When iLO is set to use the Production security state, and you disable iLO security:

- All security authorization verifications are disabled.
- If the host server is reset, the ROM-based configuration utility runs.
- iLO is not disabled and might be displayed on the network as configured.
- If iLO functionality is disabled, iLO does not log out active users and complete the disable process until the power is cycled on the server.
- A warning message is displayed on iLO web interface pages, indicating that iLO security is disabled:

  ![Alert](image)

- An iLO log entry is added to record the iLO security change.
- If an SNMP Alert Destination is configured, an SNMP alert is sent when iLO starts after you use the system maintenance switch to enable or disable iLO security.
- You cannot perform any action that requires the System Recovery privilege, even if you enter the user credentials for an existing account that has this privilege.
When you log in to iLO when security is disabled, an anonymous account is used, even if you entered a user name and password that matches an existing account.

HPE ProLiant Gen10 system intrusion detection

ProLiant Gen10 servers include an option for a chassis intrusion detection switch, which detects if the chassis access cover is open or closed. The iLO management processor monitors the switch and if there is a change (if the access cover is either opened or closed), it creates a log entry noting the intrusion. You can set various alerting mechanisms (Remote SysLog, SNMP, alertmail, etc.) to be notified of the intrusion. The switch and the iLO reporting occur as long as the server is plugged in, regardless of whether the server is powered on or off.

Enabling or disabling system intrusion detection

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > System Intrusion Detection.
2. Select a setting.
   - Enabled—Intrusion detection is enabled.
   - Disabled—Intrusion detection is not enabled.
3. Save your changes.

iLO Service Port

The Service Port is a USB port with the label iLO on ProLiant Gen10 servers and Synergy Gen10 compute modules.

When you have physical access to a server, you can use the Service Port to do the following:

- Download the Active Health System Log to a supported USB flash drive.
  - When you use this feature, the connected USB flash drive is not accessible by the host operating system.

- Connect a client (such as a laptop) with a supported USB to Ethernet adapter to access the iLO web interface, remote console, CLI, iLO RESTful API, or scripts.

When you use the iLO Service Port:

- Actions are logged in the iLO Event Log.
- The server UID blinks to indicate the Service Port status.
  - You can also retrieve the Service Port status by using a REST client and the iLO RESTful API.
- You cannot use the Service Port to boot any device within the server, or the server itself.
- You cannot access the server by connecting to the Service Port.
- You cannot access the connected device from the server.
Configuring the iLO Service Port settings

**Prerequisites**
Configure iLO Settings privilege

**Procedure**

1. Click **Security** in the navigation tree, and then click the **iLO Service Port** tab.
2. Configure the following settings:
   - iLO Service Port
   - USB flash drives
   - Require authentication
   - USB Ethernet adapters
3. Click **Apply**.
   
   The updated settings take effect immediately, and information about the configuration change is logged in the iLO Event Log.

**iLO Service Port options**

- **iLO Service Port**—Allows you to enable or disable the iLO Service Port. The default setting is enabled. When this feature is disabled, you cannot configure the features in the **Mass Storage Options** or **Networking Options** sections on this page.
  
  Do not disable the iLO Service Port when it is in use. If you disable the port when data is being copied, the data might be corrupted.

- **USB flash drives**—Allows you to connect a USB flash drive to the iLO Service Port to download the Active Health System Log. The default setting is enabled.
  
  Do not disable this setting when the iLO Service Port is in use. If you disable USB flash drives when data is being copied, the data might be corrupted.

  If you insert a USB flash drive in the iLO Service Port when this setting is disabled, the device is ignored.

- **Require authentication**—Requires you to enter an iLO user name and password in the **command.txt** file when you use the iLO Service Port to download the Active Health System Log. The default setting is disabled.

  User credentials are not required when the system maintenance switch is set to disable iLO security.

- **USB Ethernet adapters**—Allows you to use a USB to Ethernet adapter to connect a laptop to the iLO Service Port to access the Integrated Remote Console. The default setting is enabled.

  If you connect a laptop when this setting is disabled, the device is ignored.

**iLO Service Port supported devices**

**Mass storage devices**

The iLO Service Port supports USB keys with the following characteristics:
• High-speed USB 2.0 compatibility.
• FAT32 format, preferably with 512 byte blocks.
• One LUN.
• One partition with a maximum size of 127 GB and sufficient free space for the Active Health System Log download.
• Valid FAT32 partition table.
  If the USB key fails to mount, it probably has an invalid partition table. Use a utility such as Microsoft DiskPart to delete and recreate the partition.
• Not read-protected.
• Not bootable.

Mass storage devices are not supported on servers that do not have a NAND.

**USB Ethernet adapters**
The iLO Service Port supports USB Ethernet adapters that contain one of the following chips by ASIX Electronics Corporation:

• AX88772
• AX88772A
• AX88772B
• AX88772C

Hewlett Packard Enterprise recommends the HPE USB to Ethernet Adapter (part number Q7Y55A).

**Configuration security**
When configuring new HPE Gen10 servers for your organization, administrators can use the options described in the following sections to help secure their servers by doing the following:

In iLO:

• Enable or disable IPMI/DCMI over LAN
• Control access to the ILO 5 Configuration Utility
• Verify that a TPM or TM is installed and enabled.
• Configure iLO user and group accounts according to the principle of least privilege
• Control SSH keys
• Administer SSL certificates
• Configure SSO access
• Create and enable a Login Security Banner

In UEFI:
• Set a Power on Password
• Set an Admin Password
• Configure secure boot and advanced secure boot
• Configure HTTPS boot
• Set TPM options
• Enable TXT support (if available)
• Enable the availability of the one-time boot menu prompt during POST
• Enable the availability of the Intelligent Provisioning prompt during POST
• Enable the secure erasure of compatible SATA drives
• Enable UEFI Option ROM measurement

iLO settings for configuration security
Use the settings and controls described in this section to configure the security for iLO.

Preparing to set up iLO
Before setting up an iLO management processor, you must decide how to handle networking and security. The following questions can help you configure iLO:

Procedure

1. How will iLO connect to the network?
2. Will NIC Teaming be used with the Shared Network Port configuration?
3. How will iLO acquire an IP address?
4. What access security is required, and what user accounts and privileges are needed?
5. What tools will you use to configure iLO?

iLO network connection options
Typically, iLO is connected to the network through a dedicated management network or a shared connection on the production network.

Dedicated management network
In this configuration, the iLO port is on a separate network. A separate network improves performance and security because you can physically control which workstations are connected to the network. A separate network also provides redundant access to the server when a hardware failure occurs on the production network. In this configuration, iLO cannot be accessed directly from the production network. The Dedicated management network is the preferred iLO network configuration.
Figure 3: Dedicated management network

**Production network**

In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere on the network and it reduces the amount of networking hardware and infrastructure required to support iLO.

There are some drawbacks to using this configuration.

- With a shared network connection, traffic can hinder iLO performance.
- During the server boot process and when the operating system NIC drivers are loading and unloading, there are brief periods of time (2–8 seconds) when iLO cannot be reached from the network. After these short periods, iLO communication is restored and iLO will respond to network traffic.

When this situation occurs, the Remote Console and connected iLO Virtual Media devices might be disconnected.

Figure 4: Shared network connection

**NIC teaming with Shared Network Port configurations**

NIC teaming is a feature you can use to improve server NIC performance and reliability.

**NIC teaming constraints**

When you select a teaming mode to use when iLO is configured to use the Shared Network Port:

- iLO network communications will be blocked in the following conditions:
The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.

The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Because iLO and the server transmit and receive on the same switch port, the selected NIC teaming mode must allow the switch to tolerate traffic with two different MAC addresses on the same switch port. Some implementations of LACP (802.3ad) will not tolerate multiple MAC addresses on the same link.

Hewlett Packard Enterprise NIC teaming modes

If your server is configured to use Hewlett Packard Enterprise NIC teaming, observe the following guidelines.

Network Fault Tolerance

The server transmits and receives on only one NIC (the primary adapter). The other NICs (secondary adapters) that are part of the team do not transmit server traffic and they ignore received traffic. This mode allows the iLO Shared Network Port to function correctly.

Select the NIC/port iLO uses as the Preferred Primary Adapter.

Transmit Load Balancing

The server transmits on multiple adapters but receives only on the primary adapter. This mode allows the iLO Shared Network Port to function correctly.

Select the NIC/port iLO uses as the Preferred Primary Adapter.

Switch Assisted Load Balancing

This mode type refers to the following:

- HPE ProCurve Port Trunking
- Cisco Fast EtherChannel/Gigabit EtherChannel (Static Mode Only, no PAgP)
- IEEE 802.3ad Link Aggregation (Static Mode only, no LACP)
- Bay Network Multi-Link Trunking
- Extreme Network Load Sharing

In this mode, there is no concept of primary and secondary adapters. All adapters are considered equal for the purposes of sending and receiving data. This mode is the most problematic for iLO Shared Network Port configurations because traffic destined for iLO can be received on only one of the server NIC/ports. To determine the constraints that your switch vendor places on their implementation of switch assisted load balancing, see the switch vendor documentation.

For additional information, see the ProLiant Network Adapter Teaming support document.

For information about selecting a NIC teaming mode when your server uses another implementation of NIC teaming, see NIC teaming constraints and the vendor documentation.

iLO IP address acquisition

To enable iLO access after it is connected to the network, the iLO management processor must acquire an IP address and subnet mask. You can use a dynamic address or a static address.

Dynamic IP address

A dynamic IP address is set by default. iLO obtains the IP address and subnet mask from DNS or DHCP servers. This method is the simplest.
If you use DHCP:

- The iLO management port must be connected to a network that is connected to a DHCP server, and iLO must be on the network before power is applied. DHCP sends a request soon after power is applied. If the DHCP request is not answered when iLO first boots, it will reissue the request at 90-second intervals.
- The DHCP server must be configured to provide DNS and WINS name resolution.

**Static IP address**

If DNS or DHCP servers are not available on the network, a static IP address is used. A static IP address can be configured by using the iLO 5 Configuration Utility.

If you plan to use a static IP address, you must have the IP address before starting the iLO setup process.

**iLO access security**

You can use the following methods to manage access to iLO:

**Local accounts**

- Up to 12 user accounts can be stored in iLO. This configuration is ideal for small environments such as labs and small-sized or medium-sized businesses.
- Login security with local accounts is managed through the iLO Access Settings and user privileges.

**Directory services**

- Up to six directory groups can be configured in iLO. Use a directory service to authenticate and authorize iLO access. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise.
- If you plan to use directory services, consider enabling at least one local administrator account for alternate access.
- A directory provides a central point of administration for iLO devices and users, and the directory can enforce a strong password policy.

**CAC smartcard authentication**

You can configure common access smartcards together with local accounts and directory services to manage iLO user access.

**iLO configuration tools**

iLO supports various interfaces for configuration and operation. This guide discusses the following interfaces:

**iLO web interface**

- Use the iLO web interface when you can connect to iLO on the network by using a web browser. You can also use this method to reconfigure an iLO management processor.

**ROM-based setup**

- Use the iLO 5 Configuration Utility when the system environment does not use DHCP, DNS, or WINS.

**Other iLO configuration tools**

iLO configuration options not discussed in this guide follow:

**Intelligent Provisioning**

- To start Intelligent Provisioning, press F10 during POST.
- You can also access Always On Intelligent Provisioning through the iLO web interface. For more information, see the Intelligent Provisioning user guide.
iLO RESTful API

A management interface that server management tools can use to perform configuration, inventory, and monitoring of a supported server through iLO. For more information, see the following website: http://www.hpe.com/info/redfish.

HPE OneView

A management tool that interacts with the iLO management processor to configure, monitor, and manage ProLiant servers or Synergy compute modules. For more information, see the HPE OneView user guide.

HPE Scripting Toolkit

This toolkit is a server deployment product for IT experts that provides unattended automated installation for high-volume server deployments. For more information, see the Scripting Toolkit user guide for Windows or Linux.

Scripting

You can use scripting to set up multiple iLO management processors. Scripts are XML files written for a scripting language called RIBCL. You can use RIBCL scripts to configure iLO on the network during initial deployment or from a deployed host.

The following methods are available:

- **HPQLOCFG**—A Windows command-line utility that sends RIBCL scripts over the network to iLO.
- **HPONCFG**—A local online scripted setup utility that runs on the host and passes RIBCL scripts to the local iLO.
  
  When iLO is configured to use the CNSA security state, only HPONCFG for Linux is supported.

- **Custom scripting environments (LOCFG.PL)**—The iLO scripting samples include a Perl sample that can be used to send RIBCL scripts to iLO over the network.
- **SMASH CLP**—A command-line protocol that can be used when a command line is accessible through SSH or the physical serial port.

For more information about these methods, see the iLO scripting and command-line guide.

iLO sample scripts are available at the following website: http://www.hpe.com/support/ilo5.

IPMI/DCMI settings

iLO supports IPMI 2.0 and DCMI industry standard protocols. IPMI is an industry standard protocol, developed by Intel and supported by over two hundred vendors, such as Hewlett Packard Enterprise, IBM, Dell, Cisco, NEC, Fujitsu-Siemens, and Supermicro. For more information on IPMI, visit Intel’s website at http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-home.html

The Data Center Management Interface (DCMI) uses the same interfaces defined by IPMI, but fewer optional interfaces. The DCMI 1.0 specification identifies the core set of mandatory capabilities and interfaces that data centers require, and includes a subset of extensions added to IPMI 2.0 to further increase the capabilities of DCMI in the data center. DCMI differs from IPMI in that DCMI was specifically designed for the manageability needs of data centers.

iLO enables you to send industry-standard IPMI and DCMI commands over the LAN. The IPMI/DCMI port is set to 623 by default but is configurable. To enable or disable IPMI/DCMI over the LAN, use the control associated with **IPMI/DCMI over LAN** on the **Security > Access Settings** page of the iLO interface. The setting allows you to send IPMI/DCMI commands over the LAN by using a client-side application. When this setting is disabled, however, server-side IPMI/DCMI applications are still functional.

When using IPMI or DCMI over LAN, the following guidelines are suggested:
• Segment IPMI/DCMI traffic from the rest of the network. If using a shared NIC connection, a VLAN for iLO can be used to accomplish this separation. Isolate the IPMI/Management subnet using a firewall and limit access to authorized administrators.

• Do not allow IPMI/DCMI traffic from outside the network.

• iLO supports IPMI 2.0 which uses stronger encryption than IPMI 1.5. Hewlett Packard Enterprise recommends cipher suites 3 and 17.

Resolved vulnerabilities


Hewlett Packard Enterprise addressed the vulnerabilities as follows:

• Cipher 0 is an option that allows authentication to be bypassed. iLO addressed this by not allowing cipher 0 to be selected by an IPMI client.

• In the IPMI specification, user ID 1 is used to support anonymous logins. iLO does not support anonymous logins using user ID 1.

• In the IPMI specification, disabled user ID’s are configured with usernames and passwords. Often, this is preconfigured in manufacturing to well-known user ID’s and passwords. iLO does not retain disabled user ID usernames and passwords. iLO has one username preconfigured with a unique password in manufacturing. Hewlett Packard Enterprise suggests that the customer reconfigure this default user immediately.

• While the IPMI specification allows for NULL passwords, iLO does not support the setting of a user password to NULL.

• The IPMI specification requires support for RAKP authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks. As this is part of the IPMI protocol itself, Hewlett Packard Enterprise recommends that IPMI over LAN be disabled if not in use or that the IPMI management subnet be isolated.

Viewing customer advisories, bulletins, and notices

Procedure


2. On the left side of the page, under Knowledge base options, click one of the following:
   • Top issues
   • Advisories, bulletins & notices

   The chosen information appears in tabular format.

iLO security

To access the security features that you can configure with the iLO web interface, click Security in the navigation tree.

For in-depth information about iLO security, see the HPE Gen10 Security Reference Guide.
General security guidelines

When you set up and use iLO, consider the following guidelines for maximizing security:

• Configure iLO on a separate management network.
• Do not connect iLO directly to the Internet.
• Install an SSL certificate.
• Change the password for the default user account.
• Use an authentication service (for example, Active Directory or OpenLDAP), preferably with two-factor authentication.
• Disable protocols that you do not use (for example, SNMP or IPMI over LAN).
• Disable features that you do not use (for example, Remote Console or Virtual Media).
• Use HTTPS for the Integrated Remote Console.

To configure this option, enable the **IRC requires a trusted certificate in iLO** setting on the **Remote Console & Media** page **Security** tab.

Key security features

Configure iLO security features on the following web interface pages.

**Access Settings**

• Enable or disable iLO interfaces and features.
• Customize the TCP/IP ports iLO uses.
• Configure authentication failure logging and delays.
• Secure the iLO 5 Configuration Utility.

**iLO Service Port**

Configure iLO Service Port availability, authentication, and supported devices.

**Secure Shell Key**

To provide stronger security, add SSH keys to iLO user accounts.

**Certificate Mappings and CAC Smartcard**

Configure CAC Smartcard authentication and configure smartcard certificates for local users.

**SSL Certificate**

Install X.509 CA signed certificates to enable encrypted communications.

**Directory**

Configure Kerberos authentication and Directory integration.

You can configure iLO to use a directory service to authenticate and authorize its users. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise. The directory also provides a central point of administration for iLO devices and users, and the directory can enforce a strong password policy.

---

**HPE Gen10 security best practices**

43
Encryption
Implement a higher security environment by changing the iLO security state from the default Production level to a stronger setting.

HPE SSO
Configure supported tools for single-sign-on with iLO.

Login Security Banner
Add a security notice to the iLO login page.

TPM and TM
Trusted Platform Modules and Trusted Modules are computer chips that securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM or TM to store platform measurements to make sure that the platform remains trustworthy.

On a supported system, ROM decodes the TPM or TM record and passes the configuration status to iLO, the iLO RESTful API, the CLP, and the XML interface.

Viewing the TPM or TM status

Procedure
Click Information in the navigation tree.

TPM or TM status values

- Not Supported—A TPM or TM is not supported.
- Not Present—A TPM or TM is not installed.
- Present-Enabled—A TPM or TM is installed and enabled.

iLO user accounts
iLO enables you to manage user accounts stored locally in secure memory.

You can create up to 12 local user accounts with custom login names and advanced password encryption. Privileges control individual user settings, and can be customized to meet user access requirements.

If a supported application that works with iLO requires a service account, you can add a user account and designate it as a service account. You can also add service accounts by using a supported application or the RESTful API.

You can use directories to support more than 12 user accounts. iLO supports up to six directory groups.

Adding local user accounts

Prerequisites
Administer User Accounts privilege

Procedure

1. Click Administration in the navigation tree.
   The User Administration tab is displayed.
2. Click New.
3. Enter the following details:
• Login Name
• User Name
• New Password and Confirm Password

4. Select from the following privileges:

• Login
• Remote Console
• Virtual Power and Reset
• Virtual Media
• Host BIOS
• Configure iLO Settings
• Administer User Accounts
• Host NIC
• Host Storage
• Recovery Set

To select all available user privileges, click the select all check box.

5. Optional: Select the Service Account check box if the account will be used as a service account for a supported application.

   Examples of supported applications include iLO Amplifier Pack and Onboard Administrator.

6. To save the new user, click Add User.

Editing local user accounts

Prerequisites
Administer User Accounts privilege

Procedure

1. Click Administration in the navigation tree.
   The User Administration tab is displayed.

2. Select a user, and then click Edit.

3. Update the following values on the Add/Edit Local User page, as needed:

   • Login Name
   • User Name

4. To change the password, click the Change password check box, and then update the New Password and Confirm Password values.

5. Select from the following privileges:
To select all available user privileges, click the **select all** check box.

To save the user account changes, click **Update User**.

### Deleting a user account

**Prerequisites**

Administer User Accounts privilege

**Procedure**

1. Click **Administration** in the navigation tree. The **User Administration** tab is displayed.
2. Select the check box next to one or more user accounts that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the request, click **Yes, delete**.

### iLO user account options

- **User Name** appears in the user list on the **User Administration** page. It does not have to be the same as the **Login Name**. The maximum length for a user name is 39 characters. The **User Name** must use printable characters. Assigning descriptive user names can help you to identify the owner of each login name.

- **Login Name** is the name you use when logging in to iLO. It appears in the user list on the **User Administration** page, on the **Session List** page, in the menu that is displayed when you click the user icon, and in logs. The **Login Name** does not have to be the same as the **User Name**. The maximum length for a login name is 39 characters. The login name must use printable characters.

- **Password** and **Password Confirm** set and confirm the password that is used for logging in to iLO.

- **Service Account** —Designates the account as a service account. Service accounts are used by supported products that work with iLO. Examples of supported applications include iLO Amplifier Pack and Onboard Administrator.
iLO user privileges

The following privileges apply to user accounts:

- **Login**—Enables a user to log in to iLO.
- **Remote Console**—Enables a user to access the host system Remote Console, including video, keyboard, and mouse control.
  Users with this privilege can access the BIOS, and therefore might be able to perform host-based BIOS, iLO, storage, and network configuration tasks.
- **Virtual Power and Reset**—Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the Generate NMI to System button.
- **Virtual Media**—Enables a user to use the Virtual Media feature on the host system.
- **Host BIOS**—Enables a user to configure the host BIOS settings by using the UEFI System Utilities.
- **Configure iLO Settings**—Enables a user to configure most iLO settings, including security settings, and to update the iLO firmware. This privilege does not enable local user account administration.
  After iLO is configured, revoking this privilege from all users prevents reconfiguration with the web interface, iLO RESTful API, HPQLOCFG, or the CLI. Users who have access to the UEFI System Utilities or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
- **Administer User Accounts**—Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you do not have this privilege, you can view your own settings and change your own password.
- **Host NIC**—Enables a user to configure the host NIC settings.
- **Host Storage**—Enables a user to configure the host storage settings.
- **Recovery Set**—Enables a user to manage the recovery install set.
  By default, this privilege is assigned to the default Administrator account. To assign this privilege to another account, log in with an account that already has this privilege.
  This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

The following privileges are not available through the CLI or RIBCL scripts: Host NIC, Host Storage, Recovery Set, Host BIOS, and Login.

The following privileges are not available through the UEFI System Utilities iLO 5 Configuration Utility: Login and Recovery Set.

The Host BIOS, Host NIC, and Host Storage privileges do not affect configuration through host-based utilities.

Password guidelines

Hewlett Packard Enterprise recommends that you follow these password guidelines when you create and edit user accounts.

- When working with passwords:
Do not write down or record passwords.

Do not share passwords with others.

Do not use passwords that are made up of words found in a dictionary.

Do not use passwords that contain obvious words, such as the company name, product name, user name, or login name.

- Use passwords with at least three of the following characteristics:
  - One numeric character
  - One special character
  - One lowercase character
  - One uppercase character

- The minimum length for an iLO user account password is set on the Access Settings page. Depending on the configured Minimum Password Length value, the password can have a minimum of zero characters (no password) and a maximum of 39 characters. The default Minimum Password Length is eight characters.

**IMPORTANT:**
Hewlett Packard Enterprise does not recommend setting the Minimum Password Length to fewer than eight characters unless you have a physically secure management network that does not extend outside the secure data center.

**IPMI/DCMI users**

The iLO firmware follows the IPMI 2.0 specification. When you add IPMI/DCMI users, the login name must be a maximum of 16 characters, and the password must be a maximum of 20 characters.

When you select iLO user privileges, the equivalent IPMI/DCMI user privilege is displayed in the IPMI/DCMI Privilege based on above settings box.

- **User**—A user has read-only access. A user cannot configure or write to iLO, or perform system actions.
  - For IPMI User privileges: Disable all privileges. Any combination of privileges that does not meet the Operator level is an IPMI User.

- **Operator**—An operator can perform system actions, but cannot configure iLO or manage user accounts.
  - For IPMI Operator privileges: Enable Remote Console Access, Virtual Power and Reset, and Virtual Media. Any combination of privileges greater than Operator that does not meet the Administrator level is an IPMI Operator.

- **Administrator**—An administrator has read and write access to all features.
  - For IPMI Administrator privileges: Enable all privileges.

**Viewing user accounts**

**Procedure**

1. Click Administration in the navigation tree.
The User Administration page is displayed.

The Local Users table shows the login names, user names, and assigned privileges of each local user.

If service accounts are configured, the Service table shows the login names, user names, and assigned privileges of each service account. If no service accounts exist, this table is not displayed.

2. Optional: To view a privilege name, move the cursor over a privilege icon.

iLO directory groups

iLO enables you to manage directory group accounts. Use MMC or ConsoleOne to manage directory-based user accounts.

Adding directory groups

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: http://www.hpe.com/support/ilo-docs.

Procedure

1. Click Administration in the navigation tree, and then click the Directory Groups tab.
2. Click New.
3. Provide the following details in the Group Information section:
   - Group DN
   - Group SID (Kerberos authentication and Active Directory integration only)
4. Select from the following privileges:
   - Login
   - Remote Console
   - Virtual Power and Reset
   - Virtual Media
   - Host BIOS
   - Configure iLO Settings
   - Administer User Accounts
   - Host NIC
   - Host Storage
   - Recovery Set
5. To save the new directory group, click Add Group.
Editing directory groups

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).

Procedure

1. Click **Administration** in the navigation tree, and then click the **Directory Groups** tab.
2. Select a group in the **Directory Groups** section, and then click **Edit**.
3. Provide the following details in the **Group Information** section:
   - **Group DN**
   - **Group SID** (Kerberos authentication and Active Directory integration only)
4. Select from the following privileges:
   - **Login**
   - **Remote Console**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Host BIOS**
   - **Configure iLO Settings**
   - **Administer User Accounts**
   - **Host NIC**
   - **Host Storage**
   - **Recovery Set**
5. To save the directory group changes, click **Update Group**.

Deleting a directory group

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).
Procedure

1. Click Administration in the navigation tree, and then click the Directory Groups tab.
2. Select the check box next to the directory group that you want to delete.
3. Click Delete.
4. When prompted to confirm the request, click Yes, delete.
   iLO notifies you that the group was deleted.

Directory group options

Each directory group includes a DN, SID, and account privileges. For Kerberos login, the SIDs of groups are compared to the SIDs for directory groups configured for iLO. If a user is a member of multiple groups, the user account is granted the privileges of all the groups.

You can use global and universal groups to set privileges. Domain local groups are not supported.

When you add a directory group to iLO, configure the following values:

- **Group DN** (Security Group DN)—Members of this group are granted the privileges set for the group. The specified group must exist in the directory, and users who need access to iLO must be members of this group. Enter a DN from the directory (for example, CN=Group1, OU=Managed Groups, DC=domain, DC=extension).
  Shortened DNs are also supported (for example, Group1). The shortened DN is not a unique match. Hewlett Packard Enterprise recommends using the fully qualified DN.

- **Group SID** (Security ID)—Microsoft Security ID is used for Kerberos and directory group authorization. This value is required for Kerberos authentication. The required format is S-1-5-2039349.

Directory group privileges

The following privileges apply to directory groups:

- **Login**—Enables directory users to log in to iLO.
- **Remote Console**—Enables directory users to access the host system Remote Console, including video, keyboard, and mouse control.
  Users with this privilege can access the BIOS, and therefore might be able to perform host-based BIOS, iLO, storage, and network configuration tasks.
- **Virtual Power and Reset**—Enables directory users to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the Generate NMI to System button.
- **Virtual Media**—Enables directory users to use the Virtual Media feature on the host system.
- **Host BIOS**—Enables directory users to configure the host BIOS settings by using the UEFI System Utilities.
- **Configure iLO Settings**—Enables directory users to configure most iLO settings, including security settings, and to update the iLO firmware. This privilege does not enable local user account administration.
  After iLO is configured, revoking this privilege from all users prevents reconfiguration with the iLO web interface, iLO RESTful API, HPQLOCFG, or the CLI. Users who have access to the UEFI System Utilities
or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.

- **Administer User Accounts**—Enables directory users to add, edit, and delete local iLO user accounts.
- **Host NIC**—Enables directory users to configure the host NIC settings.
- **Host Storage**—Enables directory users to configure the host storage settings.
- **Recovery Set**—Enables directory users to manage the critical recovery install set.

By default, this privilege is assigned to the default Administrator account. To assign this privilege to another account, log in with an account that already has this privilege.

This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

The Host BIOS, Host NIC, and Host Storage privileges do not affect configuration through host-based utilities.

### Viewing directory groups

**Procedure**

1. Click **Administration** in the navigation tree, and then click the **Directory Groups** tab.
   
   The **Directory Groups** table shows the group DN, group SID, and the assigned privileges for the configured groups.

2. Optional: To view a privilege name, move the cursor over a privilege icon.

### Administering SSH keys

The **Secure Shell Key** page displays the hash of the SSH public key associated with each user. Each user can have only one key assigned. Use this page to view, add, or delete SSH keys.

### Authorizing a new SSH key by using the web interface

**Prerequisites**

Administer User Accounts privilege

**Procedure**

1. Generate a 2,048-bit DSA or RSA key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.
   
   ECDSA 384-bit keys that use the NIST P-384 curve are required when iLO is configured to use the CNSA security state.

2. Create the `key.pub` file.

3. Click **Security** in the navigation tree, and then click the **Secure Shell Key** tab.

4. Select the check box to the left of the user to which you want to add an SSH key.

5. Click **Authorize New Key**.

6. Copy and paste the public key into the **Public Key Import Data** box.
The key must be a 2,048-bit DSA or RSA key.

7. Click Import Public Key.

Authorizing a new SSH key by using the CLI

Prerequisites
Administer User Accounts privilege

Procedure

1. Generate a 2,048-bit DSA or RSA SSH key by using ssh-keygen, puttygen.exe, or another SSH key utility.
   ECDSA 384-bit keys that use the NIST P-384 curve are required when iLO is configured to use the CNSA security state.

2. Create the key.pub file.

3. Verify that Secure Shell (SSH) Access is enabled on the Access Settings page.

4. Use Putty.exe to open an SSH session using port 22.

5. Change to the cd /Map1/Config1 directory.

6. Enter the following command:
   
   ```
   load sshkey type "oemhpe_loadSSHkey -source <protocol://username:password@hostname:port/filename>"
   ```

   When you use this command:
   
   • The protocol value is required and must be HTTP or HTTPS.
   • The hostname and filename values are required.
   • The username:password and port values are optional.
   • oemhpe_loadSSHkey is case-sensitive.

   The CLI performs a cursory syntax verification of the values you enter. Visually verify that the URL is valid.
   The following example shows the command structure:

   ```
   oemhpe_loadSSHkey -source http://192.168.1.1/images/path/sshkey.pub
   ```

Deleting SSH keys

Use the following procedure to delete SSH keys from one or more user accounts.

When an SSH key is deleted from iLO, an SSH client cannot authenticate to iLO by using the corresponding private key.

Prerequisites
Administer User Accounts privilege
Procedure

1. Click Security in the navigation tree, and then click the Secure Shell Key tab.
2. In the Authorized SSH Keys list, select the check box to the left of one or more user accounts.
3. Click Delete Selected Key(s).
   The selected SSH keys are removed from iLO.

Requirements for authorizing SSH keys from an HPE SIM server

The mxagentconfig utility enables you to authorize SSH keys from an HPE SIM server.

- SSH must be enabled on iLO before you use mxagentconfig to authorize a key.
- The user name and password entered in mxagentconfig must correspond to an iLO user who has the Configure iLO Settings privilege. The user can be a directory user or a local user.
- The key is authorized on iLO and corresponds to the user name specified in the mxagentconfig command.

For more information about mxagentconfig, see the iLO scripting and CLI guide.

SSH keys

When you add an SSH key to iLO, you paste the SSH key file into iLO. The file must contain the user-generated public key. The iLO firmware associates each key with the selected local user account. If a user is removed after an SSH key is authorized for that user, the SSH key is removed.

Supported SSH key formats

- RFC 4716
- OpenSSH key format
- iLO legacy format

Working with SSH keys

- The supported SSH key formats are supported with the iLO web interface and the CLI.
- Only the iLO legacy format is supported with RIBCL scripts.
- Any SSH connection authenticated through the corresponding private key is authenticated as the owner of the key and has the same privileges.
- The iLO firmware can import SSH keys that have a length of 1,366 bytes or less. If the key is larger than 1,366 bytes, the authorization might fail. If a failure occurs, use the SSH client software to generate a shorter key.
- If you use the iLO web interface to enter the public key, you select the user associated with the public key.
- If you use the iLO RESTful API to enter the public key, the user name is provided with the public key in the POST body.
• If you use the CLI to enter the public key, the public key is linked to the user name that you entered to log in to iLO.
• If you use HPQLOCFG and a RIBCL script to enter the public key, you append the iLO user name to the public key data. The public key is stored with that user name.

Administering SSL certificates

SSL protocol is a standard for encrypting data so that it cannot be viewed or modified while in transit on the network. An SSL certificate is a small computer file that digitally combines a cryptographic key (the server public key) with the server name. Only the server itself has the corresponding private key, allowing for authenticated two-way communication between a user and the server.

A certificate must be signed to be valid. If it is signed by a Certificate Authority (CA), and that CA is trusted, all certificates signed by the CA are also trusted. A self-signed certificate is one in which the owner of the certificate acts as its own CA.

By default, iLO creates a self-signed certificate for use in SSL connections. This certificate enables iLO to work without additional configuration steps.

**IMPORTANT:**
Using a self-signed certificate is less secure than importing a trusted certificate. Hewlett Packard Enterprise recommends importing a trusted certificate to protect the iLO user credentials.

Viewing SSL certificate information

Procedure

To view certificate information, click Security in the navigation tree, and then click the SSL Certificate tab.

SSL certificate details

• **Issued To**—The entity to which the certificate was issued.
• **Issued By**—The CA that issued the certificate.
• **Valid From**—The first date that the certificate is valid.
• **Valid Until**—The date that the certificate expires.
• **Serial Number**—The serial number that the CA assigned to the certificate.

Obtaining and importing an SSL certificate

iLO allows you to create a Certificate Signing Request that you can send to a Certificate Authority to obtain a trusted SSL certificate to import into iLO.

An SSL certificate works only with the keys generated with its corresponding CSR. If iLO is reset to the factory default settings, or another CSR is generated before the certificate that corresponds to the previous CSR is imported, the certificate does not work. In that case, a new CSR must be generated and used to obtain a new certificate from a CA.

**Prerequisites**
Configure iLO Settings privilege
Procedure

1. **Obtain a trusted certificate from a Certificate Authority (CA).**
2. **Import the trusted certificate into iLO.**

**Obtaining a trusted certificate from a CA**

**Prerequisites**
Configure iLO Settings privilege

**Procedure**

1. Click **Security** in the navigation tree, and then click the **SSL Certificate** tab.
2. Click **Customize Certificate**.
3. On the **SSL Certificate Customization** page, enter the following:
   - Country (C)
   - State (ST)
   - City or Locality (L)
   - Organization Name (O)
   - Organizational Unit (OU)
   - Common Name (CN)
4. If you want the iLO IP addresses included in the CSR, select the **include iLO IP Address(es)** check box. This option is disabled by default because some CAs cannot accept this input.
   
   When this option is enabled, the iLO IP addresses will be included in the CSR Subject Alternative Name (SAN) extension.
5. Click **Generate CSR**.
   
   A message notifies you that a CSR is being generated and that the process might take up to 10 minutes.
6. After a few minutes (up to 10), click **Generate CSR** again.
   
   The CSR is displayed.
   
   The CSR contains a public and private key pair that validates communications between the client browser and iLO. Key sizes up to 2,048 bits are supported. The generated CSR is held in memory until a new CSR is generated, iLO is reset to the factory default settings, or a certificate is imported.
7. Select and copy the CSR text.
8. Open a browser window and navigate to a third-party CA.
9. Follow the onscreen instructions and submit the CSR to the CA.
   
   When you submit the CSR to the CA, your environment might require the specification of Subject Alternative Names. If necessary, enter the iLO DNS name.
   
   The CA generates a certificate.
10. After you obtain the certificate, make sure that:
• The CN matches the iLO FQDN. This value is listed as the **iLO Hostname** on the **Overview** page.

• The certificate is a Base64-encoded X.509 certificate.

• The first and last lines are included in the certificate.

**CSR input details**

Enter the following details when you create a CSR:

• **Country (C)**—The two-character country code that identifies the country where the company or organization that owns this iLO subsystem is located. Enter the two-letter abbreviation in capital letters.

• **State (ST)**—The state where the company or organization that owns this iLO subsystem is located.

• **City or Locality (L)**—The city or locality where the company or organization that owns this iLO subsystem is located.

• **Organization Name (O)**—The name of the company or organization that owns this iLO subsystem.

• **Organizational Unit (OU)**—(Optional) The unit within the company or organization that owns this iLO subsystem.

• **Common Name (CN)**—The FQDN of this iLO subsystem.

  The FQDN is entered automatically in the **Common Name (CN)** box.

  To enable iLO to enter the FQDN into the CSR, configure the **Domain Name** on the **Network General Settings** page.

• **include iLO IP Address(es)**—Select this check box to include the iLO IP addresses in the CSR. This option is disabled by default because some CAs cannot accept this input.

**Importing a trusted certificate**

**Prerequisites**

Configure iLO Settings privilege

**Procedure**

1. Click **Security** in the navigation tree, and then click the **SSL Certificate** tab.

2. Click **Customize Certificate**.

3. Click **Import Certificate**.

4. In the **Import Certificate** window, paste the certificate into the text box, and then click **Import**.

   iLO supports SSL certificates that are up to 3 KB (including the 609 bytes or 1,187 bytes used by the private key, for 1,024-bit and 2,048-bit certificates, respectively).

5. Reset iLO.

**HPE SSO**

HPE SSO enables you to browse directly from an HPE SSO-compliant application to iLO, bypassing an intermediate login step.

To use this feature:
• You must have a supported version of an HPE SSO-compliant application.
• Configure iLO to trust the SSO-compliant application.
• Install a trusted certificate if CAC Strict Mode is enabled.

iLO contains support for HPE SSO applications to determine the minimum HPE SSO certificate requirements. Some HPE SSO-compliant applications automatically import trust certificates when they connect to iLO. For applications that do not perform this function automatically, use the HPE SSO page to configure the SSO settings.

Configuring iLO for HPE SSO

Prerequisites
Configure iLO Settings privilege

Procedure

1. Click Security in the navigation tree, and then click the HPE SSO tab.
2. Configure the SSO Trust Mode setting.
   Hewlett Packard Enterprise recommends using the Trust by Certificate mode.
3. Configure iLO privileges for each role in the Single Sign-On Settings section.
4. To save the SSO settings, click Apply.
5. If you selected Trust by Certificate or Trust by Name, add the trusted certificate or DNS name to iLO.
   For instructions, see Adding trusted certificates on page 59 or Importing a direct DNS name on page 60.
6. After you configure SSO in iLO, log in to an HPE SSO-compliant application and browse to iLO.
   For example, log in to HPE SIM, navigate to the System page for the iLO processor, and then click the iLO link in the More Information section.

   Although a system might be registered as a trusted server, SSO might be refused because of the current trust mode or certificate status. For example, SSO would be refused when:

   • A server is registered as a trusted server, a certificate is not imported, and the trust mode is set to Trust by Certificate.
   • A server certificate is imported but the certificate has expired.
   • The installed certificate does not meet the iLO security requirements.
     - When the HighSecurity or FIPS security state is enabled, a 2048-bit certificate is required.
     - When the CNSA security state is enabled, a certificate containing a 3072-bit RSA key or a 384-bit ECDSA key with NIST P-384 curve is required.

The list of trusted servers is not used when SSO is disabled. iLO does not enforce SSO server certificate revocation.

Single Sign-On Trust Mode options

   The Single Sign-On Trust Mode affects how iLO responds to HPE SSO requests.
• **Trust None (SSO disabled)** (default)—Rejects all SSO connection requests.

• **Trust by Certificate** (most secure)—Enables SSO connections from an HPE SSO-compliant application by matching a certificate previously imported to iLO.

• **Trust by Name**—Enables SSO connections from an HPE SSO-compliant application by matching a directly imported IP address or DNS name.

• **Trust All** (least secure)—Accepts any SSO connection initiated from any HPE SSO-compliant application.

### SSO user privileges

When you log in to an HPE SSO-compliant application, you are authorized based on your HPE SSO-compliant application role assignment. The role assignment is passed to iLO when SSO is attempted.

SSO attempts to receive only the privileges assigned in the **Single Sign-On Settings** section. iLO directory settings do not apply.

The default privilege settings follow:

- **User**—Login only
- **Operator**—Login, Remote Console, Virtual Power and Reset, Virtual Media, Host BIOS.
- **Administrator**—Login, Remote Console, Virtual Power and Reset, Virtual Media, Host BIOS, Configure iLO Settings, Administer User Accounts, Host NIC, and Host Storage.

### Adding trusted certificates

The certificate repository can hold five typical certificates. However, if typical certificates are not issued, certificate sizes might vary. When all allocated storage is used, no more imports are accepted.

For information about how to extract a certificate from an HPE SSO-compliant application, see your HPE SSO-compliant application documentation.

#### Prerequisites

Configure iLO Settings privilege

#### Procedure

1. Click **Security** in the navigation tree, and then click the **HPE SSO** tab.

2. Click **Import**.

3. Use one of the following methods to add a trusted certificate:

   - **Direct import**—Copy the Base64-encoded certificate X.509 data, paste it into the text box in the **Direct Import** section, and then click **Apply**.

   - **Indirect import**—Type the DNS name or IP address in the text box in the **Import From URL** section, and then click **Apply**.

     iLO contacts the HPE SSO-compliant application over the network, retrieves the certificate, and then saves it.

---

HPE Gen10 security best practices  59
Importing a direct DNS name

**Prerequisites**
Configure iLO Settings privilege

**Procedure**

1. Click **Security** in the navigation tree, and then click the **HPE SSO** tab.
2. Click **Import**
3. Enter the DNS name or IP address in the **Import Direct DNS Name** section, and then click **Apply**.

Viewing trusted certificates and records

The **Manage Trusted Certificates and Records** table displays the status of the trusted certificates and records configured to use SSO with the current iLO management processor.

**Procedure**

Click **Security** in the navigation tree, and then click the **HPE SSO** tab.

**Trusted certificate and record details**

**Status**

The status of the certificate or record. The possible status values follow:

- ✅ The certificate or record is valid.
- ⚠️ There is a problem with the certificate or record. Possible reasons follow:
  - The record contains a DNS name, and the trust mode is set to **Trust by Certificate** (only certificates are valid).
  - A certificate is configured, and the trust mode is set to **Trust by Name** (only directly imported IP addresses or DNS names are valid).
  - **Trust None (SSO disabled)** is selected.
  - The certificate is not compliant with the configured iLO security state.

- 🔴 The certificate or record is not valid. Possible reasons follow:
  - The certificate is out-of-date. Check the certificate details for more information.
  - The iLO clock is not set or is set incorrectly. The iLO clock must be in the certificate **Valid from** and **Valid until** range.

**Certificate**

Indicates that the record contains a stored certificate. Move the cursor over the icon to view the certificate details, including subject, issuer, and dates.

**Description**

The server name or certificate subject.
Removing trusted certificates and records

**Prerequisites**
Configure iLO Settings privilege

**Procedure**

1. Click Security in the navigation tree, and then click the HPE SSO tab.
2. Select one or more trusted certificates or records in the Manage Trusted Certificates and Records table.
3. Click Delete.
   - iLO prompts you to confirm that you want to delete the selected certificates or records.
   - If you delete the certificate of a remote management system, you might experience impaired functionality when using the remote management system with iLO.
4. Click Yes.

Configuring the Login Security Banner

The Login Security Banner feature allows you to configure the security banner displayed on the iLO login page. For example, you could enter a message with contact information for the owner of the server.

**Prerequisites**
Configure iLO Settings privilege

**Procedure**

1. Click Security in the navigation tree, and then click Login Security Banner.
2. Enable the Enable Login Security Banner setting.
   - iLO uses the following default text for the Login Security Banner:
     
     This is a private system. It is to be used solely by authorized users and may be monitored for all lawful purposes. By accessing this system, you are consenting to such monitoring.

3. Optional: To customize the security message, enter a custom message in the Security Message text box.
   - The byte counter above the text box indicates the remaining number of bytes allowed for the message. The maximum is 1,500 bytes.
   
   Tip: To restore the default text, click Use Default Message.

4. Click Apply.
   - The security message is displayed at the next login.

Installing a license key by using a browser

**Prerequisites**
Configure iLO Settings privilege
Procedure

1. Click Administration in the navigation tree, and then click the Licensing tab.

2. Enter a license key in the Activation Key box.

   To move between segments, press the Tab key or click inside a segment of the Activation Key box. The cursor advances automatically when you enter data into the segments of the Activation Key box.

3. Click Install.

   iLO prompts you to confirm that you have read and accept the EULA.

   The EULA details are available in the License Pack option kit.

4. Click I agree.

   The license key is now enabled.

Viewing license information

Procedure

Click Administration in the navigation tree, and then click the Licensing tab.

License details

- **License**—The license name
- **Status**—The license status
- **Activation Key**—The installed key

Lost license key recovery

If an iLO license key is lost, send a replacement request and your proof of purchase to one of the following email addresses:

- Americas: licensing.ams@hpe.com
- Europe, Middle East, and Africa: licensing.emea@hpe.com
- Asia-Pacific and Japan: licensing.apj@hpe.com

iLO licensing

iLO standard features are included with every server to simplify server setup, perform health monitoring, monitor power and thermal control, and facilitate remote administration.

iLO licenses activate functionality such as graphical Remote Console with multiuser collaboration, video record/playback, and many more features.

**Why register your iLO licenses?**

- Registration activates a unique HPE Support Agreement ID (SAID). Your SAID identifies you and the products you use.
- You can obtain quicker HPE Support Services by using your SAID.
- Obtain access to the HPE Support Center.
- Obtain access to software updates in the HPE Update Center.
• Receive important product alerts.
• Track your HPE product license keys in one place through the HPE licensing portal.

How do I register my iLO licenses?

1. Locate the Entitlement Order Number (EON) on your License Entitlement Certificate or Licensing Confirmation Email.
2. Enter the EON in the HPE Licensing Portal.

License key information

• For information about obtaining a free iLO trial license or purchasing, registering, and redeeming a license key, see the iLO licensing guide at the following website: http://www.hpe.com/support/ilo-docs.
• One iLO license is required for each server on which the product is installed and used. Licenses are not transferable.
• You cannot license a server with a license key that is meant for a different server type.
• An iLO Advanced license is automatically included with Synergy compute modules.
• If you lose a license key, follow the lost license key instructions.

UEFI settings for configuration security

Use the settings and controls described in this section to configure the security for UEFI.

HPE Gen10 UEFI security features

Use the following UEFI features on the System Configuration > BIOS/Platform Configuration (RBSU) > Server Security page to configure UEFI security:

• Set Power On Password
  When the server powers on, a password prompt displays. Enter a valid password to continue the boot process. In the event of an ASR reboot, this password is bypassed, and the server boots normally.

• Set Admin Password
  This option sets a password that protects the server configuration. When this option is enabled, you are prompted for this password before being allowed to modify the configuration.

• Secure Boot Settings
  When booting into a UEFI-compliant operating system, secure boot checks for securely signed modules loading the BIOS. Secure boot is different than Secure Start in that it checks firmware beyond the iLO and BIOS firmware, including third party modules that may be present, and drivers that are not part of the BIOS. Additionally, secure boot checks modules that load after the computer starts, such as the Windows boot loader.
  Before configuring Secure Boot, ensure that you selected UEFI mode as the boot type, and that the UEFI Optimized Boot option is enabled (under the Boot Mode menu).

• Advanced Secure Boot (including PK, KEK, DB/DBX options)
  Use the options available for this feature to add or remove certificates in the Secure Boot databases.
• **TLS (HTTPS) Options**

This feature refers to the use of HTTP boot over a TLS session. This type of booting allows you to enter a specific HTTPS URI from which to boot a server. This gives an alternative, more secure alternative to PXE booting.

Further Advanced Security Settings are available with this feature, which include options to choose the Cipher suite, the type of certificate validation for every TLS connection, strict hostname checking, and version of the TLS protocol to be supported.

• **Trusted Platform Module Options**

Trusted Platform Modules enable the firmware and OS to take measurements of all phases of the boot process. HPE Gen10 UEFI allows the selection of either TPM 2.0 or TPM 1.2 compliance. TPM 2.0 has several advantages over TPM 1.2, including a flexible algorithm, enhanced authorization, simplified provisioning, and internally protected assets using symmetric algorithms.

The options for this feature include Chipset-TPM (which, when enabled, makes the system TPM 2.0 compliant), and the Current TPM Type and Current TPM State.

• **Intel TXT Support**

Enable or disable Intel TXT support with this option. Intel TXT uses a TPM and cryptographic techniques to measure software and platform components to prevent malfunctioning or compromised components from running, and protects from software-based attacks that would modify the system's configuration.

• **One-Time Boot Menu**

Use this option to disable the POST one-time boot F11 prompt. When disabled, this prompt does not appear, and the F11 key is disabled, during POST.

• **Intelligent Provisioning**

Use this option to enable or disable access to Intelligent Provisioning. The default is enabled. When disabled, this prompt does not appear, and the F10 key is disabled, during POST.

• **Processor AES-NI Support**

Use this option to enable or disable the Advanced Encryption Standard Instruction Set (AES-NI) in the processor. When enabled, the speed of applications performing encryption and decryption using AES is improved.

• **Backup ROM Image Authentication**

Enable this option to authenticate the backup ROM image on startup. This ensures a reliable failsafe if Secure Start determines that the current ROM is corrupted, in which case the system will use the backup ROM during boot. The backup ROM can also be selected manually in UEFI by navigating to **System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options**.

• **System Intrusion Detection**

Enable this option to allow UEFI to receive notice whenever the System Intrusion switch sends an alert.

• **Secure Start**

Enabled by default and always on, this feature scans the iLO and BIOS firmware during POST and if it finds tampering, or corruption, it loads the firmware from an integrated backup. Secure Start is ideal for
protecting against malware that may have been inserted early in the manufacturing chain. There are no separate configurable options for Secure Start.

SATA secure erase

Available at System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options. Enable the options here to allow compatible SATA hard disks attached to the system to be securely erased when the secure erase process is started from Intelligent Provisioning.

Using the iLO 5 Configuration Utility

iLO 5 Configuration Utility options

You can access the iLO 5 Configuration Utility from the physical system console, or by using an iLO 5 remote console session. The utility has the following options:

- Network Options
- Advanced Network Options
- User Management
- Setting Options
- Set to factory defaults
- Reset iLO
- About

About the tasks in this section

The following tasks must be performed by accessing the iLO 5 Configuration Utility. Access the utility through UEFI: System Utilities > System Configuration > iLO 5 Configuration Utility.

Network Options

- MAC Address (read-only)—Specifies the MAC address of the selected iLO network interface.
- Network Interface Adapter—Specifies the iLO network interface adapter to use.
  - ON—Uses the iLO Dedicated Network Port.
  - Shared Network Port—Uses the Shared Network Port. This option is only available on supported servers.
  - OFF—Disables all network interfaces to iLO.
- Transceiver Speed Autoselect (iLO Dedicated Network Port only)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network.
  This option is only available when Network Interface Adapter is set to ON.
- Transceiver Speed Manual Setting (iLO Dedicated Network Port only)—Sets the link speed for the iLO network interface.
  This option is only available when Network Interface Adapter is set to ON and Transceiver Speed Autoselect is set to OFF.
• **Transceiver Duplex Setting** (iLO Dedicated Network Port only)—Sets the link duplex setting for the iLO network interface.

  This option is only available when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.

• **VLAN Enable** (Shared Network Port only)—Enables the VLAN feature.

  When the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN. This option is only available when **Network Interface Adapter** is set to **Shared Network Port**.

• **VLAN ID** (Shared Network Port only)—When a VLAN is enabled, specifies a VLAN tag.

  All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094. This option is only available when **Network Interface Adapter** is set to **Shared Network Port**.

• **DHCP Enable**—Configures iLO to obtain its IP address (and many other settings) from a DHCP server.

• **DNS Name**—Sets the DNS name of the iLO subsystem.

  This name can only be used if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.

• **IP Address**—Specifies the iLO IP address.

  If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.

• **Subnet Mask**—Specifies the subnet mask of the iLO IP network.

  If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.

• **Gateway IP Address**—Specifies the iLO gateway IP address.

  If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.

Configuring Network Options

**Procedure**

1. From the **System Utilities** screen, select **System Configuration > iLO 5 Configuration Utility > Network Options**.

2. Select any of the **Network Options**, and then select a setting or enter a value for that option.

3. Save your settings.

Advanced Network Options

• **Gateway from DHCP**—Specifies whether iLO uses a DHCP server-supplied gateway.

• **Gateway #1, Gateway #2, and Gateway #3**—If **Gateway from DHCP** is disabled, specifies up to three iLO gateway IP addresses.

• **DHCP Routes**—Specifies whether iLO uses the DHCP server-supplied static routes.

• **Route 1, Route 2, and Route 3**—If **DHCP Routes** is disabled, specifies the iLO static route destination, mask, and gateway addresses.
- **DNS from DHCP**—Specifies whether iLO uses the DHCP server-supplied DNS server list.

- **DNS Server 1, DNS Server 2, DNS Server 3**—If DNS from DHCP is disabled, specifies the primary, secondary, and tertiary DNS servers.

- **WINS from DHCP**—Specifies whether iLO uses the DHCP server-supplied WINS server list.

- **Register with WINS Server**—Specifies whether iLO registers its name with a WINS server.

- **WINS Server #1 and WINS Server #2**—If WINS from DHCP is disabled, specifies the primary and secondary WINS servers.

- **Domain Name**—The iLO domain name. If DHCP is not used, specifies a domain name.

### Configuring Advanced Network Options

#### Procedure

1. From the **System Utilities** screen, select **System Configuration > iLO 5 Configuration Utility > Advanced Network Options**.

2. Select any of the **Advanced Network Options**, and then select a setting or enter a value for that option.

3. Save your settings.

### User Management

- **Add User**

- **Edit/Remove User**

### Add User

Use this option to add new local iLO user accounts, with the following privileges and information.

**iLO 5 user privileges**

- **Administer User Accounts**—Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users.

  If you do not have this privilege, you can view your own settings and change your own password.

- **Remote Console Access**—Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.

- **Virtual Power and Reset**—Enables a user to power-cycle or reset the host system.

  These activities interrupt the system availability. A user with this privilege can diagnose the system by using the **Generate NMI to System** button.

- **Virtual Media**—Enables a user to use the Virtual Media feature on the host system.

- **Configure Settings**—Enables a user to configure most iLO settings, including security settings, and to remotely update the iLO firmware.

  This privilege does not enable local user account administration. After iLO is configured, revoking this privilege from all users prevents reconfiguration using the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU, the iLO 5 Configuration Utility, or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.

- **Host BIOS**—Enables a user to configure the host BIOS settings by using the UEFI System Utilities.
• **Host NIC**—Enables a user to configure the host NIC settings.

• **Host Storage**—Enables a user to configure the host storage settings.

• **Recovery Set**—Enables a user to manage the recovery install set.

**NOTE:**
By default, the Recovery Set privilege is assigned to the default Administrator account. To assign this privilege to another account, log into the iLO web interface with an account that already has this privilege. This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

**New User Information**

• **New User Name**—Specifies the name that appears in the user list on the **User Administration** page. It does not have to be the same as the **Login Name**. The maximum length for a user name is 39 characters. The user name must use printable characters. Assigning descriptive user names can help you to easily identify the owner of each login name.

• **Login Name**—Specifies the name that must be used when logging in to iLO. It appears in the user list on the **User Administration** page, on the **iLO Overview** page, and in iLO logs. The **Login Name** does not have to be the same as the **User Name**. The maximum length for a login name is 39 characters. The login name must use printable characters.

• **Password** and **Password Confirm**—Sets and confirms the password that is used for logging in to iLO. The maximum length for a password is 39 characters. Enter the password twice for verification.

**Adding new user accounts**

**Procedure**

1. From the **System Utilities** screen, select **System Configuration > iLO 5 Configuration Utility > User Management > Add User**.
2. Select any of the **iLO 5 user privileges**.
3. For each option, select one of the following settings.
   - **YES**—Enables the privilege for this user.
   - **NO**—Disables the privilege for this user.
4. Select a **New User Information** entry.
5. Complete each entry for the new user.
6. Create as many user accounts as needed, and then save your settings.

**Edit/Remove User**

Use this option to edit iLO user account settings, or to delete user accounts.
Editing or removing user accounts

Procedure

1. From the System Utilities screen, select System Configuration > iLO 5 Configuration Utility > User Management > Edit/Remove User.
2. Select the Action menu for the user account you want to edit or delete.
3. Select one of the following.
   • Delete—Deletes the user account.
   • Edit—Enables you to edit the user login name, password or user permissions.
4. Update as many user accounts as needed, and then save your settings.

Setting Options

Use this menu to view and configure iLO access settings.

• iLO 5 Functionality—Specifies whether iLO functionality is available. When this setting is enabled (default), the iLO network is available and communications with operating system drivers are active. When this setting is disabled, the iLO network and communications with operating system drivers are terminated. The iLO network and communications with operating system drivers are terminated when iLO functionality is disabled.

NOTE:
For ProLiant blade servers, the iLO functionality cannot be disabled on blade servers.

• iLO 5 Configuration Utility—Enables or disables the iLO 5 Configuration Utility.
   If this option is set to Disabled, the iLO 5 Configuration Utility menu item is not available when you access the UEFI System Utilities.

• Require Login for iLO 5 Configuration—Determines whether a user-credential prompt is displayed when a user accesses the iLO 5 functionality.
   If this setting is Enabled, provide user credentials for functions, including updating with SUM and RESTful Interface Tool.

• Show iLO 5 IP Address during POST—Enables the display of the iLO network IP address during host server POST.

• Local Users—Enables or disables local user account access.

• Serial CLI Status—Specifies the login model of the CLI feature through the serial port. Settings are:
   • Enabled—Authentication Required—Enables access to the iLO CLP from a terminal connected to the host serial port. Valid iLO user credentials are required.
   • Enabled—No Authentication Required—Enables access to the iLO CLP from a terminal connected to the host serial port. iLO user credentials are not required.
   • Disabled—Disables access to the iLO CLP from the host serial port.
   Use this option if you are planning to use physical serial devices.
• **Serial CLI Speed (bits/second)**—Specifies the speed of the serial port for the CLI feature. Settings (in bits per second) are:
  - 9600
  - 19200
  - 57600
  - 115200

For correct operation, set the serial port configuration to no parity, 8 data bits, and 1 stop bit (N/8/1).

**NOTE:**
The 38400 speed is supported in the iLO web interface, but is not currently supported by the iLO 5 Configuration Utility.

• **iLO Web Interface**—Specifies whether the iLO web interface can be used to communicate with iLO. This setting is enabled by default.

**Configuring access settings**

**Procedure**

1. From the System Utilities screen, select System Configuration > iLO 5 Configuration Utility > Setting Options.
2. Update user access Setting Options.
3. Save your settings.

**Set to factory defaults**

⚠️ **CAUTION:**
This operation clears all user and license data.

Use this option to reset iLO to the factory default settings. When you do so, you cannot access the iLO 5 Configuration Utility until after the next system reboot. If you are managing iLO remotely, the remote console session is automatically ended.

If the server has a factory installed license key, the license key is retained.

**Resetting iLO to the factory default settings**

**Procedure**

1. From the System Utilities screen, select System Configuration > iLO 5 Configuration Utility > Set to factory defaults.
   - The iLO 5 Configuration Utility prompts you to select YES or NO.
2. Select YES.
3. When prompted to confirm the reset, press Enter.
   - iLO resets to the factory default settings. If you are managing iLO remotely, the remote console session is automatically ended.
4. Resume the boot process:
a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

The iLO 5 Configuration Utility screen is still open from the previous session.

b. Press Esc until the main menu is displayed.

c. Select Exit and Resume Boot in the main menu, and press Enter.

d. When prompted to confirm the request, press Enter to exit the screen and resume the boot process.

Reset iLO

If iLO is slow to respond, you can use this option to perform a reset.

Resetting iLO with this method does not make any configuration changes, but it ends all active connections to iLO. When you reset iLO, the iLO 5 Configuration Utility is not available again until the next reboot.

Resetting iLO active connections

Prerequisite
Configure iLO Settings privilege

Procedure

1. From the System Utilities screen, select System Configuration > iLO 5 Configuration Utility > Reset iLO.

The iLO 5 Configuration Utility prompts you to select YES or NO.

2. Select YES.

3. When prompted to confirm the reset, press Enter.

Active iLO connections are reset. If you are managing iLO remotely, the remote console session is automatically ended.

4. Resume the boot process:

a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

The UEFI System Utilities are still open from the previous session.

b. Press Esc until the main menu is displayed.

c. Select Exit and Resume Boot in the main menu, and press Enter.

d. When prompted to confirm the request, press Enter to exit the utility and resume the normal boot process.

About

Use this menu to view information about the following iLO components.

- **Firmware Date**—The iLO firmware revision date.
- **Firmware Version**—The iLO firmware version.
- **iLO CPLD Version**—The iLO complex programmable logic device version.
- **Host CPLD Version**—The server complex programmable logic device version.
• Serial Number—The iLO serial number.
• PCI BUS—The PCI bus to which the iLO processor is attached.
• Device—The device number assigned to iLO in the PCI bus.

Viewing information about iLO

Procedure

1. From the System Utilities screen, select System Configuration > iLO 5 Configuration Utility > About.
2. View information about iLO components.

iLO Amplifier Pack configuration security

iLO Amplifier Pack allows for detailed alert monitoring to see events, including security events, in real time. iLO Amplifier Pack also includes powerful automated recovery tools.

The following tasks must be performed from the dashboard of the iLO Amplifier Pack VM appliance.

Managed Servers Alerts

As part of the inventory process, iLO Amplifier Pack subscribes to iLO for server alerts. When certain conditions occur, iLO Amplifier Pack sends out email or IFTTT alerts when an event is received from iLO.

Viewing alerts from managed servers

Use the Managed Servers Alerts page to see detailed information about alerts that have been received from managed servers.

Prerequisites

• User privileges
  ◦ Configure Manager with Security
  ◦ Configure Manager
  ◦ Configure User
  ◦ Configure Devices
  ◦ Login

Procedure

1. On the left navigation menu, click Alerts and Event Logs.
2. Click Managed Servers Alerts.

The event list appears displaying the following information for each event:

• Severity—Severity of the event
• iLO IP Address—The IP address for the iLO
• Alert Category—Type of event
Alert Name—Name of event

TimeStamp—Date and time stamp for each event

3. Additional options on this page:

- Enter a value in the Search box to search for specific information.
- Use the Show entries menu to choose the number of events to display per page.
- Click the angle bracket icon to see a summary and description of the event, and whether any further action is required.
- Use the navigation buttons to view the first, previous, next, or last page of the alerts list. You can also click a specific page number to jump to that page.
- Click Export to CSV to download the server alerts list.
- Click Clear All to delete all alerts from the server alerts list.

Server alert severity

The following icons indicate event severity:

- ✗ Critical—The event indicates a service loss or imminent service loss. Immediate attention is needed.
- ⚠ Warning—The event is significant but does not indicate performance degradation.
- ✔ Ok—The event falls within normal operation parameters.

Server alert details

The following information is listed for each managed server alert.

- Severity—The alert severity level
- iLO IP Address—The IP address of the iLO processor on the managed server
- Alert Category—The alert type
- Alert Name—The alert name
- TimeStamp—The date and time that the alert was recorded

Clearing the Server Alert Viewer list

NOTE:
A maximum of 5000 alerts can be displayed in the server alert viewer.

Procedure

1. Select Alerts and Event Logs in the navigation tree, and then click Managed Servers Alerts.
2. Click Clear All.
3. When prompted to confirm the request, click YES.
Exporting server alerts to a .csv file

Procedure

1. Click **Alerts and Event Logs** from the left navigation menu, and then click **Managed Servers Alerts**.
2. Click **Export to CSV**.
3. Select a location to save the .csv file, and then click **Save**.

Activity Logs and Alerts

iLO Amplifier Pack records all activity that occurs in the system, whether generated by a user or by the appliance itself.

Activity Logs are sent as email or IFTTT alerts if configured by the user.

Viewing activity logs

Use this page to view logs and alerts generated by iLO Amplifier Pack.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
Procedure

1. Click **Alerts and Event Logs**.
2. Click **Activity Logs and Alerts**.
   
   The event list appears displaying the following information for each event:
   
   - **Event Name**--Name of event
   - **Time**--Date and time stamp for each event
   - **Severity**--Severity of the event
   - **Event Summary**--Description of the event
   - **Affected Systems**--Systems that are affected by the task

3. Additional options on this page:
   
   - Use the **Search** field to find a specific event.
   - Use the **Show entries** menu to choose the number of events to display per page.
   - Click the angle bracket next to an event to see a description of the event and whether any further action is required.
   - Use the navigation buttons to view the first, previous, next, or last page of the list. You can also click a specific page number to jump to that page.
   - Click **Export to CSV** to download the information in .csv format.
   - Click **Clear All** to clear the event list.

Clearing activity alerts

Procedure

1. Select **Activity Logs and Alerts** from the left navigation menu, and then click the **Activity Alerts** tab.
2. Click **Clear All**.
3. When prompted to confirm the request, click **YES**.

Recovery Management

Introduction

iLO Amplifier Pack v1.15 introduces the Server System Restore feature that works with iLO 5 v1.17 to recover Gen 10 servers according to user-created recovery policies.

When iLO detects system corruption in a server that is monitored by iLO Amplifier Pack, iLO automatically alerts iLO Amplifier Pack to initiate and manage the system recovery process. iLO Amplifier Pack checks the event against user-created recovery policies for the affected system, and then begins the recovery process as outlined in the recovery policy assigned to the server.
Prerequisites

- Gen10 server with iLO 5 v1.17 or later
- To perform any recovery related actions, iLO Amplifier Pack user must have Configure Manager with Security privilege.
- The Firmware Baseline to be used for recovery should have iLO 5.17 or later.
- For recovery administration of Gen10 servers, HPE recommends configuring the BIOS boot mode to UEFI mode.
- For Device initiated full auto recovery, the recovery policy must have all three baselines specified: Firmware + Configuration + Operating System.
- You must have at least one recovery install set in iLO before triggering a Device Initiated recovery. HPE recommends not deleting the iLO Factory Install set in order to use the recovery feature in iLO Amplifier Pack.

More information

The following pages in iLO Amplifier Pack provide the tools to define recovery policies, assign them to managed servers, and monitor the recovery process.

- Recovery Policy
- Recovery Administration
- Recovery Task Monitor

Recovery operations

Each recovery operation follows a similar path:

Automatic recovery operations

Follow these steps to perform an Automatic Server Recovery or a Device Initiated Full Recovery.

1. Import firmware and OS baselines. For more information, see Importing a firmware baseline and Importing an OS baseline.
2. Create or import a configuration baseline from a server. For more information, see Create a configuration baseline and Import a configuration baseline from a server.
3. Create a recovery policy with the firmware, configuration, and OS baselines. For more information, see Create a recovery policy.
4. Assign a recovery policy to the selected servers with Auto Recovery Action enabled. For more information, see Assign a recovery policy.
5. A recovery task is triggered in iLO Amplifier Pack once it receives a recovery message from iLO when it finds corrupted firmware.

Manual recovery operations

Follow these steps to perform a Manual Recovery:
1. Import firmware and OS baselines. For more information, see Importing a firmware baseline and Importing an OS baseline.

2. Once iLO Amplifier Pack receives a firmware corruption alert from iLO, the check box becomes enabled for the selected server on the Administration page.

3. You can select and perform a Manual Recovery by selecting the required baselines or a recovery policy. For more information, see Performing a manual recovery.

Importing a firmware baseline

Use the Import Baseline feature to make the SPP or custom SPP iso image easily accessible for firmware updates. iLO Amplifier Pack supports baseline storage up to 80 GB (which includes both firmware and OS baseline files). The percentage of space used is displayed at the top of the Firmware Baseline page.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click Baseline Management from the left navigation menu, and then click Firmware Baseline.
2. Click Import Baseline.
3. Click to select Network Share (NFS) or HTTP/HTTPS from the Import Type menu.
4. Perform one of the following:
   - For NFS, enter the IP address, mount path, and storage path.
   - Enter the HTTP or HTTPS url to the iso image.
5. Click Import to import the iso image or click Cancel to return to the Firmware Baseline page.
6. Once the import completes, the baseline is listed on the Firmware Baseline page, along with the following information:
   - Filename of the .iso file
   - Name of the baseline
   - Version
   - Status of the import
   - File size in MB
7. (Optional). Click to delete the baseline.
NOTE:
You cannot delete a baseline if it is a part of a recovery policy or if it is being used by a task.

8. (Optional). Click View Details for more information about the component, such as the component name, available version, filename, and recommendation.

The Recommendation field provides HPE recommendations for baseline components based on how critical each is for the update. The following values can help you select the baseline components you want to use:

- Recommended
- Critical
- Optional

Importing an OS baseline

OS baselines are user-created, bootable .iso images that are used in the server system restore process to recover the OS, layered applications, and data restore from backups.

Use the Import Baseline feature to import operating system .iso images for server system restore. iLO Amplifier Pack supports baseline storage up to 80 GB (which includes both firmware and OS baseline files). The percentage of space used is displayed at the top of the OS Baseline page.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click Baseline Management from the left navigation menu, and then click OS Baseline.
2. Click Import Baseline.
3. Click to select Network Share (NFS) or HTTP/HTTPS from the Import Type menu.
4. Perform one of the following:
   - For NFS, enter the IP address, mount path, and storage path.
   - Enter the HTTP or HTTPS url to the iso image.
5. Click Import to import the .iso image or click Cancel to return to the OS Baseline page.
6. Once the import completes, the baseline is listed on the OS Baseline page, along with the following information:
Working with configuration baselines

Configuration baselines are used to create or import the server configuration settings (like BIOS, iLO, and Smart Storage settings) and to restore it back on the servers during the server system restore process.

The Configuration Baseline page provides the following information in the List of Configuration Baselines:

- Status
- Configuration baseline name
- Configuration baseline type
- Created by

Use the Configuration Baseline page to create, import, edit, and delete configuration settings.

Create a configuration baseline

**Prerequisites**

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

**Procedure**

1. Click Baseline Management from the left navigation menu, and then click Configuration Baseline.
2. Click New Configuration Baseline.
3. Enter a name in the Configuration Baseline Name field.
4. Select properties from the following categories:
• **BIOS Advanced, Generic, and Platform Settings**—For more information, see the UEFI documentation available from [http://www.hpe.com/info/ProLiantUEFI/docs](http://www.hpe.com/info/ProLiantUEFI/docs).

**NOTE:**
For recovery administration of Gen10 servers, HPE recommends configuring the BIOS boot mode to UEFI mode.

• **Boot Settings**
• **Smart Storage Settings**—For more information, see the smart storage and logical drive documentation available from [http://www.hpe.com/info/storage/docs](http://www.hpe.com/info/storage/docs).
• **iLO Settings**—For more information, see the iLO documentation available from [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).

5. Scroll through the list of parameters and click the check box to select the parameters you want to include in the baseline.

6. In the **Value** column, specify a value for each selected parameter.

7. Click **Create**.

   The new configuration baseline appears in the list on the **Configuration Baseline** page.

**Import a configuration baseline from a server**

**Prerequisites**

• User privileges
  ◦ Configure Devices
  ◦ Configure User
  ◦ Configure Manager
  ◦ Configure Manager with Security

• The server must be powered ON for import configuration to work. If the server is powered OFF the import configuration task fails.

**Procedure**

1. Click **Baseline Management** from the left navigation menu, and then click **Configuration Baseline**.

2. Click **Import Configuration From Server**.

3. Enter a name in the **Configuration Baseline Name** field.

4. Click the checkbox to select a server, and then click **Import**.

   The new configuration baseline appears in the list of server configuration baselines on the **Configuration Baseline** page.

**Editing a new configuration baseline**

Use these instructions to edit customizable server configuration baselines.
NOTE:
Snapshot server configuration baselines cannot be edited.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **Configuration Baseline**.
2. Click the right arrow next to the baseline you want to edit from the **List of Server Configuration Baselines**.
   The baseline settings appear.
3. Select properties from the following categories:
   - **BIOS Advanced, Generic, and Platform Settings**—For more information, see the UEFI documentation available from [http://www.hpe.com/info/ProLiantUEFI/docs](http://www.hpe.com/info/ProLiantUEFI/docs).
   - **Boot Settings**
   - **Smart Storage Settings**—For more information, see the smart storage and logical drive documentation available from [http://www.hpe.com/info/storage/docs](http://www.hpe.com/info/storage/docs).
   - **iLO Settings**—For more information, see the iLO documentation available from [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).
4. Scroll through the list of parameters and click the check box to select the parameters you want to change in the baseline.
5. In the **Value** column, specify a value for each selected parameter.
6. Click **Update** to save your changes.

Deleting a configuration baseline

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
• Configure User
• Configure Devices

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **Configuration Baseline**.
2. Click the right arrow next to the baseline you want to delete, and then click **Delete**.

**NOTE:**
You cannot delete a baseline if it is a part of a recovery policy or if it is being used by a task.

Recovery policy
Create a recovery policy

![Create New Recovery Policy](image)

Prerequisites

• User privileges
  ◦ Configure Manager with Security

• To create a recovery policy that includes an OS baseline or a firmware baseline, you must first upload the baselines to iLO Amplifier Pack from the **Baseline Management** page.

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Policy**.
2. Click **Create new policy**.
3. Enter a name for the new policy, and then select firmware, configuration, and OS baselines.
The following combinations are supported:

- Firmware only
- Firmware + Configuration
- Operating System only
- Firmware + Configuration + Operating System

**NOTE:**

- The list of firmware baselines includes only those that have been successfully uploaded to iLO Amplifier Pack.
- The list of firmware baselines includes only those containing firmware that supports Gen10 servers and later.
- The list of configuration baselines does not list the snapshot configuration baselines that are still importing or those that failed to import.

4. Click **Create** to save the policy.
   The new policy appears in the list on the **Recovery Policy** page.

### Delete a recovery policy

**Prerequisites**

- User privileges
  - Configure Manager with Security
- Before deleting a recovery policy, unassign the policy from any servers to which it might be assigned.

**Procedure**

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Policy**.

2. Click the icon for the policy that you want to delete.

### Recovery administration

The **Recovery Administration** page lists all of the Gen10 servers with an iLO Advanced Premium Security Edition license that are managed by iLO Amplifier Pack. When a firmware corruption occurs on a system, iLO detects this corruption and sends out an event to iLO Amplifier Pack. iLO Amplifier Pack then initiates the recovery process based on the recovery policy that is assigned to the server.
Assign a recovery policy

Prerequisites

- User privileges
  - Configure Manager with Security
- Gen10 server with iLO 5 v1.17 or later
- iLO Advanced Premium Security Edition license

Procedure

1. Click Recovery Management from the left navigation menu, and then click Recovery Administration.
2. Click Assign Auto Recovery Policy.
3. Click the check box to select one or more servers, and then click Next.
4. Select one of the following options from the Action drop-down menu:
   - Auto Recovery—Recovery process starts when iLO Amplifier Pack is automatically alerted from iLO.
   - Device Initiated Full Auto Recovery—Recovery process starts when a user manually initiates a recovery alert from iLO to iLO Amplifier Pack. A user can initiate a recovery alert from iLO by logging in to iLO with a user account that has recovery set privileges. In the iLO interface, navigate to the Administration -> Firmware Verification page, and then click Send Recovery Event.
   - Quarantine—Recovery process is not started, but server is shut down automatically from iLO Amplifier Pack.
5. Select the recovery policy that you want to apply from the Recovery Policy drop-down menu, and then click Next.
6. Verify your selections as displayed on the Summary page, and then click Assign Policy or click Previous to go back to change selections.
NOTE:
For Device initiated full auto recovery, the recovery policy must have all three baselines specified:
Firmware + Configuration + Operating System

Unassign a recovery policy

Prerequisites

- User privileges
  - Configure Manager with Security

Procedure

1. Click Recovery Management from the left navigation menu, and then click Recovery Administration.
2. Click Unassign Recovery Policy.
3. Click the check box to select one or more servers, and then click Unassign.

Performing a manual recovery

The Recovery Administration page lists all of the Gen10 servers with an iLO Advanced Premium Security Edition license that are managed by iLO Amplifier. When a firmware corruption happens on a system, iLO detects this corruption and sends out an event to iLO Amplifier. When this event is received, iLO Amplifier enables the check box on the Recovery Administration page. Select the system and then perform the Manual Recovery.
Prerequisites

- User privileges
  - Configure Manager with Security

Procedure

1. Click Recovery Management from the left navigation menu, and then click Recovery Administration.
2. Select the servers on which you want to perform a manual recovery.
3. From the Actions drop-down menu, click Manual Recovery.
4. On the Manual Recovery page, select a recovery policy from the drop-down menu.
5. Select a firmware and/or configuration baseline from their respective drop-down menus, and then click Next.
6. Select an OS baseline, and then click Next.
7. Review your selections and click Back to make changes, if needed.
8. Click Start Recovery and then click Close.
   - Check the progress of the manual recovery task on the Recovery Task Monitor page.
Performing a quarantine operation

Prerequisites

- User privileges
  - Configure Manager with Security

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Administration**.
2. Select the servers on you want to quarantine.
3. From the **Actions** drop-down menu, click **Quarantine**.
4. Click **Yes** on the **Quarantine Confirmation** dialog box to continue or click **No** to cancel the operation.
   Check the progress of the quarantine task on the **Recovery Task Monitor** page.

Monitor recovery tasks

Prerequisites

- User privileges
  - Configure Manager with Security

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Monitor Recovery Tasks** to view all of the status of all running and completed tasks.
2. Click the right arrow to see details and the percentage of the task progress.
iLO Amplifier Pack applies the recovery policy in the following order:

a. The server is powered down.
b. The firmware is updated, if selected.
c. The configuration baseline is applied, if selected.
d. The server is rebooted to the OS baseline, if selected.

The recovery process may take a while to complete. See the Activity Logs and Alerts page for the status of the recovery process.

Remote management security

HPE offers the following remote management security options:

- **Remote console security lock**
  Enhances the security of the server by automatically locking an operating system or logging out a user when a Remote Console session ends or the network link to iLO is lost.

- **Integrated Remote Console trust settings**
  Controls whether a trusted SSL certificate is required when launching a .NET Integrated Remote Console session.

About the tasks in this section

The following tasks must be performed by accessing the iLO 5 web interface.

Configuring Remote Console Computer Lock settings

This feature locks the OS or logs a user out when a Remote Console session ends or the network link to iLO is lost. If you open a .NET IRC or Java IRC window when this feature is configured, the operating system will be locked when you close the window.

**Prerequisites**

Configure iLO Settings privilege

**Procedure**

1. Click **Remote Console & Media** in the navigation tree, and then click the **Security** tab.
2. Select from the following Remote Console Computer Lock settings: **Windows**, **Custom**, and **Disabled**.
3. Select a computer lock key sequence.
4. To save the changes, click **Apply**.
Remote Console Computer Lock options

- **Windows**—Use this option to configure iLO to lock a managed server running a Windows operating system. The server automatically displays the **Computer Locked** dialog box when a Remote Console session ends or the iLO network link is lost.

- **Custom**—Use this option to configure iLO to use a custom key sequence to lock a managed server or log out a user on that server. You can select up to five keys from the list. The selected key sequence is sent automatically to the server operating system when a Remote Console session ends or the iLO network link is lost.

- **Disabled** (default)—Use this option to disable the Remote Console Computer Lock feature. When a Remote Console session ends or the iLO network link is lost, the operating system on the managed server is not locked.

**Keys for configuring Remote Console computer lock keys and hot keys**

The following keys are supported when you configure Remote Console hot keys and Remote Console computer lock keys.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Value</th>
<th>Letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESC</td>
<td>SCRL LCK</td>
<td>0</td>
<td>f</td>
</tr>
<tr>
<td>L_ALT</td>
<td>SYS RQ</td>
<td>1</td>
<td>g</td>
</tr>
<tr>
<td>R_ALT</td>
<td>PRINT SCREEN</td>
<td>2</td>
<td>h</td>
</tr>
<tr>
<td>L_SHIFT</td>
<td>F1</td>
<td>3</td>
<td>l</td>
</tr>
<tr>
<td>R_SHIFT</td>
<td>F2</td>
<td>4</td>
<td>j</td>
</tr>
<tr>
<td>L_CTRL</td>
<td>F3</td>
<td>5</td>
<td>k</td>
</tr>
<tr>
<td>R_CTRL</td>
<td>F4</td>
<td>6</td>
<td>l</td>
</tr>
<tr>
<td>L_GUI</td>
<td>F5</td>
<td>7</td>
<td>m</td>
</tr>
<tr>
<td>R_GUI</td>
<td>F6</td>
<td>8</td>
<td>n</td>
</tr>
<tr>
<td>INS</td>
<td>F7</td>
<td>9</td>
<td>o</td>
</tr>
<tr>
<td>DEL</td>
<td>F8</td>
<td>;</td>
<td>p</td>
</tr>
<tr>
<td>HOME</td>
<td>F9</td>
<td>=</td>
<td>q</td>
</tr>
<tr>
<td>END</td>
<td>F10</td>
<td>[</td>
<td>r</td>
</tr>
<tr>
<td>PG UP</td>
<td>F11</td>
<td>\</td>
<td>s</td>
</tr>
<tr>
<td>PG DN</td>
<td>F12</td>
<td>]</td>
<td>t</td>
</tr>
<tr>
<td>ENTER</td>
<td>SPACE</td>
<td>.</td>
<td>u</td>
</tr>
<tr>
<td>TAB</td>
<td>.</td>
<td>a</td>
<td>v</td>
</tr>
</tbody>
</table>

*Table Continued*
Configuring the Integrated Remote Console Trust setting (.NET IRC)

The .NET IRC is launched through Microsoft ClickOnce, which is part of the Microsoft .NET Framework. ClickOnce requires that any application installed from an SSL connection must be from a trusted source. If a browser is not configured to trust an iLO processor, and this setting is enabled, ClickOnce notifies you that the application cannot start.

Hewlett Packard Enterprise recommends installing a trusted SSL certificate and enabling the IRC requires a trusted certificate in iLO setting. In this configuration, the .NET IRC is launched by using an HTTPS connection. If the IRC requires a trusted certificate in iLO setting is disabled, the .NET IRC is launched by using a non-SSL connection, and SSL is used after the .NET IRC starts to exchange encryption keys.

Prerequisites
Configure iLO Settings privilege

Procedure

1. Click Remote Console & Media in the navigation tree, and then click the Security tab.
2. To enable or disable the IRC requires a trusted certificate in iLO setting, click the toggle switch.
3. To save the changes, click Apply.

HPE ProLiant Gen10 security states

The capabilities of HPE iLO Standard that comes with every ProLiant Gen10 server gives customers the ability to configure your server in one of three security states. With the iLO Advanced Premium Security Edition license, customers that need the highest-level encryption capabilities of CNSA have a fourth security state available to them.

As you move up the scale in security, the server enforces stronger encryption rules for webpages, SSH, and network communications. Note that both ends of each network connection must support the encryption rules, or they cannot communicate, and some interfaces are shut down to limit potential security threats.

The security states include:

- Production
- HighSecurity
- FIPS
- SuiteB/CNSA
### iLO security states

**Production (default)**
When set to this security state:

- iLO uses the factory default encryption settings.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) disables the password requirement for logging in to iLO.

**HighSecurity**
When iLO is set to this security state:

- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the browser, SSH port, iLO RESTful API, and RIBCL. When HighSecurity is enabled, you must use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.
- User name and password restrictions for iLO RESTful API and RIBCL commands executed from the host system are enforced when iLO is configured to use this security state.
- Remote Console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.
- You cannot connect to the server with network-based tools that do not support TLS 1.2.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

**FIPS**
When iLO is set to this security state:

- iLO operates in a mode intended to comply with the requirements of FIPS 140-2 level 1.
  FIPS is a set of computer security standards mandated for use by United States government agencies and contractors.
  The FIPS security state is not the same as FIPS validated. FIPS validated refers to software that received validation by completing the Cryptographic Module Validation Program.
  For more information, see [Configuring a FIPS-validated environment with iLO](#) on page 95.
- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the browser, SSH port, iLO RESTful API, and RIBCL. When FIPS is enabled, you must use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.
- User name and password restrictions for iLO RESTful API and RIBCL commands executed from the host system are enforced when iLO is configured to use this security state.
- Remote Console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.
• You cannot connect to the server with network-based tools that do not support TLS 1.2.

• The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

CNSA
The CNSA security state (also called SuiteB mode) is available only when the FIPS security state is enabled. When set to this security state:

• iLO operates in a mode intended to comply with the CNSA requirements defined by the NSA, and intended to secure systems used to hold United States government top secret classified data.

• You cannot connect to the server with network-based tools that do not support TLS 1.2.

• The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

Configuring encryption settings

Enabling the Production or HighSecurity security state

Use this procedure to configure iLO to use one of the following security states: Production or HighSecurity.

To configure iLO to use the FIPS and CNSA security states, see Enabling the FIPS and CNSA security states on page 92.

Prerequisites
Configure iLO Settings privilege

Procedure

1. Optional: Install any needed firmware and software updates.

2. Click Security in the navigation tree, and then click the Encryption tab.

3. Select Production or HighSecurity in the Security State menu.

4. Click Apply.

   iLO prompts you to confirm that you want to restart iLO to apply the new settings.

5. To end your browser connection and restart iLO, click Yes, apply and reset.

   It might take several minutes before you can re-establish a connection.

6. Close all open browser windows.

   Any browser sessions that remain open might use the wrong cipher for the configured security state.

Enabling the FIPS and CNSA security states

Use this procedure to configure iLO to use the FIPS and CNSA security states. To configure iLO to use the Production or HighSecurity security states, see Enabling the Production or HighSecurity security state on page 92.

To configure iLO in a FIPS-validated environment, see Configuring a FIPS-validated environment with iLO on page 95.
The FIPS security state might be required for Common Criteria compliance, Payment Card Industry compliance, or other standards.

If your license expires or is downgraded after you enable the FIPS or CNSA security states, iLO will continue to operate with the configured security state, but all other features activated by the expired or downgraded license will be unavailable.

**Prerequisites**

- Configure iLO Settings privilege
- If you plan to enable the optional CNSA security state, an iLO license that supports this feature is installed.
- The default iLO user credentials are available.

**Procedure**

1. Optional: Capture the current iLO configuration by using the iLO backup feature or HPONCFG. For more information, see *iLO backup and restore* or the iLO scripting and CLI guide.
2. Optional: Install any needed firmware and software updates.
3. Click **Security** in the navigation tree, and then click the **Encryption** tab.
4. Select **FIPS** in the **Security State** menu, and then click **Apply**.
   
   iLO prompts you to confirm the request.

   **CAUTION:**
   
   Enabling the FIPS security state resets iLO to factory default settings. All iLO settings are erased, including user data, most configuration settings, and logs. Installed license keys are retained.
   
   The only way to disable the FIPS security state is to reset iLO to the factory default settings.

5. To confirm the request to enable the FIPS security state, click **Yes, apply and reset**.
   
   iLO reboots with the FIPS security state enabled. Wait at least 90 seconds before attempting to re-establish a connection.

6. Optional: Enable the **CNSA** security state.
   
   a. Log in to iLO by using the default user credentials.
   
   b. Click **Security** in the navigation tree, and then click the **Encryption** tab.
   
   c. Select **CNSA** in the **Security State** menu, and then click **Apply**.
      
      iLO prompts you to confirm the request.
   
   d. To confirm the request to enable **CNSA**, click **Yes, apply and reset**.
      
      iLO reboots with the CNSA security state enabled. Wait at least 90 seconds before attempting to re-establish a connection.
   
   e. Log in to iLO again by using the default iLO credentials.

7. **Install a trusted certificate.**

   The default self-signed SSL certificate is not allowed when the FIPS security state is enabled. Previously installed trusted certificates are deleted when you set iLO to use the FIPS security state.
8. Verify that IPMI/DCMI over LAN Access and SNMP Access are disabled on the Access Settings page.

**IMPORTANT:**
Some iLO interfaces, such as the standards-compliant implementations of IPMI and SNMP, are not FIPS-compliant and cannot be made FIPS-compliant.

9. Optional: Restore the iLO configuration by using the iLO restore feature or HPONCFG.

User privileges are required when you restore the configuration with HPONCFG. If you do not have the required user privileges, an error message is displayed.

HPONCFG for Windows is not supported when iLO is configured to use the CNSA security state.

For more information, see [iLO backup and restore](#) or the iLO scripting and CLI guide.

10. Optional: If you restored the configuration, set new passwords for local iLO user accounts, and confirm that IPMI/DCMI over LAN Access and SNMP Access are disabled on the Access Settings page.

These settings might be reset when you restore the configuration.

11. Optional: Configure the Login Security Banner to inform iLO users that the system is using FIPS security state.

### Connecting to iLO when using higher security states

After you enable a security state that is higher than the default value (Production), iLO requires that you connect through secure channels by using an AES cipher.

When iLO is configured to use the CNSA security state, an AES 256 GCM cipher is required.

#### Web browser

Configure the browser to support TLS 1.2 and an AES cipher. If the browser is not using an AES cipher, you cannot connect to iLO.

Different browsers use different methods for selecting a negotiated cipher. For more information, see your browser documentation.

Log out of iLO through the current browser before changing the browser cipher setting. Any changes made to the cipher settings while you are logged in to iLO might enable the browser to continue using a non-AES cipher.

#### SSH connection

For information about setting the available ciphers, see the SSH utility documentation.

#### RIBCL

- HPQLOCFG, displays the cipher details in the output, for example:
  
  Detecting iLO...
  Negotiated cipher: 256-bit Aes256 with 0-bit Sha384 and 384-bit 44550

- HPONCFG requires user credentials when the HighSecurity, FIPS, or CNSA security states are enabled. If you do not have the required user privileges, an error message is displayed.

- HPONCFG for Windows is not supported when the CNSA security state is enabled.

#### iLO RESTful API

Use a utility that supports TLS 1.2 and an AES cipher.
Configuring a FIPS-validated environment with iLO

Use the following instructions to operate iLO in a FIPS-validated environment. To use the FIPS security state in iLO, see **Enabling the FIPS and CNSA security states** on page 92.

It is important to decide if a FIPS-validated version of iLO is required for your environment, or if running iLO with the FIPS security state enabled will suffice. Because of the lengthy validation process, a FIPS-validated version of iLO might have been superseded by a nonvalidated version with new features and security enhancements. In this situation, a FIPS-validated version of iLO might be less secure than the latest version.

**Procedure**

To set up an environment with a FIPS-validated version of iLO, follow the steps in the Security Policy document that was part of the iLO FIPS validation process.

The Security Policy documents for validated versions of iLO are available on the NIST website. To review information about iLO, search for the keyword iLO in the *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules* document.

**Disabling FIPS mode**

**Procedure**

1. To disable FIPS mode for iLO (for example, if a server is decommissioned), set iLO to the factory default settings.
   
   You can perform this task by using RIBCL scripts, the iLO RESTful API, or the iLO 5 Configuration Utility.

   ![CAUTION:]
   
   When you reset iLO to the factory default settings, all iLO settings are erased, including user data, license data, configuration settings, and logs. If the server has a factory installed license key, the license key is retained.

   Events related to the reset are not logged to the iLO Event Log and Integrated Management Log because this step clears all the data in the logs.

2. Reboot the server operating system.

   During the reset to the factory default settings, SMBIOS records are cleared. Memory and network information will not be displayed in the iLO web interface until the server OS reboot is complete.

**SSH cipher, key exchange, and MAC support**

iLO provides enhanced encryption through the SSH port for secure CLP transactions.

Based on the configured security state, iLO supports the following:

**Production**

- AES256-CBC, AES128-CBC, 3DES-CBC, and AES256-CTR ciphers
- diffie-hellman-group14-sha1 and diffie-hellman-group1-sha1 key exchange
- hmac-sha1 or hmac-sha2-256 MACs
iLO provides enhanced security for remote management in distributed IT environments. SSL encryption protects web browser data. Encryption of HTTP data provided by SSL ensures that the data is secure as it is transmitted across the network.

When you log in to iLO through a browser, the browser and iLO negotiate a cipher setting to use during the session. The negotiated cipher is displayed on the Encryption page.

The following lists of supported ciphers apply to all iLO SSL connections, including connections to LDAP servers, ESKM servers, SSO servers, Insight Remote Support servers, https:// URLs used in Virtual Media, the iLO RESTful API, CLI commands, and iLO Federation Group Firmware updates.

Based on the configured security state, iLO supports the following ciphers:

**Production**

- 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES256-SHA)
- 256-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
- 256-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES256-SHA)
- 256-bit AES-GCM with RSA, and an AEAD MAC (AES256-GCM-SHA384)
- 256-bit AES with RSA, and a SHA256 MAC (AES256-SHA256)
- 256-bit AES with RSA, and a SHA1 MAC (AES256-SHA)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES128-SHA)
- 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)
- 128-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES128-SHA)
- 128-bit AES-GCM with RSA, and an AEAD MAC (AES128-GCM-SHA256)
• 128-bit AES with RSA, and a SHA256 MAC (AES128-SHA256)
• 128-bit AES with RSA, and a SHA1 MAC (AES128-SHA)
• 168-bit 3DES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-DES-CBC3-SHA)
• 168-bit 3DES with RSA, DH, and a SHA1 MAC (EDH-RSA-DES-CBC3-SHA)
• 168-bit 3DES with RSA, and a SHA1 MAC (DES-CBC3-SHA)

**FIPS or HighSecurity**

TLS 1.2 is required for these security states.

• 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
• 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
• 256-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
• 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
• 256-bit AES-GCM with RSA, and an AEAD MAC (AES256-GCM-SHA384)
• 256-bit AES with RSA, and a SHA256 MAC (AES256-SHA256)
• 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
• 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
• 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
• 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)
• 128-bit AES-GCM with RSA, and an AEAD MAC (AES128-GCM-SHA256)
• 128-bit AES with RSA, and a SHA256 MAC (AES128-SHA256)

**CNSA**

TLS 1.2 is required for this security state.

256-bit AES-GCM with ECDSA, ECDH, and an AEAD MAC (ECDHE-ECDSA-AES256-GCM-SHA384)

**Directory integration, access control, and auditing**

HPE iLO allows administrators to choose the type of directory integration and its associated access control, and the auditing of access.

**Directory authentication and authorization**

The iLO firmware supports Kerberos authentication with Microsoft Active Directory. It also supports directory integration with an Active Directory or OpenLDAP directory server.

When you configure directory integration, you can use the schema-free option or the HPE Extended Schema. The HPE Extended Schema is supported only with Active Directory. The iLO firmware connects to directory services by using SSL connections to the directory server LDAP port.

You can enable the directory server certificate validation option for schema-free and HPE Extended Schema by importing a CA certificate. This feature ensures that iLO connects to the correct directory server during LDAP authentication.
Configuring the authentication and directory server settings is one step in the process of configuring iLO to use a directory or Kerberos authentication.

Prerequisites for configuring authentication and directory server settings

Procedure

1. Verify that your iLO user account has the Configure iLO Settings privilege.
2. Install an iLO license that supports this feature.
3. Configure your environment to support Kerberos authentication or directory integration.
4. The Kerberos keytab file is available (Kerberos authentication only).

Configuring Kerberos authentication settings in iLO

Prerequisites

Your environment meets the prerequisites for using this feature.

Procedure

1. Click Security in the navigation tree, and then click the Directory tab.
2. Enable Kerberos Authentication.
3. Set Local User Accounts to enabled if you want to use local user accounts at the same time as Kerberos authentication.
4. Enter the Kerberos Realm name.
5. Enter the Kerberos KDC Server Address.
6. Enter the Kerberos KDC Server Port.
7. To add the Kerberos Keytab file, click Browse (Internet Explorer or Firefox) or Choose File (Chrome), and then follow the onscreen instructions.
8. Click Apply Settings.

Kerberos settings

- **Kerberos Authentication**—Enables or disables Kerberos login. If Kerberos login is enabled and configured correctly, the Zero Sign In button appears on the login page.
- **Kerberos Realm**—The name of the Kerberos realm in which the iLO processor operates. This value can be up to 128 characters. The realm name is usually the DNS name converted to uppercase letters. Realm names are case-sensitive.
- **Kerberos KDC Server Address**—The IP address or DNS name of the KDC server. This value can be up to 128 characters. Each realm must have at least one Key Distribution Center (KDC) that contains an authentication server and a ticket grant server. These servers can be combined.
- **Kerberos KDC Server Port**—The TCP or UDP port number on which the KDC is listening. The default value is 88.
- **Kerberos Keytab**—A binary file that contains pairs of service principal names and encrypted passwords. In the Windows environment, you use the ktpass utility to generate the keytab file.
Configuring schema-free directory settings in iLO

Prerequisites
Your environment meets the prerequisites for using this feature.

Procedure

1. Click Security in the navigation tree, and then click the Directory tab.
3. Set Local User Accounts to enabled if you want to use local user accounts at the same time as directory integration.
4. OpenLDAP users only: Enable Generic LDAP. This setting is available only if Use Directory Default Schema is selected.
5. For configurations with CAC/Smartcard authentication enabled, enter the CAC LDAP service account and password in the iLO Object Distinguished Name CAC LDAP Service Account and iLO Object Password boxes.
6. Enter the FQDN or IP address of a directory server in the Directory Server Address box.
7. Enter the directory server port number in the Directory Server LDAP Port box.
8. Optional: Import a new CA certificate.
   a. Click Import in the Certificate Status box.
   b. Paste the Base64-encoded X.509 certificate data into the Import Certificate window, and then click Import.
9. Optional: Replace an existing CA certificate.
   a. Click View in the Certificate Status box.
   b. Click New in the Certificate Details window.
   c. Paste the Base64-encoded X.509 certificate data into the Import Certificate window, and then click Import.
10. Enter valid search contexts in one or more of the Directory User Context boxes.
11. Click Apply Settings.
12. To test the communication between the directory server and iLO, click Test Settings.
13. To configure directory groups, click Administer Groups to navigate to the Directory Groups page.

Schema-free directory settings

- Use Directory Default Schema—Selects directory authentication and authorization by using user accounts in the directory. User accounts and group memberships are used to authenticate and authorize users. To disable access, select Disabled.
  This configuration supports Active Directory and OpenLDAP.

- Generic LDAP—Specifies that this configuration uses the OpenLDAP supported BIND method.
• **iLO Object Distinguished Name/CAC LDAP Service Account**—Specifies the CAC LDAP service account when CAC/Smartcard authentication is configured and used with the schema-free directory option.

  User search contexts are not applied to the iLO object DN when iLO accesses the directory server.

• **iLO Object Password**—Specifies the CAC LDAP service account password when CAC/Smartcard authentication is configured and used with the schema-free directory option.

• **Directory Server Address**—Specifies the network DNS name or IP address of the directory server. The directory server address can be up to 127 characters.

  If you enter the FQDN, ensure that the DNS settings are configured in iLO.

  Hewlett Packard Enterprise recommends using DNS round-robin when you define the directory server.

• **Directory Server LDAP Port**—Specifies the port number for the secure LDAP service on the server. The default value is 636. If your directory service is configured to use a different port, you can specify a different value. Make sure that you enter a secured LDAP port. iLO cannot connect to an unsecured LDAP port.

• **Directory User Contexts**—These boxes enable you to specify common directory subcontexts so that users do not need to enter their full DNs at login. Directory user contexts can be up to 128 characters.

• **Certificate Status**—Specifies whether a directory server CA certificate is loaded.

  If the status is **Loaded**, click **View** to display the CA certificate details. If no CA certificate is loaded, the status **Not Loaded** is displayed. iLO supports SSL certificates up to 4 KB in size.

---

### Configuring HPE Extended Schema directory settings in iLO

**Prerequisites**

Your environment meets the **prerequisites** for using this feature.

**Procedure**

1. Click **Security** in the navigation tree, and then click the **Directory** tab.

2. Select **Use HPE Extended Schema** from the **LDAP Directory Authentication** menu.

3. Set **Local User Accounts** to enabled if you want to use local user accounts at the same time as directory integration.

4. Enter the location of this iLO instance in the directory tree in the **iLO Object Distinguished Name/CAC LDAP Service Account** box.

5. Enter the FQDN or IP address of a directory server in the **Directory Server Address** box.

6. Enter the directory server port number in the **Directory Server LDAP Port** box.

7. Optional: Import a new CA certificate.

   a. Click **Import** in the **Certificate Status** text box.

   b. Paste the Base64-encoded X.509 certificate data into the **Import Certificate** window, and then click **Import**.

8. Optional: Replace an existing CA certificate.
a. Click **View** in the **Certificate Status** text box.

b. Click **New** in the **Certificate Details** window.

c. Paste the Base64-encoded X.509 certificate data into the **Import Certificate** window, and then click **Import**.

9. Enter valid search contexts in one or more of the **Directory User Context** boxes.

10. Click **Apply Settings**.

11. To test the communication between the directory server and iLO, click **Test Settings**.

**HPE Extended Schema directory settings**

- **Use iLO Extended Schema**—Selects directory authentication and authorization by using directory objects created with the HPE Extended Schema. Select this option when the directory has been extended with the HPE Extended Schema. The HPE Extended Schema works only with Microsoft Windows. To disable access, select **Disabled**.
  
  This configuration supports Active Directory.

- **Directory Server Address**—Specifies the network DNS name or IP address of the directory server. The directory server address can be up to 127 characters.
  
  If you enter the FQDN, ensure that the DNS settings are configured in iLO.
  
  Hewlett Packard Enterprise recommends using DNS round-robin when you define the directory server.

- **Directory Server LDAP Port**—Specifies the port number for the secure LDAP service on the server. The default value is 636. If your directory service is configured to use a different port, you can specify a different value. Make sure that you enter a secured LDAP port. iLO cannot connect to an unsecured LDAP port.

- **iLO Object Distinguished Name/CAC LDAP Service Account**—For the HPE Extended Schema configuration, this setting specifies where this iLO instance is listed in the directory tree (for example, cn=Mail Server iLO,ou=Management Devices,o=ab).
  
  User search contexts are not applied to the iLO object DN when iLO accesses the directory server.

- **Directory User Contexts**—These boxes enable you to specify common directory subcontexts so that users do not need to enter their full DNs at login. Directory user contexts can be up to 128 characters.

- **Certificate Status**—Specifies whether a directory server CA certificate is loaded.
  
  If the status is **Loaded**, click **View** to display the CA certificate details. If no CA certificate is loaded, the status **Not Loaded** is displayed. iLO supports SSL certificates up to 4 KB in size.

**Directory user contexts**

You can identify the objects listed in a directory by using unique DNs. However, DNs can be long, users might not know their DNs, or users might have accounts in different directory contexts. When you use user contexts, iLO attempts to contact the directory service by DN, and then applies the search contexts in order until login is successful.
• **Example 1**—If you enter the search context `ou=engineering,o=ab`, you can log in as `user` instead of logging in as `cn=user,ou=engineering,o=ab`.

• **Example 2**—If the IM, Services, and Training departments manage a system, the following search contexts enable users in these departments to log in by using their common names:

  ◦ Directory User Context 1: `ou=IM,o=ab`
  ◦ Directory User Context 2: `ou=Services,o=ab`
  ◦ Directory User Context 3: `ou=Training,o=ab`

If a user exists in both the IM organizational unit and the Training organizational unit, login is first attempted as `cn=user,ou=IM,o=ab`.

• **Example 3 (Active Directory only)**—Microsoft Active Directory allows an alternate user credential format. A user can log in as `user@domain.example.com`. Entering the search context `@domain.example.com` allows the user to log in as `user`. Only a successful login attempt can test search contexts in this format.

• **Example 4 (OpenLDAP user)**—If a user has the DN `UID=user,ou=people,o=ab`, and you enter the search context `ou=people,o=ab`, the user can log in as `user` instead of entering the DN. To use this format, you must enable Generic LDAP on the Security - Directory page.

**Directory Server CA Certificate**

During LDAP authentication, iLO validates the directory server certificate if the CA certificate is already imported. For successful certificate validation, make sure that you import the correct CA certificate. If certificate validation fails, iLO login is denied and an event is logged. If no CA certificate is imported, the directory server certificate validation step is skipped.

To verify SSL communication between the directory server and iLO, click Test Settings.

**Local user accounts with Kerberos authentication and directory integration**

Local user accounts can be active when you configure iLO to use a directory or Kerberos authentication. In this configuration, you can use local and directory-based user access.

Consider the following:

• When local user accounts are enabled, configured users can log in by using locally stored user credentials.

• When local accounts are disabled, user access is limited to valid directory credentials.

• Do not disable local user access until you have validated access through Kerberos or a directory.

• When you use Kerberos authentication or directory integration, Hewlett Packard Enterprise recommends enabling local user accounts and configuring a user account with administrator privileges. This account can be used if iLO cannot communicate with the directory server.

• Access through local user accounts is enabled when directory support is disabled or an iLO license is revoked.

**Running directory tests**

Directory tests enable you to validate the configured directory settings. The directory test results are reset when directory settings are saved, or when the directory tests are started.
Procedure

1. Click Security in the navigation tree, and then click the Directory tab.

2. At the bottom of the Directory page, click Test Settings.

   iLO displays the results of a series of simple tests designed to validate the directory settings. After your directory settings are configured correctly, you do not need to rerun these tests. The Directory Tests page does not require you to log in as a directory user.

3. In the Directory Test Controls section, enter the DN and password of a directory administrator in the Directory Administrator Distinguished Name and Directory Administrator Password boxes.

   Hewlett Packard Enterprise recommends that you use the same credentials that you used when creating the iLO objects in the directory. iLO does not store these credentials; they are used to verify the iLO object and user search contexts.

4. In the Directory Test Controls section, enter a test user name and password in the Test User Name and Test User Password boxes.

5. Click Start Test.

   Several tests begin in the background, starting with a network ping of the directory user by establishing an SSL connection to the server and evaluating user privileges.

   While the tests are running, the page refreshes periodically. You can stop the tests or manually refresh the page at any time.

Directory test input values

Enter the following values when you run directory tests:

- **Directory Administrator Distinguished Name**—Searches the directory for iLO objects, roles, and search contexts. This user must have the right to read the directory.

- **Directory Administrator Password**—Authenticates the directory administrator.

- **Test User Name and Test User Password**—Tests login and access rights to iLO. This name does not need to be fully distinguished because user search contexts can be applied. This user must be associated with a role for this iLO.

   Typically, this account is used to access the iLO processor being tested. It can be the directory administrator account, but the tests cannot verify user authentication with a superuser account. iLO does not store these credentials.

Directory test status values

iLO displays the following status values for directory tests:

- **In Progress**—Indicates that directory tests are currently being performed in the background. Click Stop Test to cancel the current tests, or click Refresh to update the contents of the page with the latest results. Using the Stop Test button might not stop the tests immediately.

- **Not Running**—Indicates that directory tests are current, and that you can supply new parameters to run the tests again. Use the Start Test button to start the tests and use the current test control values. Directory tests cannot be started after they are already in progress.

- **Stopping**—Indicates that directory tests have not yet reached a point where they can stop. You cannot restart tests until the status changes to Not Running. Use the Refresh button to determine whether the tests are complete.
Directory test results

The Directory Test Results section shows the directory test status with the date and time of the last update.

- **Overall Status**—Summarizes the results of the tests.
  - **Not Run**—No tests were run.
  - **Inconclusive**—No results were reported.
  - **Passed**—No failures were reported.
  - **Problem Detected**—A problem was reported.
  - **Failed**—A specific subtest failed. To identify the problem, check the onscreen log.
  - **Warning**—One or more of the directory tests reported a Warning status.

- **Test**—The name of each test.

- **Result**—Reports status for a specific directory setting or an operation that uses one or more directory settings. These results are generated when a sequence of tests is run. The results stop when the tests run to completion, when a test failure prevents further progress, or when the tests are stopped. Test results follow:
  - **Passed**—The test ran successfully. If more than one directory server was tested, all servers that ran this test were successful.
  - **Not Run**—The test was not run.
  - **Failed**—The test was unsuccessful on one or more directory servers. Directory support might not be available on those servers.
  - **Warning**—The test ran and reported a warning condition, for example, a certificate error. Check the Notes column for suggested actions to correct the warning condition.

- **Notes**—Indicates the results of various phases of the directory tests. The data is updated with failure details and information that is not readily available, like the directory server certificate subject and which roles were evaluated successfully.

### iLO directory tests

**Directory Server DNS Name**

If the directory server is defined in FQDN format (directory.company.com), iLO resolves the name from FQDN format to IP format, and queries the configured DNS server.

If the test is successful, iLO obtained an IP address for the configured directory server. If iLO cannot obtain an IP address for the directory server, this test and all subsequent tests fail.

If the directory server is configured with an IP address, iLO skips this test.

**Ping Directory Server**

iLO initiates a ping to the configured directory server.

The test is successful if iLO receives the ping response; it is unsuccessful if the directory server does not reply to iLO.

If the test fails, iLO will continue with the subsequent tests.

**Connect to Directory Server**

iLO attempts to negotiate an LDAP connection with the directory server.
If the test is successful, iLO was able to initiate the connection.

If the test fails, iLO was not able to initiate an LDAP connection with the specified directory server. Subsequent tests will stop.

**Connect using SSL**

iLO initiates SSL handshake and negotiation and LDAP communications with the directory server through port 636.

If the test is successful, the SSL handshake and negotiation between iLO and the directory server were successful.

LDAP server certificate validation errors are reported in the results for this test.

**Bind to Directory Server**

This test binds the connection with the user name specified in the test controls. If no user is specified, iLO does an anonymous bind.

If the test is successful, the directory server accepted the binding.

**Directory Administrator Login**

If **Directory Administrator Distinguished Name** and **Directory Administrator Password** were specified, iLO uses these values to log in to the directory server as an administrator. Providing these values is optional.

**User Authentication**

iLO authenticates to the directory server with the specified user name and password.

If the test is successful, the supplied user credentials are correct.

If the test fails, the user name and/or password is incorrect.

**User Authorization**

This test verifies that the specified user name is part of the specified directory group, and is part of the directory search context specified during directory services configuration.

**Directory User Contexts**

If **Directory Administrator Distinguished Name** was specified, iLO tries to search the specified context.

If the test is successful, iLO found the context by using the administrator credentials to search for the container in the directory.

User login is the only way that you can test contexts that begin with the @ symbol.

A failure indicates that the container could not be located.

**LOM Object Exists**

This test searches for the iLO object in the directory server by using the **LOM Object Distinguished Name** configured on the **Security - Directory** page.

If the test is successful, iLO found the object that represents itself.

**CAC Smartcard Authentication**

A common access card (CAC) is a United States Department of Defense (DoD) smartcard for multifactor authentication. Common access cards are issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard, and eligible contractor personnel. In addition to its use as an ID card, a common access card is required for access to government buildings and computer networks.
Each CAC carries a smartcard certificate that must be associated with your local user account in the iLO web interface. Upload and associate your smartcard certificate with your account by using the controls on the Certificate Mappings page.

CAC authentication with LDAP directory support uses a service account to authenticate to the directory service, and the user account must be present in the same domain as the configured directory server. Additionally, the user account must be a direct member of the configured groups or extended schema Roles. Cross-domain authentication and nested groups are not supported.

Two-factor authentication

Part of the requirement necessary to satisfy Federal Government Certification is two-factor authentication. Two-factor authentication is the dual authentication of the CAC. For example, the CAC satisfies two-factor authentication by mandating that you have the physical card and you know the PIN number associated with the card. To support CAC authentication, your smartcard must be configured to require a PIN.

Configuring CAC smart card authentication settings

Prerequisites

- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: http://www.hpe.com/support/ilo-docs.
- Optional: Install the LDAP server CA certificates for directory integration.
- Optional: Configure LDAP directory integration in Directory Default Schema mode for directory integration.

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Install a trusted CA certificate.
   This certificate is used to validate certificates that are presented to iLO. The certificate must be compliant with the configured iLO security state.
3. Configure the Authentication Options:
   a. Enable CAC Smartcard Authentication.
   b. Optional: Enable CAC Strict Mode.
   This setting identifies which portion of your user certificate will be used to identify your directory user account.
5. To save the Authentication Options and Directory User Certificate Name Mapping setting, click the Apply button.
6. Optional: To import a Certificate Revocation List (CRL), enter a URL in the Revocation List URL box, and then click Apply.
   This step allows you to invalidate previously issued certificates that have been revoked.
   The CRL size limit is 100 KB and the CRL must be in DER format.
7. Optional: To check user certificates using the Online Certificate Status Protocol, enter an HTTP or HTTPS URL, and then click Apply.

8. **Upload and map a smart card certificate** to a local iLO user account (when using iLO with local user authentication only).

**CAC smart card authentication settings**

**Authentication Options**

**CAC Smartcard Authentication**

Enables and disables authentication through a common access smart card.

**CAC Strict Mode**

Enables or disables CAC Strict Mode, which requires a client certificate for every connection to iLO. When this mode is enabled, iLO will not accept user names or passwords when connecting, and only key-based authentication methods are allowed.

**NOTE:**

If you do not have a trusted certificate, you cannot access iLO. Attempts to browse to the iLO web interface will generate an error.

**Directory User Certificate Name Mapping**

**For Directory Username**

Allows you to select the portion of the user certificate to use as your directory user name:

- **Use Certificate SAN UPN**—Uses the first subject alternative name (SAN) field of type userPrincipalName (UPN), which contains the user and domain names in an email address format as the user name. For example, upn:testuser@domain.com produces testuser@domain.com.

- **Use Certificate Subject CN**—Uses only the CN or CommonName portion of the subject as the user name. For example, in the following DN: cn=test user, ou=users,dc=domain,dc=com the common name is test user.

- **Use Full Certificate Subject DN**—Uses the complete distinguished name as the user name when searching for the user in the directory service. For example, a distinguished name appears as follows: cn=test user, ou=users,dc=domain,dc=com.

- **Use Certificate SAN RFC822 Name**—Uses the first SAN field of type rfc822Name, which contains an email address as the username. For example, rfc822Name:testuser@domain.com produces testuser@domain.com as the username.

**OCSP Settings**

**OCSP URL**

If configured, user certificates provided for authentication are checked using the Online Certificate Status Protocol.

Only HTTP and HTTPS URLs are accepted.

A response of Unknown or Revoked caused authentication to fail.

**Managing trusted certificates for CAC Smartcard Authentication**
Importing a trusted CA certificate

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Paste a trusted CA certificate in the Direct Import section.
   The certificate must be in PEM encoded Base64 format.
3. Click Apply.
   If the operation does not appear to have worked, scroll to the top of the page to see if any error messages displayed.

Deleting a trusted CA certificate

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Scroll to the Manage Trusted CA Certificates section.
3. Select the check box next to the certificate to be deleted.
4. Click Delete.
   If the operation does not appear to have worked, scroll to the top of the page to see if any error messages displayed.

Importing a certificate revocation list (CRL) from a URL

To invalidate previously issued certificates that have been revoked, import a CRL.

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).
Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.

2. Type or paste a URL in the Import Revocation List section.
   The CRL size limit is 100 KB and the CRL must be in DER format.

3. Click Apply.
   The CRL is added to the Certificate Revocation List (CRL) section, which displays the CRL description and serial number.
   If the operation does not appear to have worked, scroll to the top of the page to see if any error messages displayed.

Deleting a certificate revocation list

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: http://www.hpe.com/support/ilo-docs.

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.

2. Scroll to the Certificate Revocation List (CRL) section.

3. Click Delete.

Certificate mapping

The Certificate Mappings page displays the local users of the system and their associated SHA-256 certificate thumbprints. Use the controls on this page to add or delete a certificate.

In a smartcard or CAC environment (configured on the CAC/Smartcard page), local users must have a smartcard certificate saved and mapped to their user account to allow smartcard access.

Authorizing a new local user certificate

Prerequisites

- Administer User Accounts privilege
- A smartcard or other CAC with an embedded certificate
  The certificate must be compliant with the configured iLO security state.
- CAC Smartcard Authentication is enabled on the CAC/Smartcard tab.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: http://www.hpe.com/support/ilo-docs.
Procedure

1. Click **Security** in the navigation tree, and then click the **Certificate Mappings** tab.
   iLO displays a list of local user accounts with their associated SHA-256 certificate thumbprints.

2. Select a user account by clicking the check box next to the **Login Name**.

3. Click **Authorize New Certificate**.
   The **Certificate Import Data** paste box appears.

4. Export the certificate for the selected user account in PEM encoded Base64 format.

5. Open the certificate in a text editor.

6. Copy the certificate, and then paste it in the **Certificate Import Data** box.

7. Click **Import Certificate**.

Deleting local user certificates

**Prerequisites**

- Administer User Accounts privilege
- One or more local user accounts with associated certificates exist on the system.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: [http://www.hpe.com/support/ilo-docs](http://www.hpe.com/support/ilo-docs).

Procedure

1. Click **Security** in the navigation tree, and then click the **Certificate Mappings** tab.
   iLO displays a list of local user accounts with their associated SHA-256 certificate thumbprints.

2. Select one or more local user accounts by clicking the check box next to the **Login Name**.

3. Click **Delete Selected Certificate(s)**.
   The certificates are immediately removed and the system displays the message **Certificate(s) deleted**.

Kerberos authentication with iLO

Kerberos support enables a user to log in to iLO by clicking the **Zero Sign In** button on the login page instead of entering a user name and password. To log in successfully, the client workstation must be logged in to the domain, and the user must be a member of a directory group for which iLO is configured. If the workstation is not logged in to the domain, the user can log in to iLO by using the Kerberos UPN and domain password.

Because a system administrator establishes a trust relationship between iLO and the domain before user sign-on, any form of authentication (including two-factor authentication) is supported. For information about configuring a user account to support two-factor authentication, see the server operating system documentation.
Configuring Kerberos authentication

Procedure

1. **Configure the iLO host name and domain name.**
2. **Install an iLO license to enable Kerberos Authentication.**
3. **Prepare the domain controller for Kerberos support.**
4. **Generate a Kerberos keytab file.**
5. **Verify that your environment meets the Kerberos authentication time requirement.**
6. **Configure Kerberos support in iLO**
7. **Configure supported browsers for single-sign-on**

Configuring the iLO hostname and domain name for Kerberos authentication

If a DHCP server does not supply the domain name or DNS servers you want to use:

Procedure

1. Click **iLO Dedicated Network Port** in the navigation tree.
2. Click the **IPv4** tab.
3. Clear the following check boxes, and then click **Submit**.
   - Use DHCPv4 Supplied Domain Name
   - Use DHCPv4 Supplied DNS Servers
4. Click the **IPv6** tab.
5. Clear the following check boxes, and then click **Submit**.
   - Use DHCPv6 Supplied Domain Name
   - Use DHCPv6 Supplied DNS Servers
6. Click the **General** tab.
7. Optional: Update the **iLO Subsystem Name (Hostname)**.
8. Update the **Domain Name**.
9. Click **Submit**.
10. To restart iLO, click **Reset**.
iLO hostname and domain name requirements for Kerberos authentication

- **Domain Name**—The iLO domain name value must match the Kerberos realm name, which is typically the domain name converted to uppercase letters. For example, if the parent domain name is `somedomain.net`, the Kerberos realm name is `SOMEDOMAIN.NET`.

- **iLO Subsystem Name (Hostname)**—The configured iLO hostname must be identical to the iLO hostname that you use when you generate the keytab file. The iLO hostname is case-sensitive.

Preparing the domain controller for Kerberos support

In a Windows Server environment, Kerberos support is part of the domain controller, and the Kerberos realm name is usually the domain name converted to uppercase letters.

**Procedure**

1. Create and enable computer accounts in the domain directory for each iLO system.
   
   Create the user account in the **Active Directory Users and Computers** snap-in. For example:

   - **iLO hostname**: `myilo`
   - **Parent domain name**: `somedomain.net`
   - **iLO domain name (fully qualified)**: `myilo.somedomain.net`

2. Ensure that a user account exists in the domain directory for each user who is allowed to log in to iLO.

3. Create universal and global user groups in the domain directory.

   To set permissions in iLO, you must create a security group in the domain directory. Users who log in to iLO are granted the sum of the permissions for all groups of which they are a member. Only universal and global user groups can be used to set permissions. Domain local groups are not supported.

Generating a keytab file for iLO in a Windows environment

**Procedure**

1. Use the **Ktpass.exe** tool to generate a keytab file and set the shared secret.

   For Windows Vista only: See Microsoft hotfix KB960830 and use `Ktpass.exe` version 6.0.6001.22331 or later.

2. Optional: Use the `Setspn` command to assign the Kerberos SPN to the iLO system.

3. Optional: Use the `Setspn -L <iLO name>` command to view the SPN for the iLO system.

   Verify that the **HTTP/myilo.somedomain.net** service is displayed.

**Ktpass**

**Syntax**

```
Ktpass [options]
```
Description
Ktpass generates a binary file called the keytab file, which contains pairs of service principal names and encrypted passwords for Kerberos authentication.

Parameters
+rndPass
  Specifies a random password.
-ptype KRB5_NT_SRV_HST
  The principal type. Use the host service instance (KRB5_NT_SRV_HST) type.
-princ <principal name>
  Specifies the case-sensitive principal name. For example, HTTP/myilo.somedomain.net@SOMEDOMAIN.net.
  • The service type must use uppercase letters (HTTP).
  • The iLO hostname must use lowercase letters (myilo.somedomain.net).
  • The REALM name must use uppercase letters (@SOMEDOMAIN.NET).
-mapuser <user account>
  Maps the principal name to the iLO system domain account.
-out <file name>
  Specifies the file name for the .keytab file.
-crypto <encryption>
  Specifies the encryption of the keys generated in the .keytab file.
  If iLO is configured to use the HighSecurity, FIPS, or CNSA security state, you must use an AES Kerberos key type.
kvno
  Override key version number.

!important:
Do not use this parameter. This option causes the kvno in the keytab file to be out of sync with the kvno in Active Directory.

Example command
Ktpass +rndPass -ptype KRB5_NT_SRV_HST -princ HTTP/myilo.somedomain.net@SOMEDOMAIN.NET -mapuser myilo$@somedomain.net -out myilo.keytab

Example output
Targeting domain controller: domaincontroller.example.net
Using legacy password setting method
Successfully mapped HTTP/iloname.example.net to iloname.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to myilo.keytab:
Keytab version: 0x502

HPE Gen10 security best practices 113
The `Ktpass` command might display a message about not being able to set the UPN. This result is acceptable because iLO is a service, not a user. You might be prompted to confirm the password change on the computer object. To close the window and continue creating the keytab file, click **OK**.

**Setspn**

**Syntax**

`Setspn [options]`

**Description**

The `Setspn` command displays, modifies, and deletes SPNs.

**Parameters**

- `-A <SPN>`
  
  Specifies an SPN to add.

- `-L`
  
  Lists the current SPN for a system.

**Example command**

`SetSPN -A HTTP/myilo.somedomain.net myilo`

The SPN components are case-sensitive. The primary (service type) must be in uppercase letters, for example, `HTTP`. The instance (iLO hostname) must be in lowercase letters, for example, `myilo.somedomain.net`.

The `SetSPN` command might display a message about not being able to set the UPN. This result is acceptable because iLO is a service, not a user. You might be prompted to confirm the password change on the computer object. Click **OK** to close the window and continue creating the keytab file.

**Verifying that your environment meets the Kerberos authentication time requirement**

For Kerberos authentication to function properly, the date and time must be synchronized between the iLO processor, the KDC, and the client workstation. Set the date and time in iLO with the server, or obtain the date and time from the network by enabling the SNTP feature in iLO.

**Procedure**

1. Verify that the date and time of the following are set to within 5 minutes of one another:
• The iLO date and time setting
• The client running the web browser
• The servers performing the authentication

Configuring Kerberos support in iLO

Procedure
1. Configure the iLO Kerberos-specific parameters.
2. Configure directory groups.

Configuring supported browsers for single sign-on

Users who are allowed to log in to iLO must be members of the groups for which permissions are assigned. For Windows clients, locking and unlocking the workstation refreshes the credentials that are used to log in to iLO. Home versions of the Windows operating system do not support Kerberos login.

The procedures in this section enable login if Active Directory is configured correctly for iLO, and iLO is configured correctly for Kerberos login.

Enabling single-sign-on in Internet Explorer

The following procedure is based on Internet Explorer 11. Other browser versions might have different steps.

Procedure
1. Enable authentication in Internet Explorer.
   a. Select Tools > Internet options.
   b. Click the Advanced tab.
   c. Scroll to the Security section.
   d. Verify that the Enable Integrated Windows Authentication option is selected.
   e. Click OK.
2. Add the iLO domain to the Intranet zone.
   a. Select Tools > Internet options.
   b. Click the Security tab.
   c. Click the Local intranet icon.
   d. Click the Sites button.
   e. Click the Advanced button.
   f. Enter the site to add in the Add this website to the zone box.
   g. On a corporate network, *.example.net is sufficient.
   h. Click Add.
   i. Click Close.
j. To close the Local intranet dialog box, click OK.
k. To close the Internet Options dialog box, click OK.

3. Enable the Automatic login only in Intranet zone setting.
   a. Select Tools > Internet options.
   b. Click the Security tab.
   c. Click the Local intranet icon.
   d. Click Custom level.
   e. Scroll to the User Authentication section.
   f. Verify that the Automatic logon only in Intranet zone option is selected.
   g. To close the Security Settings — Local Intranet Zone window, click OK.
   h. To close the Internet Options dialog box, click OK.

4. If any options were changed in steps 1–3, close and restart Internet Explorer.

5. Verify the single sign-on configuration.

Enabling single-sign on in Firefox

Procedure

1. Enter about:config in the browser location bar to open the browser configuration page.
   The message This might void your warranty! might be displayed.
2. If the message This might void your warranty! appeared, click I accept the risk! button.
3. Enter network.negotiate in the Search box.
5. Enter the iLO DNS domain name (for example, example.net), and then click OK.
6. Test the configuration. For more information, see Verifying the single sign-on (Zero Sign In) configuration on page 116.

Single-sign on with Chrome

Configuration is not required for Chrome.

Verifying the single sign-on (Zero Sign In) configuration

Procedure

1. Navigate to the iLO login page (for example, http://iloname.example.net).
2. Click the Zero Sign In button.
Verifying that login by name works

Procedure

1. Navigate to the iLO login page.
2. Enter the user name in the Kerberos UPN format (for example, user@EXAMPLE.NET).
3. Enter the associated domain password.
4. Click Log In.

Directory integration

Using a directory with iLO provides the following benefits:

- **Scalability**—The directory can be leveraged to support thousands of users on thousands of iLO processors.
- **Security**—Robust user-password policies are inherited from the directory. User-password complexity, rotation frequency, and expiration are policy examples.
- **User accountability**—In some environments, users share iLO accounts, which makes it difficult to determine who performed an operation.
- **Role-based administration** (HPE Extended Schema configuration)—You can create roles (for example, clerical, remote control of the host, complete control) and associate them with users or user groups. A change to a single role applies to all users and iLO devices associated with that role.
- **Single point of administration** (HPE Extended Schema configuration)—You can use native administration tools like MMC to administer iLO users.
- **Immediacy**—A single change in the directory rolls out immediately to associated iLO processors. This feature eliminates the need to script this process.
- **Simpler credentials**—You can use existing user accounts and passwords in the directory without having to record a new set of credentials for iLO.
- **Flexibility** (HPE Extended Schema configuration)—You can create a single role for a single user on a single iLO processor, a single role for multiple users on multiple iLO processors, or a combination of roles suited to your enterprise. With the HPE Extended Schema configuration, access can be limited to a time of day or a certain range of IP addresses.
- **Compatibility**—iLO directory integration supports Active Directory and OpenLDAP.
- **Standards**—iLO directory support is based on the LDAP 2.0 standard for secure directory access. iLO Kerberos support is based on LDAP v3.

Choosing a directory configuration to use with iLO

Before you configure iLO for directories, you must choose between the schema-free and HPE Extended Schema configuration options.

Consider the following questions:

1. **Can you apply schema extensions to your directory?**
   - **Yes**—Continue to question 2.
   - **No**—You are using Active Directory, and your company policy prohibits applying extensions.
No—You are using OpenLDAP. The HPE Extended Schema is not currently supported with OpenLDAP.
No—Directory integration with the HPE Extended Schema does not fit your environment.

Use group-based schema-free directory integration. Consider deploying an evaluation server to assess the benefits of directory integration with the HPE Extended Schema configuration.

2. Is your configuration scalable?
   The following questions can help you determine whether your configuration is scalable:

   • Are you likely to change the rights or privileges for a group of directory users?
   • Will you regularly script iLO changes?
   • Do you use more than five groups to control iLO privileges?

   Depending on your answer to these questions, choose from the following options:

   • No—Deploy an instance of the schema-free directory integration to evaluate whether this method meets your policy and procedural requirements. If necessary, you can deploy an HPE Extended Schema configuration later.
   • Yes—Use the HPE Extended Schema configuration.

Schema-free directory authentication

When you use the schema-free directory authentication option, users and groups reside in the directory, and group privileges reside in the iLO settings. iLO uses the directory login credentials to read the user object in the directory and retrieve the user group memberships, which are compared to the group configuration stored in iLO. If the directory user account is verified as a member of a configured iLO directory group, iLO login is successful.

Advantages of schema-free directory integration

• Extending the directory schema is not required.
• Minimal setup is required for users in the directory. If no setup exists, the directory uses existing users and group memberships to access iLO. For example, if you have a domain administrator named User1, you can copy the DN of the domain administrator security group to iLO and give it full privileges. User1 would then have access to iLO.

Disadvantage of schema-free directory integration

Group privileges are administered on each iLO system. This disadvantage has minimal impact because group privileges rarely change, and the task of changing group membership is administered in the directory and not on each iLO system. Hewlett Packard Enterprise provides tools that enable you to configure many iLO systems at the same time.

Schema-free configuration options

The schema-free setup options are the same, regardless of the method you use to configure the directory. You can configure the directory settings for minimum login flexibility, better login flexibility, or maximum login flexibility.
Minimum login flexibility

With this configuration, you can log in to iLO by entering your full DN and password. You must be a member of a group that iLO recognizes.

To use this configuration, enter the following settings:

- The directory server DNS name or IP address and LDAP port. Typically, the LDAP port for an SSL connection is 636.
- The DN for at least one group. This group can be a security group (for example, CN=Administrators,CN=Builtin,DC=HPE,DC=com for Active Directory, or UID=username,ou=People,dc=hpe,dc=com for OpenLDAP) or any other group, as long as the intended iLO users are group members.

Better login flexibility

With this configuration, you can log in to iLO by entering your login name and password. You must be a member of a group that iLO recognizes. At login time, the login name and user context are combined to make the user DN.

To use this configuration, enter the minimum login flexibility settings and at least one directory user context.

For example, if a user logs in as JOHN.SMITH, and the user context CN=USERS,DC=HPE,DC=COM is configured, iLO uses the following DN: CN=JOHN.SMITH,CN=USERS,DC=HPE,DC=COM.

Maximum login flexibility

With this configuration, you can log in to iLO by using your full DN and password, your name as it appears in the directory, the NetBIOS format (domain\login_name), or the email format (login_name@domain).

To use this configuration, configure the directory server address in iLO by entering the directory DNS name instead of the IP address. The DNS name must be resolvable to an IP address from both iLO and the client system.

Prerequisites for using schema-free directory integration

Procedure

1. Install Active Directory and DNS.
2. Install the root CA to enable SSL. iLO communicates with the directory only over a secure SSL connection.
   For information about using Certificate Services with Active Directory, see the Microsoft documentation.
3. Ensure that the directory DN of at least one user and the DN of a security group that contains that user are available. This information is used for validating the directory setup.
4. Install an iLO license that enables Directory Service Authentication.
5. Verify that the correct DNS server is specified on the iLO network settings IPv4 or IPv6 page.

Process overview: Configuring iLO for schema-free directory integration

Procedure

1. Configure the iLO schema-free directory parameters.
2. Configure directory groups.
Schema-free nested groups (Active Directory only)

Many organizations have users and administrators arranged in groups. This arrangement is convenient because you can associate a group with one or more iLO systems. You can update the configuration by adding or deleting group members.

Microsoft Active Directory supports placing one group in another group to create a nested group.

In a schema-free configuration, users who are indirect members (a member of a group that is a nested group of the primary group) are allowed to log in to iLO.

Nested groups are not supported when you use CAC Smartcard authentication.

HPE Extended Schema directory authentication

Using the HPE Extended Schema directory authentication option enables you to do the following:

- Authenticate users from a shared, consolidated, scalable user database.
- Control user privileges (authorization) by using the directory service.
- Use roles in the directory service for group-level administration of iLO management processors and iLO users.

Advantages of HPE Extended Schema directory integration

- Groups are maintained in the directory, not on each iLO.
- Flexible access control—Access can be limited to a time of day or a certain range of IP addresses.

Process overview: Configuring the HPE Extended Schema with Active Directory

Procedure

1. Plan

   Review the following:

   - Directory-enabled remote management
   - Directory services schema (See the iLO 5 user guide appendix Directory services schema for more information.)
   - Active Directory requirements for the HPE Extended Schema configuration

2. Install

   a. Install an iLO license to enable directory service authentication.

   b. Download the Directories Support for ProLiant Management Processors package and install the utilities required by your environment.

      You can install the Schema extender, snap-ins, and the Directories Support for ProLiant Management Processors utility.

   c. Run the Schema Extender to extend the schema.

   d. Install the appropriate snap-ins for your directory service on one or more management workstations.
3. Update

Set directory server settings and the DN of the management processor objects on the page in the iLO web interface.

You can also complete this step by using the Directories Support for ProLiant Management Processors software.

4. Manage roles and objects

a. Use the snap-ins to create a management device object and a role object.

b. Assign rights to the role object, as necessary, and associate the role with the management device object.

c. Add users to the role object.

5. Handle exceptions

The iLO utilities are easier to use with a single role. If you plan to create multiple roles in the directory, you might need to use directory scripting utilities, like LDIFDE or VBScript utilities. These utilities create complex role associations.

Prerequisites for configuring Active Directory with the HPE Extended Schema configuration

Procedure

1. Install Active Directory and DNS.

2. Install the root CA to enable SSL. iLO communicates with the directory only over a secure SSL connection.

For information about using Certificate Services with Active Directory, see the Microsoft documentation.

iLO requires a secure connection to communicate with the directory service. This connection requires the installation of the Microsoft CA. For more information, see the Microsoft Knowledge Base Article 321051: How to Enable LDAP over SSL with a Third-Party Certification Authority.

3. Before you install snap-ins and schema for Active Directory, read the following Microsoft Knowledge Base article: 299687 MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed.

Directory services support

iLO software is designed to run with the Microsoft Active Directory Users and Computers snap-in, enabling you to manage user accounts through the directory.

iLO supports Microsoft Active Directory with the HPE Extended Schema configuration.

Installing the iLO directory support software

Procedure


2. Install the .NET Framework 3.5 or later on the target server.

   The .NET Framework 3.5 or later is used to install the Directories Support for ProLiant Management Processors software.
3. Double-click the downloaded EXE file.

4. Click Next.

5. Select I accept the terms in the license agreement, and then click Next.

6. In the Directories Support window, click Schema Extender to install the schema extender software.
   a. In the Schema Extender setup wizard window, click Next.
   b. In the License Agreement window, select I Agree, and then click Next.
   c. In the Select Installation Folder window, select the installation directory and user preference, and then click Next.
   d. When prompted to confirm the installation request, click Next.

   The Installation Complete window opens.

   e. Click Close.

7. To install the snap-ins for your console, verify that the MMC Console is closed, and then click Snap-ins (x86) or Snap-ins (x64).
   a. In the snap-ins setup wizard window, click Next.
   b. In the License Agreement window, select I Agree, and then click Next.
   c. Read the details in the Information window, and then click Next.
   d. When prompted to confirm the installation request, click Next.

   The Installation Complete window opens.

8. To install the Directories Support for ProLiant Management Processors software, click Directories Support for ProLiant Management Processors.
   a. In the Welcome window, click Next.
   b. In the License Agreement window, select I Agree, and then click Next.
   c. In the Select Installation Folder window, select the installation directory and user preference, and then click Next.
   d. When prompted to confirm the installation request, click Next.

   The Installation Complete window opens.

   e. Click Close.

Directories Support for ProLiant Management Processors install options

- Schema Extender—The .xml files bundled with the Schema Extender contain the schemas that are added to the directory. Typically, one of these files contains a core schema that is common to all the supported directory services. The other files contain product-specific schemas. The schema installer requires the .NET Framework.

   You cannot run the schema installer on a domain controller that hosts Windows Server Core. For security and performance reasons, Windows Server Core does not use a GUI. To use the schema installer, you
must install a GUI on the domain controller or use a domain controller that hosts an earlier version of Windows.

- **Snap-ins (x86) or Snap-ins (x64)**—The management snap–in installer installs the snap-ins required to manage iLO objects in a Microsoft Active Directory Users and Computers directory or Novell ConsoleOne directory.

iLO snap-ins are used to perform the following tasks in creating an iLO directory:

- Creating and managing the iLO objects and role objects
- Making the associations between the iLO objects and the role objects

- **Directories Support for ProLiant Management Processors**—This utility allows you to configure Kerberos authentication and Directory services with iLO.

  The **HPLOMIG.exe** file, the required DLLs, the license agreement, and other files are installed in the **directory** `C:\Program Files (x86)\Hewlett Packard Enterprise\Directories Support for ProLiant Management Processors`. You can select a different directory. The installer creates a shortcut to Directories Support for ProLiant Management Processors on the **Start** menu.

  If the installation utility detects that the .NET Framework is not installed, it displays an error message and exits.

**Running the Schema Extender**

**Procedure**

1. Start the Management Devices Schema Extender from the Windows **Start** menu.

   - Windows 7 and Windows Server 2008—Click the Windows menu, and then select **All Programs > Hewlett-Packard Enterprise > Management Devices Schema Extender**.
   - For Windows 8 and Windows Server 2012—Click the Windows menu, and look for the **Management Devices Schema Extender**.
   - For Windows 10—Click the Windows menu, and then select **All apps > Hewlett-Packard Enterprise > Management Devices Schema Extender**.

2. Verify that **Lights Out Management** is selected, and then click **Next**.

3. Read the information in the **Preparation** window, and then click **Next**.

4. In the **Schema Preview** window, click **Next**.

5. In the **Setup** window, enter the following details:

   - Directory server type, name, and port.
   - Directory login information and SSL preference

The **Results** window displays the results of the installation, including whether the schema could be extended and what attributes were changed.
Schema Extender required information

Directory Server

- **Type**—The directory server type.
- **Name**—The directory server name.
- **Port**—The port to use for LDAP communications.

Directory Login

- **Login Name**—A user name to log in to the directory.

A directory user name and password might be required to complete the schema extension.

When you enter credentials, use the Administrator login along with the domain name, for example, Administrator@domain.com or domain\Administrator.

Extending the schema for Active Directory requires a user who is an authenticated schema administrator, that the schema is not write protected, and that the directory is the FSMO role owner in the tree. The installer attempts to make the target directory server the FSMO schema master of the forest.

- **Password**—A password to log in to the directory.
- **Use SSL for this Session**—Sets the form of secure authentication to be used. If this option is selected, directory authentication through SSL is used. If this option is not selected and Active Directory is selected, Windows authentication is used.

Directory services objects

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization allows the administrator to build relationships between the managed device and users or groups within the directory service. User management of iLO requires the following basic objects in the directory service:

- Lights-Out Management object
- Role object
- User objects

Each object represents a device, user, or relationship that is required for directory-based management.

After the snap-ins are installed, iLO objects and iLO roles can be created in the directory. By using the Active Directory Users and Computers tool, the user completes the following tasks:

- Creates iLO and role objects
- Adds users to the role objects
- Sets the rights and restrictions of the role objects

---

**NOTE:**

After the snap-ins are installed, restart ConsoleOne and MMC to show the new entries.
Directory-enabled remote management (HPE Extended Schema configuration)

This section is for administrators who are familiar with directory services and the iLO product and want to use the HPE schema directory integration option for iLO.

Directory-enabled remote management enables you to:

Create Lights-Out Management objects

You must create one LOM device object to represent each device that will use the directory service to authenticate and authorize users. You can use the Hewlett Packard Enterprise snap-ins to create LOM objects.

Hewlett Packard Enterprise recommends giving the LOM device objects meaningful names, such as the device network address, DNS name, host server name, or serial number.

Configure Lights-Out management devices

Every LOM device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. In general, you can configure each device with the appropriate directory server address, LOM object DN, and user contexts. The server address is the IP address or DNS name of a local directory server or, for more redundancy, a multihost DNS name.

Roles based on organizational structure

Often, administrators in an organization are placed in a hierarchy in which subordinate administrators must assign rights independently of ranking administrators. In this case, it is useful to have one role that represents the rights assigned by higher-level administrators, and to allow subordinate administrators to create and manage their own roles.

Using existing groups

Many organizations have users and administrators arranged in groups. In many cases, it is convenient to use the existing groups and associate them with one or more LOM role objects. When the devices are associated with the role objects, the administrator controls access to the Lights-Out devices associated with the role by adding or deleting members from the groups.

When you use Microsoft Active Directory, you can place one group within another (that is, use nested groups). Role objects are considered groups and can include other groups directly. Add the existing nested group directly to the role, and assign the appropriate rights and restrictions. You can add new users to either the existing group or the role.

When you use trustee or directory rights assignments to extend role membership, users must be able to read the LOM object that represents the LOM device. Some environments require that the trustees of a role also be read trustees of the object to authenticate users successfully.

Using multiple roles

Most deployments do not require that the same user must be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When users build multiple-role relationships, they receive all rights assigned by every applicable role. Roles can only grant rights, never revoke them. If one role grants a user a right, then the user has the right, even if the user is in another role that does not grant that right.

Typically, a directory administrator creates a base role with the minimum number of rights assigned, and then creates additional roles to add rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

For example, an organization might have two types of users: Administrators of the LOM device or host server, and users of the LOM device. In this situation, it makes sense to create two roles, one for the administrators and one for the users. Both roles include some of the same devices but grant different rights. Sometimes it is useful to assign generic rights to the lesser role and include the LOM administrators in that role, as well as the administrative role.
**Multiple roles (overlapping)** shows an example in which the Admin user gains the Login privilege from the User role, and advanced privileges are assigned through the Admin role.

![Diagram of overlapping roles](image)

*Figure 5: Multiple roles (overlapping)*

If you do not want to use overlapping roles, you could assign the Login, Virtual Power and Reset, and Remote Console privileges to the Admin role, and assign the Login privilege to the User role, as shown in **Multiple roles (separate)**.

![Diagram of separate roles](image)

*Figure 6: Multiple roles (separate)*

**How role access restrictions are enforced**

Two sets of restrictions can limit directory user access to LOM devices.

- **User access restrictions** limit user access to authenticate to the directory.
- **Role access restrictions** limit the ability of an authenticated user to receive LOM privileges based on rights specified in one or more roles.
User access restrictions

User address restrictions

Administrators can place network address restrictions on a directory user account. The directory server enforces these restrictions.

For information about the enforcement of address restrictions on LDAP clients, such as a user logging in to a LOM device, see the directory service documentation.

Network address restrictions placed on a user in a directory might not be enforced as expected when a directory user logs in through a proxy server. When a user logs in to a LOM device as a directory user, the LOM device attempts authentication to the directory as that user, which means that address restrictions placed on the user account apply when the user accesses the LOM device. When a proxy server is used, the network address of the authentication attempt is that of the LOM device, not that of the client workstation.

IPv4 address range restrictions

IP address range restrictions enable the administrator to specify network addresses that are granted or denied access.

The address range is typically specified in a low-to-high range format. An address range can be specified to grant or deny access to a single address. Addresses that fall within the low-to-high IP address range meet the IP address restriction.

IPv4 address and subnet mask restrictions

IP address and subnet mask restrictions enable the administrator to specify a range of addresses that are granted or denied access.

This format is similar to an IP address range restriction, but it might be more native to your networking environment. An IP address and subnet mask range is typically specified through a subnet address and address bit mask that identifies addresses on the same logical network.

In binary math, if the bits of a client machine address, combined with the bits of the subnet mask, match the subnet address in the restriction, the client meets the restriction.

DNS-based restrictions

DNS-based restrictions use the network name service to examine the logical name of the client machine by looking up machine names assigned to the client IP addresses. DNS restrictions require a functional name server. If the name service goes down or cannot be reached, DNS restrictions cannot be matched and the client machine fails to meet the restriction.
DNS-based restrictions can limit access to a specific machine name or to machines that share a common domain suffix. For example, the DNS restriction www.example.com matches hosts that are assigned the domain name www.example.com. However, the DNS restriction *.example.com matches any machine that originates from the example company.

DNS restrictions might cause ambiguity because a host can be multihomed. DNS restrictions do not necessarily match one to one with a single system.

Using DNS-based restrictions might create security complications. Name service protocols are not secure. Any individual who has malicious intent and access to the network can place a rogue DNS service on the network and create a fake address restriction criterion. When implementing DNS-based address restrictions, consider your organizational security policies.

**User time restrictions**

Time restrictions limit the ability of a user to log in (authenticate) to the directory. Typically, time restrictions are enforced using the time at the directory server. If the directory server is located in a different time zone, or if a replica in a different time zone is accessed, time-zone information from the managed object can be used to adjust for relative time.

The directory server evaluates user time restrictions, but the determination might be complicated by time-zone changes or the authentication mechanism.

**Role access restrictions**

Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users who have dynamic rights that can change based on the time of day or network address of the client.

When directories are enabled, access to an iLO system is based on whether the user has read access to a role object that contains the corresponding iLO object. This includes, but is not limited to, the members listed in the role object. If the role is configured to allow inheritable permissions to propagate from a parent, members of the parent that have read access privileges will also have access to iLO.

To view the access control list, navigate to Active Directory Users and Computers, open the Properties page for the role object, and then click the Security tab. The Advanced View must be enabled in MMC to view the Security tab.

**Role-based time restrictions**

Administrators can place time restrictions on LOM roles. Users are granted the rights specified for the LOM devices listed in the role only if they are members of the role and meet the time restrictions for the role.

Role-based time restrictions can be met only if the time is set on the LOM device. LOM devices use local host time to enforce time restrictions. If the LOM device clock is not set, the role-based time restriction fails unless no time restrictions are specified for the role. The time is normally set when the host is booted.
The time setting can be maintained by configuring SNTP, which allows the LOM device to compensate for leap years and minimize clock drift with respect to the host. Events, such as unexpected power loss or flashing LOM firmware, can cause the LOM device clock not to be set. The host time must be correct for the LOM device to preserve the time setting across firmware flashes.

Role-based address restrictions

The LOM firmware enforces role-based address restrictions based on the client IP network address. When the address restrictions are met for a role, the rights granted by the role apply.

Address restrictions can be difficult to manage when access is attempted across firewalls or through network proxies. Either of these mechanisms can change the apparent network address of the client, causing the address restrictions to be enforced in an unexpected manner.

Multiple restrictions and roles

The most useful application of multiple roles is restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables the administrator to create arbitrary, complex rights relationships with a minimum number of roles.

For example, an organization might have a security policy in which LOM administrators are allowed to use the LOM device from within the corporate network, but can reset the server only after regular business hours.

Directory administrators might be tempted to create two roles to address this situation, but extra caution is required. Creating a role that provides the required server reset rights and restricting it to after hours might allow administrators outside the corporate network to reset the server, which is contrary to most security policies.

Creating restrictions and roles shows a security policy that dictates that general use is restricted to clients in the corporate subnet, and server reset capability is restricted to after hours.

![Diagram of role-based access restrictions](image)

**Figure 9: Creating restrictions and roles**

Alternatively, the directory administrator might create a role that grants the login right and restrict it to the corporate network, and then create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because ongoing administration might create another role that grants the login right to users from addresses outside the corporate network. This role might unintentionally grant the LOM administrators in the server reset role the ability to reset the server from anywhere, if they satisfy the role time constraints.

The configuration shown in **Creating restrictions and roles** meets corporate security requirements. However, adding another role that grants the login right can inadvertently grant server reset privileges from outside the corporate subnet after hours. A more manageable solution is to restrict the Reset role and the General Use role, as shown in **Restricting the Reset and General Use roles**.
Tools for configuring multiple iLO systems at a time

Configuring large numbers of LOM objects for Kerberos authentication and directory services is time consuming. You can use the following utilities to configure several LOM objects at a time.

Directories Support for ProLiant Management Processors

This software includes a GUI that provides a step-by-step approach to configuring Kerberos authentication and directory services with large numbers of management processors. Hewlett Packard Enterprise recommends using this tool when you want to configure several management processors.

Traditional import utilities

Administrators familiar with tools such as LDIFDE or the NDS Import/Export Wizard can use these utilities to import or create LOM device directory objects. Administrators must still configure the devices manually, but can do so at any time. Programmatic or scripting interfaces can be used to create LOM device objects in the same way as users or other objects. For information about attributes and attribute data formats when you are creating LOM objects, see the Directory services schema.

User login using directory services

The Login Name box on the iLO login page accepts directory users and local users. The maximum length of the login name is 39 characters for local users and 127 characters for directory users. When you connect through the diagnostics port (on a blade server), Zero Sign In and directory user login are not supported and you must use a local account.

Directory users

The following formats are supported:

- LDAP fully distinguished names (Active Directory and OpenLDAP)
  Example: CN=John Smith,CN=Users,DC=HPE,DC=COM or @HPE.com
  The short form of the login name does not notify the directory which domain you are trying to access. Provide the domain name or use the LDAP DN of your account.

- DOMAIN\username format (Active Directory)
  Example: HPE\jsmith

- username@domain format (Active Directory)
  Example: jsmith@hpe.com
Directory users specified using the @ searchable form might be located in one of three searchable contexts, which are configured on the Directory page.

- Username format (Active Directory)
  Example: John Smith
  Directory users specified using the username format might be located in one of three searchable contexts, which are configured on the Directory page.

Local users
Enter the Login Name of your iLO local user account.

UEFI, passwords, and the Trusted Platform Module

The UEFI System Utilities includes a wide range of security options, giving fine control of server security options, such as power-on and administrator password control. Along with other options to increase security, such as TLS/HTTPS, Trusted Platform Module settings, and so on, UEFI can also be swapped over to a backup ROM in case of corruption or tampering.

Server Security options

- Set Power On Password
- Set Admin Password
- Secure Boot Settings
- TLS (HTTPS) Options
- Trusted Platform Module options
- Intel (R) TXT Support
- One-Time Boot Menu (F11 Prompt)
- System Intrusion Detection
- Backup ROM Image Authentication

Setting the power-on password

Use the Set Power On Password option to set a password for accessing the server during the boot process. When you are powering on the server, a prompt appears where you enter the password to continue. To disable or clear the password, enter the password followed by a / (slash) when prompted to enter the password.

NOTE:
In the event of an Automatic Server Recovery (ASR) reboot, the power-on password is bypassed and the server boots normally.
Procedure


2. Enter your password.
   A password can be:
   - 31 characters maximum
   - Any combination of numbers, letters, and special characters

3. Confirm the password and press Enter.
   A message appears confirming that the password is set.

4. Save your changes.

5. Reboot the server.

Setting an administrator password

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Set Admin Password.

2. Enter the password.
   A password can be:
   - 31 characters maximum
   - Any combination of numbers, letters, and special characters

3. Confirm the password and press Enter.
   A message appears confirming that the password is set.

4. Save your changes.

5. Reboot the server.

Secure Boot

Secure Boot is a server security feature that is implemented in the BIOS and does not require special hardware. Secure Boot ensures that each component launched during the boot process is digitally signed and that the signature is validated against a set of trusted certificates embedded in the UEFI BIOS. Secure Boot validates the software identity of the following components in the boot process:

- UEFI drivers loaded from PCIe cards
- UEFI drivers loaded from mass storage devices
- Preboot UEFI Shell applications
- OS UEFI boot loaders

When Secure Boot is enabled:
• Firmware components and operating systems with boot loaders must have an appropriate digital signature to execute during the boot process.

• Operating systems must support Secure Boot and have an EFI boot loader signed with one of the authorized keys to boot. For more information about supported operating systems, see http://www.hpe.com/servers/ossupport.

You can customize the certificates embedded in the UEFI BIOS by adding or removing your own certificates, either from a management console directly attached to the server, or by remotely connecting to the server using the iLO Remote Console.

You can configure Secure Boot:

• Using the System Utilities options described in the following sections.

• Using the iLO RESTful API to clear and restore certificates. For more information, see the Hewlett Packard Enterprise website (http://www.hpe.com/info/redfish).

• Using the secboot command in the Embedded UEFI Shell to display Secure Boot databases, keys, and security reports.

Enabling or disabling Secure Boot

Prerequisite
To enable this option:

• Set Boot Mode to UEFI Mode.

• Enable UEFI Optimized Boot.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Attempt Secure Boot.

2. Select a setting.

   • Enabled—Enables Secure Boot.
   • Disabled—Disables Secure Boot.

3. Save your changes.

4. Reboot the server.

Configuring Trusted Platform Module options

Trusted Platform Modules are computer chips that securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM to store platform measurements to make sure that the platform remains trustworthy. For servers configured with a Trusted Platform Module, TPM enables the firmware and operating system to take measurements of all phases of the boot process. For information on installing and enabling the TPM module option, see the user documentation for your server model.

When enabling the Trusted Platform module, observe the following guidelines:
• By default, the Trusted Platform Module is enabled as TPM 2.0 when the server is powered on after installing it.

• In UEFI Mode, the Trusted Platform Module can be configured to operate as TPM 2.0 or TPM 1.2.

• In Legacy Boot Mode, the Trusted Platform Module configuration can be changed between TPM 1.2 and TPM 2.0, but only TPM 1.2 operation is supported.

⚠️ CAUTION:

An OS that is using TPM might lock all data access if you do not follow proper procedures for modifying the server and suspending or disabling TPM in the OS. This includes updating system or option firmware, replacing hardware such as the system board and hard drive, and modifying TPM OS settings. Changing the TPM mode after installing an OS might cause problems, including loss of data.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Trusted Platform Module options.

2. Select an option. On servers configured with an optional TPM, you can set the following:

   • **TPM 2.0 Operation**—Sets the operation of TPM 2.0 to execute after a reboot. Options are:
     - No Action—There is no TPM configured.
     - Clear—TPM is cleared during reboot, and **TPM 2.0 Operation** is set to No Action.

   • **TPM Mode Switch**—Sets the TPM mode to execute after a reboot. Options are:
     - No Action
     - TPM 1.2
     - TPM 2.0

   • **TPM 2.0 Visibility**—Sets whether TPM is hidden from the operating system. Options are:
     - Visible
     - Hidden—Hides TPM from the operating system. Use this setting to remove TPM options from the system without having to remove the actual hardware.

   • **TPM UEFI Option ROM Measurement**—Enables or disables (skips) measuring UEFI PCI operation ROMs. Options are:
     - Enabled
     - Disabled

3. Save your changes.

4. Reboot the system.
After the system reboots, you can view the **Current TPM Type** and **Current TPM State** settings.

5. Verify that your new **Current TPM Type** and **Current TPM State** settings appear at the top of the screen.

### Advanced Secure Boot Options

- **PK - Platform Key**—Establishes a trust relationship between the platform owner and the platform firmware.
- **KEK - Key Exchange Key**—Protects the signature database from unauthorized modifications. No changes can be made to the signature database without the private portion of this key.
- **DB - Allowed Signatures Database**—Maintains a secure boot allowed signature database of signatures that are authorized to run on the platform.
- **DBX - Forbidden Signatures Database**—Maintains a secure boot blacklist signature database of signatures that are not authorized to run on the platform.
- **DBT - Timestamp Signatures Database**—Maintains signatures of codes in the timestamp signatures database.
- **Delete all keys**
- **Export all keys**
- **Reset all keys to platform defaults**

**NOTE:**
Changing the default security certificates can cause the system to fail booting from some devices. It can also cause the system to fail launching certain system software such as Intelligent Provisioning.

### Viewing Advanced Secure Boot Options settings

**Procedure**

1. From the **System Utilities** screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options**.
2. Select an exchange key or a signatures database option.
3. Select the **View** entry for the exchange key or signatures database option.
4. Select the entry for the option you want to view.

**Example: Viewing HPE UEFI Secure Boot 2016 PK Key details**

From the **System Utilities** screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > PK - Platform Key > View PK entry > HPE UEFI Secure Boot 2016 PK Key.**
Enrolling a Secure Boot certificate key or database signature

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Select Enroll <option name>.
4. Select Enroll <option name> using file.
   The File Explorer screen shows attached media devices.
5. Select the attached media device where the certificate file is located and press Enter.
6. Continue selecting the menu path for the certificate file. Press Enter after each selection.
7. (Optional) Select a Signature Owner GUID.
8. (Optional) If you selected Other for the signature owner GUID, enter a Signature GUID.
   Use the following format (36 characters): 11111111-2222-3333-4444-1234567890ab
   • For Hewlett Packard Enterprise certificates, enter F5A96B31-DBA0-4faa-A42A-7A0C9832768E
   • For Microsoft certificates, enter 77fa9abd-0359-4d32-bd60-28f4e78f784b
   • For SUSE certificates, enter 2879c886-57ee-45cc-b126-f92f24f906b9
9. Select Commit changes and exit.

Example: Enrolling a KEK entry

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > KEK - Key Exchange Key > Enroll KEK entry.
2. Select Enroll KEK using file.
3. Select the location of the certificate file from an attached media device.
4. (Optional) Select a Signature Owner GUID.
5. (Optional) If you selected Other for the signature owner GUID, enter a Signature GUID.
6. Select Commit changes and exit.

Deleting a Secure Boot certificate key or database signature

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Do one of the following.
• If there is one option available for deletion:
  a. Select the Delete <option name> check box.
  b. Click Yes.

• If there is more than one option available for deletion:
  a. Select Delete <option name>.
  b. Select the check box for the option you want to delete.
  c. Click Yes.

Example: Deleting a KEK entry

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > KEK - Key Exchange Key > Delete KEK entry.
2. Select the check box for the entry you want to delete.
3. Click Yes.

Deleting all keys

The Delete all keys option deletes all keys in the system, including the Platform Key.

IMPORTANT:

After you delete all keys, the system is forced to immediately disable Secure Boot. Secure Boot remains disabled upon system reboot until valid secure boot keys are restored.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > Delete all keys.
2. Press Enter to delete all keys.
3. Confirm the deletion.

Exporting a Secure Boot certificate key or database signature

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Select Export <option name>.
4. Select the entry you want to export.
Example: Exporting an Allowed Signatures Database signature

2. Select the entry you want to export.
3. Do one of the following.
   • Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press Enter after each selection.
   • To export to a new file, press +, and enter a file name.

Exporting all Secure Boot certificate keys

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > Export all keys.
2. Do one of the following.
   • Select an attached media device where you want to export the files, and then continue selecting the menu path for the certificate file. Press Enter after each selection.
   • To export to a new file, press +, and enter a file name.

Resetting a Secure Boot certificate key or database signature to platform defaults

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Select Reset to platform defaults.
4. Click Yes.
Resetting all Secure Boot certificate keys to platform defaults

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > Reset all keys to platform defaults.
2. Click Yes.

TLS (HTTPS) Options

Viewing TLS certificate details

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > View Certificates.
2. Select a certificate.

Enrolling a TLS certificate

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Enroll Certificate.
2. Select Enroll certificate using File Explorer.
   The File Explorer screen shows attached media devices.
3. Select the attached media device where the certificate file is located and press Enter.
4. Continue selecting the menu path for the certificate file. Press Enter after each selection.
5. Select Commit changes and exit.

Deleting a TLS certificate

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Delete Certificate.
2. From the list of certificates, select the certificates you want to delete.
3. Select Commit changes and exit.

Deleting all TLS certificates

The Delete all Certificates option deletes all certificates in the system.
Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Delete all Certificates.

2. Press Enter.

3. Confirm the deletion.

Exporting a TLS certificate

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Export Certificate.

2. Select a file format for the exported certificate.

A File Explorer screen shows attached media devices.

3. Do one of the following.

   • Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press Enter after each selection.

   • To export to a new file, press +, and enter a file name.

Exporting all TLS certificates

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Export all Certificates.

A File Explorer screen shows attached media devices.

2. Do one of the following.

   • Select an attached media device where you want to export the files, and then continue selecting the menu path for the certificate file. Press Enter after each selection.

   • To export to a new file, press +, and enter a file name.

Resetting all TLS settings to platform defaults

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Reset all settings to platform defaults.

2. Click OK.
Configuring advanced TLS security settings

Procedure


2. Configure options.

   • To configure which cipher suites are allowed for TLS connections:
     a. Select Cipher suites allowed for TLS connections.
     b. Select one of the following:
        ◦ Individual check boxes for the cipher suites you want to allow.
        ◦ Select Platform Default Cipher suites
     c. Select Commit changes and exit.

   • To configure the certificate validation process for every TLS connection:
     a. Select Certificate validation process for every TLS connection.
     b. Select a setting:
        ◦ PEER (recommended)—The certificate presented by the peer is validated for secure communication.
        ◦ NONE—Does not validate the certificate.

   • To enable or disable strict host name checking:
     a. Select Strict Hostname checking.
     b. Select a setting:
        ◦ ENABLE—The host name of the connected server is validated with the host name in the certificate supplied by the server.
        ◦ DISABLE—The host name of the connected server is not validated with the host name in the certificate supplied by the server.

   • To specify which protocol version to use for TLS connections:
     b. Select a setting:
- **AUTO**—Negotiates the highest protocol version that is supported by both the TLS server and the client.
- **1.0**—Uses TLS protocol version 1.0.
- **1.1**—Uses TLS protocol version 1.1.
- **1.2**—Uses TLS protocol version 1.2.

3. Save your changes.

**Enabling or disabling Intel TXT support**

Use the Intel TXT Support option to enable or disable Intel TXT (Trusted Execution Technology) support for servers with Intel processors that support this feature.

**NOTE:**
Intel TXT is supported in both TPM 2.0 and TPM 1.2 modes.

**Prerequisites**
Before you can enable Intel TXT support, you must enable:

- All Intel processor cores
- Hyperthreading
- VT-d
- TPM

Disabling any of these features while TXT is enabled can prevent TXT from working properly.

**NOTE:**
A physical TPM is always enabled, discoverable, and working by default.

**Procedure**

1. From the **System Utilities** screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intel (R) TXT Support**.
2. Select a setting.
   - **Enabled**—Enables TXT support
   - **Disabled**—Disables TXT support.
3. Save your changes.

**Enabling or disabling the One-Time Boot Menu F11 prompt**

Use this option to control whether you can press the F11 key to boot directly to the One-Time Boot Menu during the current boot. This option does not modify the normal boot order settings. When this option is
enabled, you can boot directly into the One-Time Boot Menu in the System Utilities by pressing F11 in the POST screen after a server reboot.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > One-Time Boot Menu (F11 Prompt).
2. Select a setting.
   - Enabled
   - Disabled
3. Save your changes.

Enabling or disabling processor AES-NI support

Use the Processor AES-NI option to enable or disable the Advanced Encryption Standard Instruction Set in the processor.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Processor AES-NI Support.
2. Select a setting.
   - Enabled—Enables AES-NI support.
   - Disabled—Disables AES-NI support.
3. Save your changes.

Enabling or disabling backup ROM image authentication

Use the Backup ROM Image Authentication option to enable or disable cryptographic authentication of the backup ROM image on startup.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Backup ROM Image Authentication.
2. Select a setting.
   - Enabled—The backup ROM image is authenticated on startup.
   - Disabled—The backup ROM image is not authenticated on startup. Only the primary image is authenticated.
3. Save your changes.
Managing firmware, OS software, and language packs

Special procedures previously required for updating firmware in iLO 5 v1.10 and SUM 8.0 are no longer needed. For specific procedures for managing firmware, OS software, and language packs, see the following guides (available on the HPE Information Library):

- Smart Update Manager 8.1.0 User Guide
- HPE iLO 5 User Guide
- Intelligent Provisioning User Guide for HPE ProLiant Gen10 Servers and HPE Synergy
- HPE iLO 5 Scripting and Command Line Guide

Firmware updates

Firmware updates enhance server and iLO functionality with new features, improvements, and security updates.

You can update firmware by using an online or offline firmware update method.

Online firmware update

When you use an online method to update firmware, you can perform the update without shutting down the server operating system. Online firmware updates can be performed in-band or out-of-band.

In-band

Firmware is sent to iLO from the server host operating system.

The iLO 5 Channel Interface Driver is required for in-band firmware updates.

During a host-based firmware update, if iLO is set to the Production security state, it does not verify user credentials or privileges. The host-based utilities require a root (Linux and VMware) or Administrator (Windows) login.

When iLO is configured to use the HighSecurity, FIPS, or CNSA security states, user credentials are required.

An error message is displayed if you do not have the required user privileges when you use HPONCFG version 5.2.0 or later with iLO 5 1.20 or later.

The iLO Online ROM Flash Component and HPONCFG are examples of online in-band firmware update methods.

Out-of-band

Firmware is sent to iLO over a network connection. Users with the Configure iLO Settings privilege can update firmware by using an out-of-band method. If the system maintenance switch is set to disable iLO security, any user can update firmware with an out-of-band method.

The iLO web interface, HPQLOCFG, HPLOMIG, the iLO RESTful API, LOCFG.PL, and SMASH CLP are examples of online out-of-band firmware update methods.

Online firmware update methods

In-band firmware updates

- **Online ROM Flash Component**—Use an executable file to update firmware while the server is running. The executable file contains the installer and the firmware package.

  You can download online ROM flash components for iLO and server firmware at the following website: [http://www.hpe.com/support/ilo5](http://www.hpe.com/support/ilo5).
This option is supported when iLO is configured to use the Production security state.

- **HPONCFG**—Use this utility to update firmware by using XML scripts. Download the iLO or server firmware image and the `Update_Firmware.xml` sample script. Edit the sample script with your setup details, and then run the script.

  Sample scripts are available at [http://www.hpe.com/support/ilo5](http://www.hpe.com/support/ilo5). For more information about scripting, see the iLO scripting and CLI guide.

  When iLO is configured to use the CNSA security state, only HPONCFG for Linux is supported.

### Out-of-band firmware updates

- **iLO web interface**—Download a supported firmware file and install it by using the iLO web interface. You can update firmware for a single server or an iLO Federation group.

- **iLO RESTful API**—Use the iLO RESTful API and a REST client such as the RESTful Interface Tool to update firmware.

  For more information, see [http://www.hpe.com/info/restfulinterface/docs](http://www.hpe.com/info/restfulinterface/docs).

- **HPQLOCFG**—Use this utility to update firmware by using XML scripts. Download the iLO or server firmware image and the `Update_Firmware.xml` sample script. Edit the sample script with your setup details, and then run the script.

  Sample scripts are available at [http://www.hpe.com/support/ilo5](http://www.hpe.com/support/ilo5). For more information about scripting, see the iLO scripting and CLI guide.

- **HPLOMIG** (also called Directories Support for ProLiant Management Processors)—You do not need to use directory integration to take advantage of the HPLOMIG firmware update capabilities. HPLOMIG can be used to discover multiple iLO processors and update their firmware in one step.

- **SMASH CLP**—Access SMASH CLP through the SSH port, and use standard commands to view firmware information and update firmware.

  For more information about SMASH CLP, see the iLO scripting and CLI guide.

### Offline firmware update

When you use an offline method to update the firmware, you must reboot the server by using an offline utility. The SPP, SUM, the Scripting Toolkit for Windows, and the Scripting Toolkit for Linux are examples of offline firmware update methods.

#### Offline firmware update methods

You can use the following offline firmware update methods:

- **SPP**

  Use the SPP to install firmware. For more information, see the following website: [http://www.hpe.com/info/spp/documentation](http://www.hpe.com/info/spp/documentation).

- **SUM**

  SUM is a tool for firmware, driver, and software maintenance on supported servers and other nodes.

  You can use SUM together with iLO to access the iLO Repository and manage install sets and the installation queue.
Scripting Toolkit

Use the Scripting Toolkit to configure several settings within the server and update firmware. This method is useful for deploying to multiple servers. For instructions, see the Scripting Toolkit user guide for Windows or Linux.
Operating system security provisioning

**Intelligent Provisioning, UEFI, and server boot security**

HPE Gen10 systems offer a variety of ways to securely configure, deploy, and boot operating systems.

**Available methods of operating system deployment**

Administrators can use the following methods of operating system deployment for HPE Gen10 ProLiant servers:

- Intelligent Provisioning offers a wide range of security settings and includes options for deploying an operating system to the server.


- Secure boot over PXE (configured in UEFI settings) to a network installation image.

  See the *UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy* or the *UEFI Deployment Guide for HPE ProLiant Gen10 Servers and HPE Synergy* in the HPE Information Library for more information about the PXE settings: [http://www.hpe.com/info/ProLiantUEFI/docs](http://www.hpe.com/info/ProLiantUEFI/docs).
Lifecycle security

Updates and patches
Updates and patches are made available for Gen10 ProLiant servers over the life of the hardware, allowing HPE to continue to increase the reliability and security of server firmware in an ongoing manner.

Secure decommissioning

Using Secure Erase
Intelligent Provisioning provides secure erase functionality for the internal system storage and hard disks following the guidelines outlined in DoD 5220.22-M. Secure erase overwrites all block devices attached to the system through applying random patterns in a three-pass process. These block devices include hard disks, storage systems attached to the server, as well as the internal storage used by iLO. Depending on the amount of storage installed on a system, the secure erase process can take many hours or even days to complete.

⚠️ CAUTION:

- Secure Erase should be used with extreme caution, and only when a system is being decommissioned. The secure erase process resets iLO and deletes all licenses stored there, resets BIOS settings in many cases, and deletes all AHS and warranty data stored on the system. The secure erase process also deletes any deployment settings profiles. iLO reboots multiple times after the process is complete.

- Disconnect any FCoE, iSCSI, external SAS, and Fibre Channel storage before using secure erase, unless they should also be erased.

Securely erasing server data
Access Intelligent Provisioning in one of two ways:

- Press F10 during the server POST
- In iLO 5, click Intelligent Provisioning and then click Always On

Procedure

1. Click Perform Maintenance.
2. Click System Erase and Reset.
3. Select the devices to be erased.
4. Click Submit.

NOTE:

Hard Drive Secure Erases may take hours, or, for larger drives, days to complete. This is expected behavior for this thorough erase procedure. Erases using the guidelines from DoD 5220.22-M Date Wipe. Erase NAND requires an iLO license.
System Erase and Reset options

The following table includes the options in the System Erase and Reset menu and a description of what selecting each option will do.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All hard drives</td>
<td>Erase all hard drives on this server.</td>
</tr>
<tr>
<td>Wipe hard drives</td>
<td>Displays if All Hard Drives is selected.</td>
</tr>
<tr>
<td></td>
<td>Writes a data pattern over all sectors. This will take several hours per hard drive.</td>
</tr>
<tr>
<td>Secure Erase of Non-Volatile Storage¹</td>
<td>Triggers a secure hardware erase of all user and warranty information. This may take up to 24 hours and cannot be aborted until it completes.</td>
</tr>
<tr>
<td>Intelligent Provisioning Preferences</td>
<td>Clear Intelligent Provisioning preferences.</td>
</tr>
</tbody>
</table>

¹ Erases using the guidelines from DoD 5220.22-M Data Wipe.

iLO Backup & Restore

The Backup & Restore feature allows you to restore the iLO configuration on a system with the same hardware configuration as the system that was backed up. This feature is not meant to duplicate a configuration and apply it to a different iLO system.

In general, it is not expected that you will need to perform an iLO restore operation. However, there are cases in which having a backup of the configuration eases and expedites the return to a normal operating environment.

As with any computer system, backing up your data is a recommended practice to minimize the impact from failures. Hewlett Packard Enterprise recommends performing a backup each time that you update the iLO firmware.

You might want to restore the iLO configuration in the following situations:

**Battery failure or removal**

Various configuration parameters are stored in the battery-powered SRAM. Although rare, the battery can fail. In some situations, battery removal and replacement might be required. To avoid the loss of configuration information, restore the iLO configuration from a backup file after the battery is replaced.

**Reset to factory defaults**

In some cases, you might need to reset iLO to the factory default settings to erase settings external to iLO. Resetting iLO to the factory default settings erases the iLO configuration. To recover the iLO configuration quickly, restore the configuration from a backup file after the reset to the factory default settings is complete.
**Accidental or incorrect configuration change**

In some cases, the iLO configuration might be changed incorrectly, causing important settings to be lost. This situation might occur if iLO is set to the factory default settings or user accounts are deleted. To recover the original configuration, restore the configuration from a backup file.

**System board replacement**

If a system board replacement is required to address a hardware issue, you can use this feature to transfer the iLO configuration from the original system board to the new system board.

**Lost license key**

If a license key is accidentally replaced, or you reset iLO to the factory default settings, and you are not sure which key to install, you can restore the license key and other configuration settings from a backup file.
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.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>• Control <strong>access to the appliance</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Allow HPE Services access</td>
</tr>
<tr>
<td></td>
<td>◦ Disable access to the Hardware setup feature so that an installation technician can not access the console</td>
</tr>
<tr>
<td>Accounts</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• If local accounts are used, protect the built-in administrator account with a strong password.</td>
</tr>
<tr>
<td></td>
<td>• Do not use the built-in Administrator account. All users must login using their own credentials to facilitate auditing.</td>
</tr>
<tr>
<td>Audit logs</td>
<td>Download the appliance audit logs at regular intervals.</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Topic</th>
<th>Best Practice</th>
</tr>
</thead>
</table>
| Certificates | • Use certificates signed by a trusted certificate authority (CA). 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.  
  The appliance supports self-signed certificates and certificates signed by a CA.  
  The appliance is initially configured with self-signed certificates for the web server and the State Change Message Bus (SCMB).  
  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, or through another trusted CA.  
  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.  
  ◦ 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, then 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.  
  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.  
  See Use a certificate authority on page 187.                                                                                                                                                                                                                                                                                                                                                      |
<table>
<thead>
<tr>
<th>Topic</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network</strong></td>
<td>- 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).</td>
</tr>
<tr>
<td></td>
<td>◦ <strong>Management LAN</strong></td>
</tr>
<tr>
<td></td>
<td>Grant management LAN access to authorized personnel only. For example, Infrastructure administrators, Network administrators, and Server administrators.</td>
</tr>
<tr>
<td></td>
<td>◦ <strong>Production LAN</strong></td>
</tr>
<tr>
<td></td>
<td>Connect all NICs for managed devices to the production LAN.</td>
</tr>
<tr>
<td></td>
<td>- Do not connect management systems (for example, the Composer, the iLO) directly to the Internet.</td>
</tr>
<tr>
<td></td>
<td>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 &quot;Preparing for remote support registration&quot; or &quot;Configure the proxy settings&quot; in the online help for more information.</td>
</tr>
<tr>
<td><strong>Passwords</strong></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- The appliance maintenance console uses a local administrator account. Hewlett Packard Enterprise recommends that you set a password for appliance maintenance console access.</td>
</tr>
<tr>
<td><strong>Permissions</strong></td>
<td>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 <em>HPE OneView Online help</em>.</td>
</tr>
<tr>
<td></td>
<td>◦ <strong>Role:</strong> 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 &quot;About user roles&quot; in the online help.</td>
</tr>
<tr>
<td></td>
<td>◦ <strong>Scope:</strong> 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.</td>
</tr>
</tbody>
</table>
HPE OneView supports two-factor authentication. Deploy **two-factor authentication** for increased security.

**Updates**
- Sign up for HPE OneView bulletins at: [http://www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
- Install updates for all components in your environment on a regular basis.

**Managed Environment**
- 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.

### Understanding the security features of HPE OneView

HPE OneView runs on a dedicated HPE Synergy Composer (management software embedded into the hardware). HPE OneView is configured to be fully secure out-of-the-box.

**High-level overview**

- **Security-hardened appliance** on page 175
- **Best practices for maintaining a secure appliance** on page 151
- **Nonbrowser clients** on page 193

**User access and authentication**

- **About complex passwords** on page 155
- **About directory service authentication** on page 155
- **Authentication for appliance access** on page 177
- **Controlling access for authorized users** on page 182
- **Creating a login session** on page 177
- **Specifying user accounts and roles** on page 182
- **Protecting credentials** on page 184

**Console access**

- **Controlling access to the appliance console** on page 195

**Certificates**

- **Two-factor Authentication** on page 178
- **Managing certificates from a browser** on page 186
- **Certificate management** on page 216

**Learn more**

- **Algorithms for securing the appliance** on page 196
- **Ports required for HPE OneView** on page 193
- **Files you can download from the appliance** on page 201
- **Understanding the audit log** on page 184
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.

About directory service authentication

You can use an external enterprise directory service (EDS) to authenticate and provide single sign-on to individual users or user groups. An enterprise directory is a requirement for using two-factor authentication. Each user in a group is assigned the same role (for example, Infrastructure administrator). An example of an enterprise directory is a corporate directory that uses Active Directory or LDAP (Lightweight Directory Access Protocol). Active Directory is required for two-factor authentication.

After the directory service is configured, any user in the group can log in to the appliance (or use a smart card and PIN, if two-factor authentication is enabled).

If logging in with a *user name* and *password*, on the login window, a user:

- Enters their *user name* (typically, the Common-Name attribute, CN).
  
  The format for the *user name* depends on the Directory type.

- Enters their *password*.

- Selects the enterprise directory service.

If authentication using a smart card, a user:

- Inserts their smart card in a smart card reader.

- Selects their certificate when prompted by the browser.

- Enters their *PIN*.

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.

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 users’ sessions are ended when such modifications are made.

Authenticating users

When you add an enterprise directory service to the appliance, you provide location criteria so that the appliance can find the group.

If two-factor authentication is enabled, you create a service account that the appliance uses to access the authentication directory when validating a security certificate from a smart card.
Adding a directory server

If you replicate the enterprise directory service for high availability or disaster tolerance, add the replicated directory service as a separate directory service.

After configuring and adding a directory server, you can designate it as the default directory service.

When you add a new directory with a different server for which the certificate is not trusted, a prompt is generated for trusting the root CA. Additionally, an alert is generated when an upgraded directory configuration has a missing certificate chain or an imported root CA. If the root CA certificate you imported is a X509 v1 type certificate, it is treated as a self-signed certificate and when the CRL is uploaded the certificate is treated as a CA certificate.

After you add an enterprise directory service and server

You can:

Add a group, which had already been defined in the directory service, so that all its members can login on the appliance.

Allow local logins only, which is the default.

Allow both local logins and logins for user accounts authenticated by the directory service.

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.

Considerations for configuring a Microsoft Active Directory directory service

- The following maps the Active Directory attribute to the LDAP property:

<table>
<thead>
<tr>
<th>LDAP property</th>
<th>Active Directory attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>Common-Name</td>
</tr>
<tr>
<td>uid</td>
<td>UID</td>
</tr>
<tr>
<td>userPrincipalName</td>
<td>User-Principal-Name</td>
</tr>
<tr>
<td>sAMAccountName</td>
<td>SAM-Account-Name</td>
</tr>
</tbody>
</table>

If the user name does not contain either an @ character (to denote a UPN) or a \ character (to denote domain\login), then these logins are attempted in this order:

1. The user name is treated as the sAMAccountName and directory-name gets prepended as (directory-name\user-name)

2. The user name is treated as a UID.

3. The user name is treated as a CN.

- 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’s name, displayed here with the corresponding attribute:
<table>
<thead>
<tr>
<th>User name component</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>givenName</td>
</tr>
<tr>
<td>Initials</td>
<td>initial</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
</tr>
</tbody>
</table>

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

\[ \text{givenName}.initials.givenName.initial.sn \]

In the **New Object – user** dialog box, you are also required to specify a **User logon name**. This, 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:

\[ \text{LogonName}@DNSDomain \]

For example:

*JoeUser@exampledomain.example.com*

- Finally, as you enter the **User logon name**, the first twenty 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.

**About emergency local login**

When configured to use a directory service, administrators can choose to disable local logins for improved security. If the 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 4.0 version, 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 155.
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 174 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.

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.

**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**

<table>
<thead>
<tr>
<th>Role</th>
<th>Type of user</th>
<th>Permissions or privileges</th>
</tr>
</thead>
</table>
| **Full**        | Infrastructure administrator | View, create, edit, or remove resources managed or monitored by the appliance, including management of the appliance, through the UI or using REST APIs.  
An Infrastructure administrator can also manage information provided by the appliance in the form of activities, notifications, and logs.  
Only an Infrastructure administrator can restore an appliance from a backup file. |
| **Read only**   | Read only          | View managed or monitored resource information.                                            
Cannot add, create, edit, remove, or delete resources. |
| **Specialized** | Backup administrator | Create and download backup files, view the appliance settings and activities.               
Has the authority to use scripts to log in to the appliance and run scripts to back up the appliance.  
Cannot restore the appliance from a backup file. |
| **Network**     | Network administrator | View, create, edit, or remove networks, network sets, connections, interconnects, uplink sets, and firmware bundles.  
View related activities, logs, and notifications.  
Cannot manage user accounts. |

**NOTE:**

This role is specifically 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.

Hewlett Packard Enterprise recommends that users with this role should not initiate interactive login sessions through the HPE OneView user interface.
<table>
<thead>
<tr>
<th>Role</th>
<th>Type of user</th>
<th>Permissions or privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server administrator</strong></td>
<td>View, create, edit, or remove server profiles and templates, network sets, enclosures, and firmware bundles. Access the physical servers. View connections, networks, racks, power, and related activities, logs, and notifications. Add volumes, but cannot add storage pools or storage systems. Cannot manage user accounts.</td>
<td></td>
</tr>
<tr>
<td><strong>Server firmware operator</strong></td>
<td>View managed or monitored resource information. Access the physical servers. Edit, but not create or delete, physical servers. Edits the server hardware, firmware baseline, firmware installation method and activation schedule values on server profiles.</td>
<td></td>
</tr>
<tr>
<td><strong>Server profile architect</strong></td>
<td>Create and manage server profiles, server profile templates, storage volumes, labels, and network sets. Use networks, enclosures, firmware drivers, server hardware, storage pools, and storage volume templates.</td>
<td></td>
</tr>
<tr>
<td><strong>Server profile administrator</strong></td>
<td>Create and manage server profiles, storage volumes, labels, and network sets. Use networks, enclosures, firmware drivers, server hardware, server profile templates, storage pools, and storage volume templates.</td>
<td></td>
</tr>
<tr>
<td><strong>Server profile operator</strong></td>
<td>Create, delete, and update labels. Update server hardware, and server profiles Use networks, network sets, enclosures, firmware drivers, server hardware, server profiles, storage pools, and storage volume templates.</td>
<td></td>
</tr>
<tr>
<td><strong>Scope administrator</strong></td>
<td>Create and delete scopes. Update scopes, add and remove scope resources. Cannot modify any resource other than scopes.</td>
<td></td>
</tr>
<tr>
<td><strong>Scope operator</strong></td>
<td>Update scopes, add and remove scope resources. Cannot modify any resource other than scopes. Cannot create or delete scopes.</td>
<td></td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Role</th>
<th>Type of user</th>
<th>Permissions or privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage administrator</td>
<td>View, add, edit, or remove storage systems.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View, add, or remove storage pools.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View, create, edit, add, or delete volumes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View, create, edit, or delete volume templates.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View, add, or edit SAN managers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View or edit SANs.</td>
<td></td>
</tr>
<tr>
<td>Software Administrator</td>
<td>Creates and modifies Image Streamer artifacts like plan scripts, build plans, and deployment plans.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assigns a golden image for deployment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performs a capture from a web server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performs all the actions pertaining to the artifact bundles.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can perform activities like appliance restart, shutdown, update firmware, backup, restore, and activate standby.</td>
<td></td>
</tr>
<tr>
<td>HardwareSetup</td>
<td>A credential-less login for data center technicians that allows them to verify cabling of HPE Synergy hardware and fix alerts related to first time setup of hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installs HPE Synergy hardware, verifies cabling, and uses HP OneView to verify minimum operation.</td>
<td></td>
</tr>
</tbody>
</table>

**Action privileges for user roles**

The following table lists 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**

<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA</td>
<td>Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td>Server admin</td>
<td>Network admin</td>
</tr>
<tr>
<td>activities</td>
<td>CRUD</td>
</tr>
<tr>
<td>alerts</td>
<td>RUD</td>
</tr>
<tr>
<td>appliance</td>
<td>CRUD</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Category</th>
<th>IA</th>
<th>Server admin</th>
<th>Network admin</th>
<th>Backup admin</th>
<th>Storage admin</th>
<th>Software admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>artifact-bundles</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>audit logs</td>
<td>CR</td>
<td>R</td>
<td>R</td>
<td>—</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>backups</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>CRD</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>certificates</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>community string</td>
<td>RU</td>
<td>R</td>
<td>CRU</td>
<td>—</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>connections</td>
<td>CRUD</td>
<td>R</td>
<td>CR</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>connection templates</td>
<td>CRUD, Use</td>
<td>R, Use</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>console users</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>data centers</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>debug logs</td>
<td>CRUD</td>
<td>CRU</td>
<td>CRU</td>
<td>—</td>
<td>R</td>
<td>CRU</td>
</tr>
<tr>
<td>deployed-targets</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>deployment-clusters</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>deployment-groups</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>deployment-managers</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>device bays</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>domains</td>
<td>CRUD</td>
<td>R</td>
<td>CRU</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>drive enclosures</td>
<td>CRUD</td>
<td>CRUD, Use</td>
<td>R, Use</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>enclosures</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>enclosure groups</td>
<td>CRUD, Use</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Ethernet networks</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Category</td>
<td>Action privileges for user roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>IA</strong></td>
<td><strong>Server admin</strong></td>
<td><strong>Network admin</strong></td>
<td><strong>Backup admin</strong></td>
<td><strong>Storage admin</strong></td>
<td><strong>Software admin</strong></td>
</tr>
<tr>
<td>events</td>
<td>CRU</td>
<td>CRU</td>
<td>CRU</td>
<td>—</td>
<td>R</td>
<td>CRU</td>
</tr>
<tr>
<td>fabrics</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC aliases</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>FC device managers</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>FC endpoints</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC networks</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FCOE networks</td>
<td>CRUD, Use</td>
<td>R</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC ports</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC providers</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC SANs</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>FC SAN services</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>FC switches</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC tasks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC zones</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>firmware drivers</td>
<td>CRUD</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>global settings</td>
<td>CRUD</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>CRUD</td>
</tr>
<tr>
<td>golden- images</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>golden- volumes</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>grouptorole mappings</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>hardware setup</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>hosts</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

_Table Continued_
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator</td>
</tr>
<tr>
<td></td>
<td>(C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td></td>
<td>IA</td>
</tr>
<tr>
<td>host clusters</td>
<td>CRUD</td>
</tr>
<tr>
<td>i3s- maintenance-services</td>
<td>CRUD</td>
</tr>
<tr>
<td>i3s-volume-services</td>
<td>CRUD</td>
</tr>
<tr>
<td>ID range ipv4</td>
<td>CRUD</td>
</tr>
<tr>
<td>ID range ipv4 subnet</td>
<td>CRUD</td>
</tr>
<tr>
<td>ID range vmacs (MAC addresses)</td>
<td>CRUD</td>
</tr>
<tr>
<td>ID range vsns (serial numbers)</td>
<td>CRUD</td>
</tr>
<tr>
<td>ID range vwwns (World Wide Names)</td>
<td>CRUD</td>
</tr>
<tr>
<td>infrastructure vms</td>
<td>CRUD</td>
</tr>
<tr>
<td>integrated tools</td>
<td>CRUD</td>
</tr>
<tr>
<td>interconnects</td>
<td>CRUD</td>
</tr>
<tr>
<td>interconnect types</td>
<td>R, Use</td>
</tr>
<tr>
<td>labels</td>
<td>CRUD</td>
</tr>
<tr>
<td>licenses</td>
<td>CRUD</td>
</tr>
<tr>
<td>logical downlinks</td>
<td>R</td>
</tr>
<tr>
<td>logical enclosures</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>logical interconnects</td>
<td>RU, Use</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Category</th>
<th>IA</th>
<th>Server admin</th>
<th>Network admin</th>
<th>Backup admin</th>
<th>Storage admin</th>
<th>Software admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>logical interconnects groups</td>
<td>CRUD, Use</td>
<td>R, Use</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>login domains</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>login sessions</td>
<td>CRUD</td>
<td>RU</td>
<td>RU</td>
<td>RU</td>
<td>RU</td>
<td>—</td>
</tr>
<tr>
<td>managed SANs</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R</td>
<td>CRUD, Use</td>
<td>—</td>
</tr>
<tr>
<td>migratable VC domains</td>
<td>CRUD, Use</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>R</td>
</tr>
<tr>
<td>networks</td>
<td>CRUD, Use</td>
<td>R, Use</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>network sets</td>
<td>CRUD, Use</td>
<td>CRUD¹</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>notifications</td>
<td>CRUD</td>
<td>CRD</td>
<td>CRD</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>oe-build- plans</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>oe-deployment-plans</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>organizations</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>os-volumes</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>plan-scripts</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>ports</td>
<td>RU, Use</td>
<td>—</td>
<td>RU, Use</td>
<td>—</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>power devices</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>racks</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>reports</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>repository manager</td>
<td>CRUD</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>restores</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td>IA</td>
<td>Server admin</td>
</tr>
<tr>
<td>role</td>
<td>CRUD</td>
</tr>
<tr>
<td>SANS</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>SAN manager</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>SAS interconnects</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>SAS logical interconnect groups</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>SAS logical interconnects</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>scopes</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>server hardware</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>server hardware types</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>server profiles</td>
<td>CRUD</td>
</tr>
<tr>
<td>server profile templates</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>stateless- servers</td>
<td>CRUD</td>
</tr>
<tr>
<td>storage pools</td>
<td>CRD</td>
</tr>
<tr>
<td>storage systems</td>
<td>CRUD</td>
</tr>
<tr>
<td>storage target ports</td>
<td>CRUD</td>
</tr>
<tr>
<td>storage volumes</td>
<td>CRUD</td>
</tr>
<tr>
<td>storage volume attachments</td>
<td>CRUD</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for user roles</th>
<th>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</th>
<th>IA</th>
<th>Server admin</th>
<th>Network admin</th>
<th>Backup admin</th>
<th>Storage admin</th>
<th>Software admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage volumes</td>
<td></td>
<td></td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>templates</td>
<td></td>
<td></td>
<td>CRUD, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>support</td>
<td></td>
<td></td>
<td>CRUD, Use</td>
<td>RU</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>switches</td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>tasks</td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>trap forwarding</td>
<td></td>
<td></td>
<td>RU</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>unmanaged devices</td>
<td></td>
<td></td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>update</td>
<td></td>
<td></td>
<td>R</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>uplink sets</td>
<td></td>
<td></td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>users</td>
<td></td>
<td></td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>user preferences</td>
<td></td>
<td></td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

1 Server administrators cannot edit bandwidths.

**Table 3: Action privileges for specialized user roles**

<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
<th>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</th>
<th>Read only</th>
<th>Scope admin</th>
<th>Scope operator</th>
<th>Server firmware operator</th>
<th>Server profile architect</th>
<th>Server profile admin</th>
<th>Server profile operator</th>
<th>Hardware setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>activities</td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRU</td>
</tr>
<tr>
<td>alerts</td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>RUD</td>
</tr>
<tr>
<td>appliance</td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>artifact-bundles</td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Category</td>
<td>Action privileges for specialized user roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator</td>
<td>(C=Create, R=Read, U=Update, D=Delete, Use)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Read only</th>
<th>Scope admin</th>
<th>Scope operator</th>
<th>Server firmware operator</th>
<th>Server profile architect</th>
<th>Server profile admin</th>
<th>Server profile operator</th>
<th>Hardware setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit logs</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>backups</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>certificates</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>community string</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>connections</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>connection templates</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>console users</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>data centers</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>debug logs</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>deployed-targets</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>deployment clusters</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>deployment groups</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>deployment managers</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>device bays</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>domains</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>drive enclosures</td>
<td>R</td>
<td>R, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>enclosures</td>
<td>R</td>
<td>R, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>enclosure groups</td>
<td>R</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>—</td>
</tr>
<tr>
<td>Ethernet networks</td>
<td>R</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td>—</td>
</tr>
<tr>
<td>events</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CR</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
<th>IA=Infrastructure administrator, admin=administrator</th>
<th>(C=Create, R=Read, U=Update, D=Delete, Use)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read only</td>
<td>Scope admin</td>
<td>Scope operator</td>
</tr>
<tr>
<td>fabrics</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC aliases</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC device managers</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC endpoints</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC networks</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>FCOE networks</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>FC ports</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC providers</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC SANs</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC SAN services</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC switches</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC tasks</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC zones</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>firmware drivers</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>global settings</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>golden-images</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>golden-volumes</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>group or role mappings</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>hardware setup</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>hosts</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Category</td>
<td>Read only</td>
<td>Scope admin</td>
<td>Scope operator</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>host clusters</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>i3s-maintenance-services</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>i3s-volume-services</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>ID range ipv4</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>ID range ipv4 subnet</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>ID range vmacs (MAC addresses)</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>ID range vsns (serial numbers)</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>ID range vwwn (World Wide Names)</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>infrastructure vms</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>integrated tools</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>interconnects</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>interconnect types</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>labels</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>licenses</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>logical downlinks</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>logical enclosures</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA=Infrastructure administrator, admin=administrator</td>
<td>(C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td></td>
<td>Read only</td>
</tr>
<tr>
<td>logical interconnects</td>
<td>R</td>
</tr>
<tr>
<td>logical interconnect groups</td>
<td>R</td>
</tr>
<tr>
<td>logical switch groups</td>
<td>R</td>
</tr>
<tr>
<td>login domains</td>
<td>R</td>
</tr>
<tr>
<td>login sessions</td>
<td>RU</td>
</tr>
<tr>
<td>managed SANs</td>
<td>R</td>
</tr>
<tr>
<td>migratable VC domains</td>
<td>—</td>
</tr>
<tr>
<td>networks</td>
<td>R</td>
</tr>
<tr>
<td>network sets</td>
<td>R</td>
</tr>
<tr>
<td>notifications</td>
<td>R</td>
</tr>
<tr>
<td>oe-build-plans</td>
<td>R</td>
</tr>
<tr>
<td>oe-deployment-plans</td>
<td>R</td>
</tr>
<tr>
<td>organizations</td>
<td>R</td>
</tr>
<tr>
<td>os-volumes</td>
<td>R</td>
</tr>
<tr>
<td>plan-scripts</td>
<td>R</td>
</tr>
<tr>
<td>ports</td>
<td>—</td>
</tr>
<tr>
<td>power devices</td>
<td>R</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
<th>WA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read only</td>
<td>Scope admin</td>
</tr>
<tr>
<td>racks</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>reports</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>repository manager</td>
<td>—</td>
<td>R</td>
</tr>
<tr>
<td>restores</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>roles</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>SANs</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>SAN manager</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>SAS interconnects</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>SAS logical interconnects groups</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>SAS logical interconnects</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>scopes</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>server hardware</td>
<td>R</td>
<td>R, Use</td>
</tr>
<tr>
<td>server hardware types</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>server profiles</td>
<td>R</td>
<td>R, Use</td>
</tr>
<tr>
<td>server profile templates</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>stateless-servers</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>storage pools</td>
<td>R</td>
<td>R, Use</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator</td>
</tr>
<tr>
<td></td>
<td>(C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td></td>
<td>Read只读</td>
</tr>
<tr>
<td>storage systems</td>
<td>R</td>
</tr>
<tr>
<td>storage target ports</td>
<td>R</td>
</tr>
<tr>
<td>storage volumes</td>
<td>R</td>
</tr>
<tr>
<td>storage volume attachments</td>
<td>R</td>
</tr>
<tr>
<td>storage volume templates</td>
<td>R</td>
</tr>
<tr>
<td>support</td>
<td>—</td>
</tr>
<tr>
<td>switches</td>
<td>R</td>
</tr>
<tr>
<td>switch domains</td>
<td>R</td>
</tr>
<tr>
<td>switch groups</td>
<td>R</td>
</tr>
<tr>
<td>tasks</td>
<td>R</td>
</tr>
<tr>
<td>trap forwarding</td>
<td>R</td>
</tr>
<tr>
<td>unmanaged devices</td>
<td>R</td>
</tr>
<tr>
<td>update</td>
<td>R</td>
</tr>
<tr>
<td>uplink sets</td>
<td>R</td>
</tr>
<tr>
<td>users</td>
<td>R</td>
</tr>
<tr>
<td>user preferences</td>
<td>R</td>
</tr>
</tbody>
</table>

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

**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 Servers

**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 are sent.

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.

---

**Security-hardened appliance**

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

- Some examples of best-practice security hardening used within HPE OneView on HPE Synergy Composer are:
  - The appliance uses a customized operating system that eliminates all non-essential services in order 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 graphical user interface)
    - 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 completely 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 firmware image of the HPE Synergy Composer is digitally signed by Hewlett Packard Enterprise. When re-imaging the Composer in order to quickly bring it to a specific firmware revision level, the digital signature is verified by the re-imaging process. This ensures the authenticity and integrity of the image.

• 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.
• HPE OneView supports **Service console access** which enables an Hewlett Packard Enterprise. Support representative to obtain, with customer permission, a one-time password for privileged access to the appliance in order to perform advanced diagnostics.

• 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.

- Two-factor login: You can configure the appliance to perform smart card 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**.

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 card 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

- **Two-factor Authentication** on page 178

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/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 is as follows:

1. The user types 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 set up 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.

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:

```
```

**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 pass phrase>` with the actual pass phrase. 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 \[ CN=(^[a-zA-Z]*, [a-zA-Z]+$) \]
- 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:
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

The appliance enables SSO (single sign-on) to iLO without storing user-created iLO credentials. The following table describes the mapping of roles between the appliance and iLO.

<table>
<thead>
<tr>
<th>Appliance role</th>
<th>SSO to iLO roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure administrator</td>
<td>Admin</td>
</tr>
<tr>
<td>Server administrator</td>
<td>Admin</td>
</tr>
</tbody>
</table>
### 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.

### Mapping appliance interactions with iLO and iPDU

The appliance performs configurations on the iLO 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](#).

<table>
<thead>
<tr>
<th>Protocol or interaction</th>
<th>Description</th>
<th>iLO</th>
<th>iPDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>Configures NTP</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>Enables and configures SNMP to collect information</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>Enables and configures SNMP traps sent to appliance</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTTPS (RIBCL/SOAP/JSON)</td>
<td>Collects information (the specific protocol varies, but all use TLS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Console</td>
<td>Links from the UI to the iLO Remote Console</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Not used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Not used</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table Continued*
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 appliance 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 the remote access to the appliance via SSH.

NOTE:
SSH access must be enabled to access the serial console CLI. The serial console CLI is used to access unmanaged interconnects.

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.

Understanding the 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:

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/time</td>
<td>The date and time of the event</td>
</tr>
<tr>
<td>Internal component ID</td>
<td>The unique identifier of an internal component</td>
</tr>
<tr>
<td>Reserved</td>
<td>The organization ID. Reserved for internal use</td>
</tr>
<tr>
<td>User domain</td>
<td>The login domain name of the user</td>
</tr>
<tr>
<td>User name/ID</td>
<td>The user name</td>
</tr>
<tr>
<td>Session ID</td>
<td>The user session ID associated with the message</td>
</tr>
<tr>
<td>Task ID</td>
<td>The URI of the task resource associated with the message</td>
</tr>
<tr>
<td>Client host/IP</td>
<td>The client (browser) IP address identifies the client machine that initiated the request</td>
</tr>
<tr>
<td>Result</td>
<td>The result of the action, which can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• SUCCESS</td>
</tr>
<tr>
<td></td>
<td>• FAILURE</td>
</tr>
<tr>
<td></td>
<td>• SOME_FAILURES</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td></td>
<td>• KILLED</td>
</tr>
<tr>
<td>Action</td>
<td>A description of the action, which can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• ADD</td>
</tr>
<tr>
<td></td>
<td>• MODIFY</td>
</tr>
<tr>
<td></td>
<td>• DELETE</td>
</tr>
<tr>
<td></td>
<td>• ACCESS</td>
</tr>
<tr>
<td></td>
<td>• RUN</td>
</tr>
<tr>
<td></td>
<td>• LIST</td>
</tr>
<tr>
<td></td>
<td>• ENABLE</td>
</tr>
<tr>
<td></td>
<td>• DISABLE</td>
</tr>
<tr>
<td></td>
<td>• SAVE</td>
</tr>
<tr>
<td></td>
<td>• SETUP</td>
</tr>
<tr>
<td></td>
<td>• UNSETUP</td>
</tr>
<tr>
<td></td>
<td>• DEPLOY</td>
</tr>
<tr>
<td></td>
<td>• START</td>
</tr>
<tr>
<td></td>
<td>• DONE</td>
</tr>
<tr>
<td></td>
<td>• KILLED</td>
</tr>
<tr>
<td></td>
<td>• CANCELED</td>
</tr>
<tr>
<td></td>
<td>• LOGIN</td>
</tr>
<tr>
<td></td>
<td>• LOGOUT</td>
</tr>
<tr>
<td></td>
<td>• DOWNLOAD_S</td>
</tr>
<tr>
<td></td>
<td>• START_TART</td>
</tr>
</tbody>
</table>
## Token Description

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>A description of the severity of the event, which can be one of the following values, listed in descending order of importance:</td>
</tr>
<tr>
<td></td>
<td>• INFO</td>
</tr>
<tr>
<td></td>
<td>• NOTICE</td>
</tr>
<tr>
<td></td>
<td>• WARNING</td>
</tr>
<tr>
<td></td>
<td>• ERROR</td>
</tr>
<tr>
<td></td>
<td>• ALERT</td>
</tr>
<tr>
<td></td>
<td>• CRITICAL</td>
</tr>
<tr>
<td>Resource category</td>
<td>For REST API category information, see the <em>HPE OneView API Reference</em>.</td>
</tr>
<tr>
<td>Resource URI/name</td>
<td>The resource URI/name associated with the task</td>
</tr>
<tr>
<td>Message</td>
<td>The output message that appears in the audit log</td>
</tr>
</tbody>
</table>

### Maintenance console entries

The audit log includes entries for all Maintenance console events except for viewing.

### 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 191

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 188.

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, Import an appliance certificate on page 190.

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 188.

**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
   ```
2. Using the new key pair, create a Certificate Signing Request (CSR) for the client certificate.
   This command creates a CSR using data input via interactive prompts:
   ```
   openssl req -new -key cert.key -out cert.csr
   ```
   The Common Name for this command must be set to "rabbitmq_readonly", since the SCMB server is configured to accept connections from this user. Otherwise, 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:

```plaintext
[ 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. Please 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:

```plaintext
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.

```plaintext
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
```

Any active connections to the SCMB server will break and need to be reestablished 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 the troubleshooting steps in "Unable to connect to the SCMB server using a CA-signed client certificate" in the online help.

**Import an appliance certificate**

After sending a certificate signing request to the CA and receiving a certificate, you must import it.

**Prerequisites**

- Privileges: Infrastructure administrator.
- Ensure that no other users are logged in to the appliance.
Procedure

1. From the main menu, select **Settings**.
2. Click **Security**.
3. Select **Actions > Import certificate**.
4. Copy the certificate text and paste it into the box provided.
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.

**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 on **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 via 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. An SSH connection using other authorized HPE OneView accounts can be used to access the command line interface (CLI) for connecting to serial consoles of Synergy devices.

Ports required for HPE OneView

HPE OneView requires specific ports to be available to the appliance to manage servers, enclosures, and interconnects.
<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Inbound and Outbound</td>
<td>Used for SSH and SFTP. SSH is required to communicate with interconnect modules. SFTP is required for actions such as firmware upgrades and support dumps.</td>
</tr>
<tr>
<td>53</td>
<td>UDP and TCP</td>
<td>Outbound</td>
<td>Used for DNS client queries.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Inbound</td>
<td>Used for the HTTP interface. Typically, this port redirects to port 443; this port provides the access required by the iLO.</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Inbound</td>
<td>HPE OneView acts as an NTP server, iLO requires access.</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Outbound</td>
<td>Used as an NTP client to synchronize the appliance time.</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>Outbound</td>
<td>Supports SNMP GET calls to obtain status data from a server through iLO. Also used for iPDU.</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>Inbound and Outbound for trap forwarding from HPE OneView</td>
<td>Used for SNMP trap support from the iLO, and iPDU devices. This port is also used to monitor the VC interconnects and trap forwarding.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Inbound</td>
<td>Used for the HTTPS interface to user interface and APIs.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Outbound</td>
<td>Used for secure SSL access to the iLO, Frame link module, remote support access to Hewlett Packard Enterprise, and other devices. Used for Redfish, RIBCL, SOAP, and iPDU communication.</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>Outbound</td>
<td>Secure LDAP. Used for enterprise directory integration (Microsoft Active Directory, OpenLDAP)</td>
</tr>
<tr>
<td>2162</td>
<td>UDP</td>
<td>Inbound</td>
<td>Used as an alternative SNMP trap port.</td>
</tr>
<tr>
<td>3269</td>
<td>TCP</td>
<td>Outbound</td>
<td>Used for Microsoft Active directory LDAP global catalog port.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>Inbound</td>
<td>Allows external scripts or applications to connect to and monitor messages from the SCMB (State-Change Message Bus).</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17988</td>
<td>TCP</td>
<td>iLO Integrated Remote Console to iLO</td>
<td>Integrated Remote Console initiating a connection to the iLO.</td>
</tr>
<tr>
<td>17990</td>
<td>TCP</td>
<td>Browser to iLO</td>
<td>Provides browser access to the integrated remote console.</td>
</tr>
<tr>
<td>63001 and 63002</td>
<td>TCP</td>
<td>Local, on host OS</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Controlling access to the appliance console**

Control physical access to the HPE Synergy frame. Unauthorized personnel cannot get physical access to the system console or computer components.

Typical legitimate uses for access to the console are:

- Performing initial hardware setup
- Troubleshooting network configuration issues
- Resetting an appliance administrator password
- Enabling service access by an on-site Authorized technical support representative

**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 on-site Authorized technical support. By default, on-site Authorized technical support personnel are allowed to access your system through the appliance console and diagnose issues that you have reported.

Support access is privileged, which enables the on-site authorized 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 UI.

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 an /rest/appliance/settings/enableServiceAccess REST API to enable or disable services access.

⚠️ CAUTION:
Hewlett Packard Enterprise recommends that you enable access. Otherwise, the authorized support representative will not be able to access the appliance to correctly troubleshoot issues.

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

Algorithms for securing the appliance

This section covers the following information:
• Local user passwords
• Backup files
• Managed device credentials
• Updates
• Support dumps
• Certificates
• Administrator password reset and Hewlett Packard Enterprise support access
• Supported SSL cipher suites
• Supported SSH cipher suites
• Supported RabbitMQ cipher suites
• Supported SNMP authentication protocols for interconnects
• Supported SNMP privacy protocols for interconnects
• Supported SNMP authentication protocols for trap forwarding
• Supported SNMP authentication protocols for trap forwarding
• SNMP server management

Local user passwords
SHA-384 Hashing algorithm with 64-bit Salt and 1000 iterations are used to hash the password

Backup files
Backup files are encrypted with a simple symmetric key cryptography and the key is unique per appliance. This form of encryption helps prevent casual attempts at reading or tampering the backup files. Hewlett Packard Enterprise strongly recommends that you encrypt backup files on the backup server with an encryption key that you generate to ensure confidentiality and the integrity of the backup file.

Managed device credentials
Passwords of managed devices and external servers are encrypted with AES-256 algorithm.

Updates
HPE OneView Update binary (update.bin) and the Red Hat package managers (RPM) contained in the update.bin are signed using SHA-512 and 4096-bit RSA key.

Support dumps
Support dumps are encrypted using AES/CTR/No Padding:256 algorithm and the AES key is encrypted separately using 3072-bit RSA asymmetric key pair.

Certificates
By default, on a fresh installation of the HPE OneView appliance, the self-signed certificate is signed using SHA-256 digital signature algorithm with a 2048 bit RSA key. On an upgraded appliance any existing self-signed certificates are retained. If a user has a certificate authority-signed SHA1 certificate, then the SHA1 certificate is retained post upgrade. The user is notified with an alert to regenerate or re-import a higher strength certificate.
Administrator password reset and Hewlett Packard Enterprise support access

S/KEY: A one-time challenge-response password scheme

Supported SSL cipher suites

- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-SHA384
- ECDH-RSA-AES256-SHA256
- AES256-SHA256
- DH-RSA-AES256-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-SHA256
- ECDH-RSA-AES128-SHA
- AES128-SHA
- ECDHE-RSA-AES128-SHA
- ECDH-RSA-AES128-SHA
- DHE-RSA-AES128-SHA
- AES128-SHA
- DHE-DSS-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA
- ECDH-ECDSA-AES256-SHA
- ECDH-RSA-AES256-SHA
- ECDHE-ECDSA-AES128-SHA
- ECDH-ECDSA-AES128-SHA
- CAMELLIA128-SHA
- CAMELLIA256-SHA
- PSK-AES256-CBC-SHA
- SEED-SHA
- DH-DSS-CAMELLIA256-SHA
- DH-DSS-AES256-SHA
- DHE-DSS-AES128-SHA
- DH-DSS-AES256-SHA256
- DH-RSA-CAMELLIA256-SHA
- KRB5-IDEA-CBC-MD5
- DH-DSS-AES256-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-CAMELLIA128-SHA
- PSK-AES128-CBC-SHA
- DHE-DSS-CAMELLIA128-SHA
- DHE-DSS-AES256-SHA256
- DH-DSS-SEED-SHA
- DHE-DSS-CAMELLIA128-SHA
- HPE OneView 4.0 for VMs security
### Supported SSH cipher suites

<table>
<thead>
<tr>
<th>SSH service</th>
<th>Algorithms and ciphers supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ciphers</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>aes256-ctr</td>
</tr>
<tr>
<td></td>
<td>aes256-cbc</td>
</tr>
<tr>
<td></td>
<td>aes192-cbc</td>
</tr>
<tr>
<td></td>
<td>aes192-ctr</td>
</tr>
<tr>
<td></td>
<td>aes128-ctr</td>
</tr>
<tr>
<td><strong>Message Authentication Code (MAC)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hmac-sha2-512</td>
</tr>
<tr>
<td></td>
<td>hmac-sha2-256</td>
</tr>
<tr>
<td></td>
<td>hmac-sha1</td>
</tr>
<tr>
<td></td>
<td>hmac-sha1-96</td>
</tr>
<tr>
<td></td>
<td>hmac-md5</td>
</tr>
<tr>
<td></td>
<td>hmac-md5-96</td>
</tr>
<tr>
<td><strong>Key Exchange</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp384:384</td>
</tr>
<tr>
<td></td>
<td>diffie-hellman-group-exchange-sha256</td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp256</td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp521</td>
</tr>
<tr>
<td></td>
<td>diffie-hellman-group-exchange-sha1</td>
</tr>
<tr>
<td></td>
<td>diffie-hellman-group14-sha1</td>
</tr>
<tr>
<td></td>
<td>diffie-hellman-group1-sha1</td>
</tr>
<tr>
<td><strong>Host Key algorithms (for clients)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ssh-rsa:3072</td>
</tr>
<tr>
<td></td>
<td>ssh-rsa:2048</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>SSH service</th>
<th>Algorithms and ciphers supported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ssh-rsa:4096</td>
</tr>
<tr>
<td></td>
<td>ssh-dss:1024</td>
</tr>
<tr>
<td></td>
<td>ecdsa-sha2-nistp384:384</td>
</tr>
<tr>
<td></td>
<td>ecdsa-sha2-nistp256:256</td>
</tr>
<tr>
<td></td>
<td>ecdsa-sha2-nistp521:521</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Host Key algorithms (HPE OneView host key algorithms)</th>
<th>ssh-rsa:2048</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ssh-dsa:1024</td>
</tr>
</tbody>
</table>

| HPE OneView Key-based authentication | rsa:2048 |

**Supported RabbitMQ cipher suites**

```
ecdhe_ecdsa,aes_256_cbc,sha384,sha384
ecdhe_rsa,aes_256_cbc,sha384,sha384
ecdh_ecdsa,aes_256_cbc,sha256,sha256
ecdh_rsa,aes_256_cbc,sha256,sha256
dhe_rsa,aes_256_cbc,sha256,sha256
ecdh_ecdsa,aes_128_cbc,sha256,sha256
ecdh_rsa,aes_128_cbc,sha256,sha256
dhe_rsa,aes_128_cbc,sha256,sha256
ecdh_ecdsa,aes_256_cbc,sha256,sha256
ecdh_rsa,aes_256_cbc,sha256,sha256
ecdh_rsa,aes_128_cbc,sha256,sha256
ecdh_rsa,aes_256_cbc,sha256,sha256
dhe_dss,aes_128_cbc,sha256
ecdhe_ecdsa,aes_256_cbc,sha256
ecdh_ecdsa,aes_256_cbc,sha256
ecdh_rsa,aes_256_cbc,sha256
ecdhe_ecdsa,aes_128_cbc,sha256
ecdh_rsa,aes_128_cbc,sha256
ecdhe_ecdsa,aes_128_cbc,sha256
ecdh_rsa,aes_128_cbc,sha256
ecdhe_ecdsa,'3des_ede_cbc',sha256
ecdhe_rsa,'3des_ede_cbc',sha256
ecdhe_ecdsa,'3des_ede_cbc',sha256
ecdhe_rsa,'3des_ede_cbc',sha256
ecdh_rsa,'3des_ede_cbc',sha256
ecdh_rsa,'3des_ede_cbc',sha256
```
Supported SNMP authentication protocols for interconnects

MD5
SHA1
SHA-256
SHA-384
SHA-512

Supported SNMP privacy protocols for interconnects

MD5
DES
3DES
AES-128
AES-192
AES-256

Supported SNMP authentication protocols for trap forwarding

MD5
SHA1
SHA256
SHA384
SHA512

Supported SNMP privacy protocols for trap forwarding

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

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.

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**
Modeling scope-based access control in HPE OneView

I want to ...

- Implement scope-based access control
- "Troubleshoot authorization failures" in the Online help
- "See more tasks" in the Online help

Learn more

- About user accounts
- About permissions
- About user roles
- About scope-based access control
- About scopes

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:
<table>
<thead>
<tr>
<th>Action</th>
<th>Action semantic</th>
<th>Authorization check semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Controls the right to create a resource.</td>
<td>A permission must grant the user Create rights on the resource category. If a single scope-restricted permission grants Create, the resource is assigned to the permission scope. If multiple scoped permissions grant Create, the desired scope must be specified.</td>
<td>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.</td>
</tr>
<tr>
<td>Delete</td>
<td>Controls the right to delete a resource.</td>
<td>A permission must grant the user Delete 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.</td>
<td>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.</td>
</tr>
<tr>
<td>Update</td>
<td>Controls the right to modify a resource. This includes changing the state of a resource.</td>
<td>A permission must grant the user Update 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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

**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 HPE OneView API Reference for more information.

*Table Continued*
<table>
<thead>
<tr>
<th>Action</th>
<th>Action semantic</th>
<th>Authorization check semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Controls the right to view a resource.</td>
<td>A permission must grant the user <strong>Read</strong> rights on the resource category. <strong>Read rights</strong> are not restricted by scope.</td>
<td>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. However, no <strong>Use</strong> checks are performed when you set the server hardware to <strong>unassigned</strong> in a server profile or remove a SAN storage volume.</td>
</tr>
</tbody>
</table>
| Use      | 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**. **Exception:** **Use rights** are required to unassign a template (for example, server profile template or volume template) from its **associated resource**. | A permission must grant the user the following rights:  
  • 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. |                                                                                                                                                 |

**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**.

---

**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.
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:

<table>
<thead>
<tr>
<th>HPE OneView main menu</th>
<th>Related role category names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Bundles</td>
<td>firmware-drivers</td>
</tr>
<tr>
<td>Interconnects</td>
<td>interconnects, sas-interconnects</td>
</tr>
<tr>
<td>Logical Interconnect Groups</td>
<td>logical-interconnect-groups, sas-logical-interconnect-groups</td>
</tr>
<tr>
<td>Logical Interconnects</td>
<td>logical-interconnects, sas-logical-interconnects</td>
</tr>
<tr>
<td>Networks</td>
<td>ethernet-networks, fcoe-networks, fc-networks</td>
</tr>
<tr>
<td>Power Delivery Devices</td>
<td>power-devices</td>
</tr>
<tr>
<td>SAN Managers</td>
<td>fc-device-managers</td>
</tr>
<tr>
<td>SANs</td>
<td>fc-sans</td>
</tr>
<tr>
<td>Settings</td>
<td>appliance</td>
</tr>
<tr>
<td>Users and Groups</td>
<td>users, grouptorolemappings</td>
</tr>
<tr>
<td>Volume Templates</td>
<td>storage-volume-templates</td>
</tr>
<tr>
<td>Volumes</td>
<td>storage-volumes</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate IT</td>
<td>Senior technologists</td>
<td>HPE OneView appliance and all managed resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Server administrators</td>
<td>All server resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Network administrators</td>
<td>All network resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Storage administrators</td>
<td>All storage resources</td>
</tr>
<tr>
<td>Finance</td>
<td>OS and Application administrators</td>
<td>OS and applications operating on servers assigned to the Finance department</td>
</tr>
<tr>
<td>Human Resources</td>
<td>OS and Application administrators</td>
<td>OS and applications operating on servers assigned to the Human Resources department</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>SRV Cloud provisioning and allocation process</td>
</tr>
</tbody>
</table>

*Table Continued*
### 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:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate IT</td>
<td>Senior technologists</td>
<td>Infrastructure administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Storage administrators</td>
<td>Storage Administrator</td>
<td>All resources</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Cloud IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>VM Cloud</td>
</tr>
<tr>
<td>VM Cloud IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>VM Cloud</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Rights</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labels</td>
<td>Create, Read, Update, Delete</td>
<td>Allows SRV IT users to assign labels to any resource in a category granted Update 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.</td>
</tr>
<tr>
<td>Network Sets</td>
<td>Create, Read, Update, Delete</td>
<td>Allows SRV IT to create network sets in the SRV Cloud scope.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Server profile architect</td>
<td>SRV Cloud</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Scope operator</td>
<td>SRV Cloud</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Rights</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labels</td>
<td>Create, Read, Update, Delete</td>
<td>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.</td>
</tr>
<tr>
<td>Server Hardware</td>
<td>Read, Update</td>
<td>Aligned with desired privileges.</td>
</tr>
<tr>
<td>Server Profiles</td>
<td>Read, Update</td>
<td>Aligned with desired privileges.</td>
</tr>
</tbody>
</table>

Human Resources and Finance users are granted the following permissions:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Finance</td>
</tr>
<tr>
<td>Human Resources</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Human Resources</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate IT</td>
<td>Senior technologists</td>
<td>Infrastructure administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Storage administrators</td>
<td>Storage administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Finance</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Finance</td>
</tr>
<tr>
<td>Human Resources</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Human Resources</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Server profile architect</td>
<td>SRV Cloud</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Scope operator</td>
<td>SRV Cloud</td>
</tr>
<tr>
<td>VM Cloud IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>VM Cloud</td>
</tr>
<tr>
<td>VM Cloud IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>VM Cloud</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create networks</td>
<td>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.</td>
</tr>
<tr>
<td>Create network sets</td>
<td>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.</td>
</tr>
<tr>
<td>Create logical interconnect groups</td>
<td>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 uplink sets.</td>
</tr>
<tr>
<td>Create enclosure groups</td>
<td>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.</td>
</tr>
<tr>
<td>Create logical enclosures</td>
<td>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.</td>
</tr>
<tr>
<td>Power on/off/Refresh interconnects</td>
<td>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.</td>
</tr>
<tr>
<td>Power on/off/Refresh drive enclosures</td>
<td>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.</td>
</tr>
<tr>
<td>Operation</td>
<td>Analysis</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Launch console/Power on/off/Reset/Refresh server hardware</td>
<td>Corporate IT must assign the blades in the VM Cloud enclosures to the VM Cloud scope.</td>
</tr>
<tr>
<td>Create server profile templates</td>
<td>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.</td>
</tr>
<tr>
<td>Create server profiles</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch console/Power on/off/Reset/Refresh server hardware</td>
<td>Corporate IT needs to assign the blades in the SRV Cloud enclosures to the SRV Cloud scope.</td>
</tr>
<tr>
<td>Create server profile templates</td>
<td>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.</td>
</tr>
<tr>
<td>Create server profiles</td>
<td>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.</td>
</tr>
<tr>
<td>Assign SRV Cloud resources to Human Resources and Finance scopes</td>
<td>Both an Update and Use 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 Update rights on the Human Resources scope and Use 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.</td>
</tr>
</tbody>
</table>

Finally, Corporate IT completes the analysis of the Human Resources and Finance scopes.
<table>
<thead>
<tr>
<th>Operation</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch console/Power on/off/Reset/Refresh server hardware</td>
<td>SRV Cloud IT is responsible for assigning SRV Cloud server hardware to the Human Resources and Finance scopes.</td>
</tr>
<tr>
<td>Update server profiles</td>
<td>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.</td>
</tr>
</tbody>
</table>

To summarize, the authentication model for the pilot defines four permission scopes and nine directory group accounts with associated permissions.

<table>
<thead>
<tr>
<th>Permission Scope</th>
<th>Resources explicitly assigned to the scope by Corporate IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>None</td>
</tr>
<tr>
<td>Human Resources</td>
<td>None</td>
</tr>
<tr>
<td>SRV Cloud</td>
<td>The blades contained in the two enclosures dedicated to the SRV Cloud pilot. The firmware bundles approved for use by SRV Cloud IT. The networks approved for use by SRV Cloud IT. 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.</td>
</tr>
<tr>
<td>VM Cloud</td>
<td>The three enclosures dedicated to the VM Cloud pilot. The blades contained in the three enclosures. The interconnects contained in the three enclosures. The drive enclosures contained in the three enclosures. The firmware bundles approved for use by VM Cloud IT. The volume templates approved for use by VM Cloud IT.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directory Group</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CorpIT-FULL</td>
<td>(Infrastructure administrator, All resources)</td>
</tr>
<tr>
<td>CorpIT-NA</td>
<td>(Network administrator, All resources)</td>
</tr>
<tr>
<td>CorpIT-SA</td>
<td>(Server administrator, All resources)</td>
</tr>
<tr>
<td>CorpIT-SA</td>
<td>(Server administrator, All resources)</td>
</tr>
<tr>
<td>Finance-Admins</td>
<td>(Server profile operator, Finance)</td>
</tr>
<tr>
<td>HR-Admins</td>
<td>(Server profile operator, Human Resources)</td>
</tr>
<tr>
<td>SRVCloudIT-Admins</td>
<td>(Server profile architect, SRV Cloud); (Scope operator, SRV Cloud)</td>
</tr>
<tr>
<td>VMCloudIT-SA</td>
<td>(Server administrator, VM Cloud)</td>
</tr>
<tr>
<td>VMCloudIT-NA</td>
<td>(Network administrator, VM Cloud)</td>
</tr>
</tbody>
</table>
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 offers 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.

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 and the allowed usage of that key (for example, digital signatures, certificate signing, encryption, and so on).

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
- "Two-factor Authentication using Client Certificates" in the online help

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 access the appliance console and view the appliance self-signed certificate without using HTTPS, connect a laptop or a keyboard, monitor, and mouse to the Synergy frame.

- 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.

In an HPE Synergy environment, securely connecting to the composer, frame link modules, and compute module iLOs is most easily achieved before the initial frame link topology is wired to the management LAN. Also, when you add a new frame or compute module to an existing frame link topology, you need not disconnect from the management LAN. Instead, use the automatic initial trust approach for establishing trust for the new devices.

**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, frame link modules, and the appliance all provide REST APIs for generating CSRs and uploading the resulting CA-signed certificates and CRLs.

See the REST API online help for more information about REST APIs.

**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 frame link modules 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:**

Automatic additions of certificates happens only during discovery. The automatic initial trust approach is used only 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 sections below.

• 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:

• **Synergy frame link topology**
  
  To establish initial trust in an HPE Synergy system using only self-signed certificate, perform hardware discovery of the initial frame link topology before connecting the frame link modules to the management network. When all the devices are isolated from the management network, there is no possibility of a man-in-the-middle attack and all the self-signed certificates are stored securely in the HPE OneView trust store.

  **NOTE:**
  
  This approach is only applicable during setup of the original frame link topology. As additional frames, remote frame link topologies, or additional compute modules are inserted, the self-signed certificates for those devices must be individually validated using the automatic initial trust approach.

• **For Synergy Gen10 compute modules**
  
  SSH to HPE OneView and use the following command to connect serially to each of the iLOs and obtain the certificate fingerprint:

  ```
  cd /map1/sslcert1/hpiLO
  show
  ```

  In order for the SSH connection itself to be trusted, the HP OneView SSH host key must be saved during the initial Synergy configuration, before the frame link topology is connected to the management network. This approach only works for compute modules in the ‘Production’ security mode of the iLO. Alternate approaches require that the iLO be isolated from the management network as described in the Gen9 compute modules section.

• **For Synergy Gen9 compute modules**
  
  For the Gen9 compute module, the only way to securely obtain a self-signed certificate is to connect to the iLO when the frame is isolated from the frame link topology and is disconnected from the management network. Connect a device with a web browser (such as a laptop) to the management network port of the iLO and browse each iLO to view its certificate fingerprint.

• **Frame Link Modules**
  
  The console user interface of the Frame Link Module displays its certificate’s fingerprint. Frame Link Modules are automatically trusted initially and also after a factory reset of the Frame Link Module.
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 pre-bundled 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 are 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 communication to the remote support server to be trusted and secure:

- 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

**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.

### 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 file 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 CRL files downloaded from a CA to the appliance. HPE OneView then validates all certificates signed by the CA against this CRL. CRLs themselves have an expiration date and must be uploaded into the appliance before their expiration.

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.

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
Locate CRL Distribution Points in the HPE OneView Online Help provides details on how to locate the CRL DPs for these certificates.

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.

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

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.

iLO3 and iLO4 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 or not 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 also occur on iLO4-based Synergy Gen9 compute modules in addition to the 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.

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.
### 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.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access</strong></td>
<td>• Control <a href="#">access to the appliance</a></td>
</tr>
<tr>
<td></td>
<td>◦ Allow HPE Services access</td>
</tr>
<tr>
<td></td>
<td>◦ Disable access to the Hardware setup feature so that an installation technician can not access the console</td>
</tr>
<tr>
<td><strong>Accounts</strong></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• If local accounts are used, protect the built-in administrator account with a strong password.</td>
</tr>
<tr>
<td></td>
<td>• Do not use the built-in Administrator account. All users must login using their own credentials to facilitate auditing.</td>
</tr>
<tr>
<td><strong>Audit logs</strong></td>
<td>Download the appliance audit logs at regular intervals.</td>
</tr>
</tbody>
</table>
Certificates

- Use certificates signed by a trusted certificate authority (CA).

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.

The appliance supports self-signed certificates and certificates signed by a CA.

The appliance is initially configured with self-signed certificates for the web server and the State Change Message Bus (SCMB).

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, or through another trusted CA.

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.

- 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, then 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.

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.

See Use a certificate authority on page 187.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates</td>
<td>• Use certificates signed by a trusted certificate authority (CA).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The appliance supports self-signed certificates and certificates signed by a CA.</td>
</tr>
<tr>
<td></td>
<td>The appliance is initially configured with self-signed certificates for the web server and the State Change Message Bus (SCMB).</td>
</tr>
<tr>
<td></td>
<td>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, or through another trusted CA.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If your company does not have its own certificate authority, then 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See Use a certificate authority on page 187.</td>
</tr>
<tr>
<td>Topic</td>
<td>Best Practice</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Network** | • 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).  
  ◦ **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.  
  • Do not connect management systems (for example, the Composer, the iLO) 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. |
| **Passwords**| • 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** | 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 *HPE OneView Online help*.  
  • **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. |
<table>
<thead>
<tr>
<th>Topic</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-factor authentication</td>
<td>HPE OneView supports two-factor authentication. Deploy <strong>two-factor authentication</strong> for increased security.</td>
</tr>
<tr>
<td>Updates</td>
<td>• Sign up for HPE OneView bulletins at: <a href="http://www.hpe.com/support/e-updates">http://www.hpe.com/support/e-updates</a></td>
</tr>
<tr>
<td></td>
<td>• Install updates for all components in your environment on a regular basis.</td>
</tr>
<tr>
<td>Managed Environment</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

### Understanding the security features of HPE OneView

HPE OneView runs on a dedicated HPE Synergy Composer (management software embedded into the hardware). HPE OneView is configured to be fully secure out-of-the-box.

**High-level overview**

<table>
<thead>
<tr>
<th>Security-hardened appliance</th>
<th>on page 175</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best practices for maintaining a secure appliance</td>
<td>on page 151</td>
</tr>
<tr>
<td>Nonbrowser clients</td>
<td>on page 193</td>
</tr>
</tbody>
</table>

**User access and authentication**

| About complex passwords | on page 155 |
| About directory service authentication | on page 155 |
| Authentication for appliance access | on page 177 |
| Controlling access for authorized users | on page 182 |
| Creating a login session | on page 177 |
| Specifying user accounts and roles | on page 182 |
| Protecting credentials | on page 184 |

**Console access**

| Controlling access to the appliance console | on page 195 |

**Certificates**

| Two-factor Authentication | on page 178 |
| Managing certificates from a browser | on page 186 |
| Certificate management | on page 216 |

**Learn more**

| Algorithms for securing the appliance | on page 196 |
| Ports required for HPE OneView | on page 193 |
| Files you can download from the appliance | on page 201 |
| Understanding the audit log | on page 184 |
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 includes:

- Not performing expiration checks for self-signed certificates
- For certificate authority (CA) signed certificates, relaxed certificate revocation list (CRL) checking.

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.

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 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

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.
About directory service authentication

You can use an external enterprise directory service (EDS) to authenticate and provide single sign-on to individual users or user groups. An enterprise directory is a requirement for using two-factor authentication. Each user in a group is assigned the same role (for example, Infrastructure administrator). An example of an enterprise directory is a corporate directory that uses Active Directory or LDAP (Lightweight Directory Access Protocol). Active Directory is required for two-factor authentication.

After the directory service is configured, any user in the group can log in to the appliance (or use a smart card and PIN, if two-factor authentication is enabled).

If logging in with a user name and password, on the login window, a user:

- Enters their user name (typically, the Common-Name attribute, CN).
  - The format for the user name depends on the Directory type.
- Enters their password.
- Selects the enterprise directory service.

If authentication using a smart card, a user:

- Inserts their smart card in a smart card reader.
- Selects their certificate when prompted by the browser.
- Enters their PIN.

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.

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 users’ sessions are ended when such modifications are made.

Authenticating users

When you add an enterprise directory service to the appliance, you provide location criteria so that the appliance can find the group.

If two-factor authentication is enabled, you create a service account that the appliance uses to access the authentication directory when validating a security certificate from a smart card.

Adding a directory server

If you replicate the enterprise directory service for high availability or disaster tolerance, add the replicated directory service as a separate directory service.

After configuring and adding a directory server, you can designate it as the default directory service.

When you add a new directory with a different server for which the certificate is not trusted, a prompt is generated for trusting the root CA. Additionally, an alert is generated when an upgraded directory configuration has a missing certificate chain or an imported root CA. If the root CA certificate you imported is
A X509 v1 type certificate, it is treated as a self-signed certificate and when the CRL is uploaded the certificate is treated as a CA certificate.

**After you add an enterprise directory service and server**

You can:

Add a group, which had already been defined in the directory service, so that all its members can login on the appliance.

Allow local logins only, which is the default.

Allow both local logins and logins for user accounts authenticated by the directory service.

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.

**Considerations for configuring a Microsoft Active Directory directory service**

- The following maps the Active Directory attribute to the LDAP property:

<table>
<thead>
<tr>
<th>LDAP property</th>
<th>Active Directory attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>Common-Name</td>
</tr>
<tr>
<td>uid</td>
<td>UID</td>
</tr>
<tr>
<td>userPrincipalName</td>
<td>User-Principal-Name</td>
</tr>
<tr>
<td>sAMAccountName</td>
<td>SAM-Account-Name</td>
</tr>
</tbody>
</table>

If the *user name* does not contain either an @ character (to denote a UPN) or a \ character (to denote domain\login), then these logins are attempted in this order:

1. The *user name* is treated as the sAMAccountName and directory-name gets prepended as (directory-name\user-name)
2. The *user name* is treated as a UID.
3. The *user name* is treated as a CN.

- 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’s name, displayed here with the corresponding attribute:

<table>
<thead>
<tr>
<th>User name component</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>givenName</td>
</tr>
<tr>
<td>Initials</td>
<td>initial</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
</tr>
</tbody>
</table>

The field labeled Full Name defaults to this format and 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. This, 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:

\texttt{LogonName@DNSDomain}

For example:

\texttt{JoeUser@exampledomain.example.com}

- Finally, as you enter the User logon name, the first twenty 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.

**About emergency local login**

When configured to use a directory service, administrators can choose to disable local logins for improved security. If the 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 4.0 version, 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 155.

**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 174 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.
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.

**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 5: User role permissions

<table>
<thead>
<tr>
<th>Role</th>
<th>Type of user</th>
<th>Permissions or privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full</strong></td>
<td>Infrastructure administrator</td>
<td>View, create, edit, or remove resources managed or monitored by the appliance, including management of the appliance, through the UI or using REST APIs. An Infrastructure administrator can also manage information provided by the appliance in the form of activities, notifications, and logs. Only an Infrastructure administrator can restore an appliance from a backup file.</td>
</tr>
<tr>
<td>Read only</td>
<td>Read only</td>
<td>View managed or monitored resource information. Cannot add, create, edit, remove, or delete resources.</td>
</tr>
<tr>
<td>Specialized</td>
<td>Backup administrator</td>
<td>Create and download backup files, view the appliance settings and activities. Has the authority to use scripts to log in to the appliance and run scripts to back up the appliance. Cannot restore the appliance from a backup file.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td></td>
<td>This role is specifically 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. Hewlett Packard Enterprise recommends that users with this role should not initiate interactive login sessions through the HPE OneView user interface.</td>
</tr>
<tr>
<td>Network administrator</td>
<td></td>
<td>View, create, edit, or remove networks, network sets, connections, interconnects, uplink sets, and firmware bundles. View related activities, logs, and notifications. Cannot manage user accounts.</td>
</tr>
<tr>
<td>Server administrator</td>
<td></td>
<td>View, create, edit, or remove server profiles and templates, network sets, enclosures, and firmware bundles. Access the physical servers. View connections, networks, racks, power, and related activities, logs, and notifications. Add volumes, but cannot add storage pools or storage systems. Cannot manage user accounts.</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Role</th>
<th>Type of user</th>
<th>Permissions or privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Server firmware operator</strong></td>
<td>View managed or monitored resource information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit, but not create or delete, physical servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edits the server hardware, firmware baseline, firmware installation method and activation schedule values on server profiles.</td>
</tr>
<tr>
<td></td>
<td><strong>Server profile architect</strong></td>
<td>Create and manage server profiles, server profile templates, storage volumes, labels, and network sets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use networks, enclosures, firmware drivers, server hardware, storage pools, and storage volume templates.</td>
</tr>
<tr>
<td></td>
<td><strong>Server profile administrator</strong></td>
<td>Create and manage server profiles, storage volumes, labels, and network sets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use networks, enclosures, firmware drivers, server hardware, server profile templates, storage pools, and storage volume templates.</td>
</tr>
<tr>
<td></td>
<td><strong>Server profile operator</strong></td>
<td>Create, delete, and update labels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update server hardware, and server profiles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use networks, network sets, enclosures, firmware drivers, server hardware, server profiles, storage pools, and storage volume templates.</td>
</tr>
<tr>
<td></td>
<td><strong>Scope administrator</strong></td>
<td>Create and delete scopes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update scopes, add and remove scope resources.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cannot modify any resource other than scopes.</td>
</tr>
<tr>
<td></td>
<td><strong>Scope operator</strong></td>
<td>Update scopes, add and remove scope resources.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cannot modify any resource other than scopes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cannot create or delete scopes.</td>
</tr>
<tr>
<td></td>
<td><strong>Storage administrator</strong></td>
<td>View, add, edit, or remove storage systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View, add, or remove storage pools.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View, create, edit, add, or delete volumes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View, create, edit, or delete volume templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View, add, or edit SAN managers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View or edit SANs.</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Role</th>
<th>Type of user</th>
<th>Permissions or privileges</th>
</tr>
</thead>
</table>
| Software Administrator      |                       | Creates and modifies Image Streamer artifacts like plan scripts, build plans, and deployment plans.  
Assigns a golden image for deployment.  
Performs a capture from a web server.  
Performs all the actions pertaining to the artifact bundles.  
Can perform activities like appliance restart, shutdown, update firmware, backup, restore, and activate standby. |

| HardwareSetup                |                       | A credential-less login for data center technicians that allows them to verify cabling of HPE Synergy hardware and fix alerts related to first time setup of hardware.  
Installs HPE Synergy hardware, verifies cabling, and uses HP OneView to verify minimum operation. |

**Action privileges for user roles**

The following tables lists 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 6: Action privileges for user roles**

<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for user roles</th>
<th>IA=Infrastructure administrator, admin=administrator</th>
<th>(C=Create, R=Read, U=Update, D=Delete, Use)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA</td>
<td>Server admin</td>
<td>Network admin</td>
</tr>
<tr>
<td>activities</td>
<td>CRUD</td>
<td>CRU</td>
<td>CRUD</td>
</tr>
<tr>
<td>alerts</td>
<td>RUD</td>
<td>RUD</td>
<td>RUD</td>
</tr>
<tr>
<td>appliance</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>artifact-bundles</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>audit logs</td>
<td>CR</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>backups</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>certificates</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>community string</td>
<td>RU</td>
<td>R</td>
<td>CRU</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator</td>
</tr>
<tr>
<td></td>
<td>(C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td></td>
<td><strong>IA</strong>  <strong>Server admin</strong>  <strong>Network admin</strong>  <strong>Backup admin</strong>  <strong>Storage admin</strong>  <strong>Software admin</strong></td>
</tr>
<tr>
<td>connections</td>
<td>CRUD  R  CR  R  R  R</td>
</tr>
<tr>
<td>connection templates</td>
<td>CRUD, Use  R, Use  CRUD  R  R  R</td>
</tr>
<tr>
<td>console users</td>
<td>CRUD  —  —  —  —  —</td>
</tr>
<tr>
<td>data centers</td>
<td>CRUD  CRUD  R  R  R  R</td>
</tr>
<tr>
<td>debug logs</td>
<td>CRUD  CRU  CRU  —  R  CRU</td>
</tr>
<tr>
<td>deployed- targets</td>
<td>CRUD  CRUD  R  R  R  R</td>
</tr>
<tr>
<td>deployment-clusters</td>
<td>CRUD  R  R  R  R  R</td>
</tr>
<tr>
<td>deployment-groups</td>
<td>CRUD  R  R  R  R  R</td>
</tr>
<tr>
<td>deployment-managers</td>
<td>CRUD  R  R  R  R  R</td>
</tr>
<tr>
<td>device bays</td>
<td>CRUD  CRUD  R  R  R  R</td>
</tr>
<tr>
<td>domains</td>
<td>CRUD  R  CRU  R  R  R</td>
</tr>
<tr>
<td>drive enclosures</td>
<td>CRUD  CRUD, Use  R, Use</td>
</tr>
<tr>
<td>enclosures</td>
<td>CRUD  CRUD  R  R  R  R</td>
</tr>
<tr>
<td>enclosure groups</td>
<td>CRUD, Use  CRUD, Use  R  R  R  R</td>
</tr>
<tr>
<td>Ethernet networks</td>
<td>CRUD  R  CRUD  R  R  R</td>
</tr>
<tr>
<td>events</td>
<td>CRU  CRU  CRU  —  R  CRU</td>
</tr>
<tr>
<td>fabrics</td>
<td>CRUD  R  CRUD  R  R  R</td>
</tr>
<tr>
<td>FC aliases</td>
<td>CRUD  R  R  R  CRUD  R</td>
</tr>
<tr>
<td>FC device managers</td>
<td>CRUD  R  R  R  CRUD  R</td>
</tr>
<tr>
<td>FC endpoints</td>
<td>R  R  R  R  R  R</td>
</tr>
</tbody>
</table>

*Table Continued*
### Action privileges for user roles

IA=Infrastructure administrator, admin=administrator

(C=Create, R=Read, U=Update, D=Delete, Use)

<table>
<thead>
<tr>
<th>Category</th>
<th>IA</th>
<th>Server admin</th>
<th>Network admin</th>
<th>Backup admin</th>
<th>Storage admin</th>
<th>Software admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC networks</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FCOE networks</td>
<td>CRUD, Use</td>
<td>R</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC ports</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC providers</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC SANs</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>FC SAN services</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>FC switches</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC tasks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>FC zones</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>firmware drivers</td>
<td>CRUD</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>global settings</td>
<td>CRUD</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>CRUD</td>
</tr>
<tr>
<td>golden- images</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>golden- volumes</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>grouptorole mappings</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>hardware setup</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>hosts</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>host clusters</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>i3s- maintenance-services</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>i3s-volume-services</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>ID range ipv4</td>
<td>CRUD</td>
<td>RU</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator</td>
</tr>
<tr>
<td></td>
<td>(C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td>login sessions</td>
<td>IA: CRUD, Server admin: RU, Network admin: RU, Backup admin: RU, Storage admin: RU, Software admin: —</td>
</tr>
<tr>
<td>Category</td>
<td>Action privileges for user roles</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td></td>
<td><strong>IA</strong></td>
</tr>
<tr>
<td>migratable VC domains</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>networks</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>network sets</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>notifications</td>
<td>CRUD</td>
</tr>
<tr>
<td>oe-build- plans</td>
<td>CRUD</td>
</tr>
<tr>
<td>oe- deployment-plans</td>
<td>CRUD</td>
</tr>
<tr>
<td>organizations</td>
<td>CRUD</td>
</tr>
<tr>
<td>os-volumes</td>
<td>CRUD</td>
</tr>
<tr>
<td>plan-scripts</td>
<td>CRUD</td>
</tr>
<tr>
<td>ports</td>
<td>RU, Use</td>
</tr>
<tr>
<td>power devices</td>
<td>CRUD</td>
</tr>
<tr>
<td>racks</td>
<td>CRUD</td>
</tr>
<tr>
<td>reports</td>
<td>R</td>
</tr>
<tr>
<td>repository manager</td>
<td>CRUD</td>
</tr>
<tr>
<td>restores</td>
<td>CRUD</td>
</tr>
<tr>
<td>roles</td>
<td>CRUD</td>
</tr>
<tr>
<td>SANS</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>SAN manager</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>SAS interconnects</td>
<td>CRUD, Use</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Category</th>
<th>IA</th>
<th>Server admin</th>
<th>Network admin</th>
<th>Backup admin</th>
<th>Storage admin</th>
<th>Software admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS logical interconnect groups</td>
<td>CRUD, Use</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>SAS logical interconnects</td>
<td>CRUD, Use</td>
<td>CRUD, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>scopes</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>server hardware</td>
<td>CRUD, Use</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>server hardware types</td>
<td>CRUD, Use</td>
<td>CRUD, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>server profiles</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>server profile templates</td>
<td>CRUD, Use</td>
<td>CRUD, Use</td>
<td>—</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>stateless- servers</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>storage pools</td>
<td>CRD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>storage systems</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>storage target ports</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>storage volumes</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>storage volume attachments</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>storage volume templates</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>support</td>
<td>CRUD, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>switches</td>
<td>CRUD, Use</td>
<td>RU</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>tasks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>IA</th>
<th>Server admin</th>
<th>Network admin</th>
<th>Backup admin</th>
<th>Storage admin</th>
<th>Software admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>trap forwarding</td>
<td>RU</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>unmanaged devices</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>update</td>
<td>R</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>uplink sets</td>
<td>CRUD</td>
<td>R</td>
<td>CRUD</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>users</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>user preferences</td>
<td>CRUD</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

1 Server administrators cannot edit bandwidths.

**Table 7: Action privileges for specialized user roles**

<table>
<thead>
<tr>
<th>Category</th>
<th>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read only</td>
</tr>
<tr>
<td>activities</td>
<td>R</td>
</tr>
<tr>
<td>alerts</td>
<td>R</td>
</tr>
<tr>
<td>appliance</td>
<td>R</td>
</tr>
<tr>
<td>artifact-bundles</td>
<td>R</td>
</tr>
<tr>
<td>audit logs</td>
<td>—</td>
</tr>
<tr>
<td>backups</td>
<td>R</td>
</tr>
<tr>
<td>certificates</td>
<td>R</td>
</tr>
<tr>
<td>community string</td>
<td>—</td>
</tr>
<tr>
<td>connections</td>
<td>R</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td>Read only</td>
<td>Scope admin</td>
</tr>
<tr>
<td>connection templates</td>
<td>R</td>
</tr>
<tr>
<td>console users</td>
<td>—</td>
</tr>
<tr>
<td>data centers</td>
<td>R</td>
</tr>
<tr>
<td>debug logs</td>
<td>R</td>
</tr>
<tr>
<td>deployed-targets</td>
<td>R</td>
</tr>
<tr>
<td>deployment clusters</td>
<td>R</td>
</tr>
<tr>
<td>deployment groups</td>
<td>R</td>
</tr>
<tr>
<td>deployment managers</td>
<td>R</td>
</tr>
<tr>
<td>device bays</td>
<td>R</td>
</tr>
<tr>
<td>domains</td>
<td>R</td>
</tr>
<tr>
<td>drive enclosures</td>
<td>R</td>
</tr>
<tr>
<td>enclosures</td>
<td>R</td>
</tr>
<tr>
<td>enclosure groups</td>
<td>R</td>
</tr>
<tr>
<td>Ethernet networks</td>
<td>R</td>
</tr>
<tr>
<td>events</td>
<td>R</td>
</tr>
<tr>
<td>fabrics</td>
<td>R</td>
</tr>
<tr>
<td>FC aliases</td>
<td>R</td>
</tr>
<tr>
<td>FC device managers</td>
<td>R</td>
</tr>
<tr>
<td>FC endpoints</td>
<td>R</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Read only</th>
<th>Scope admin</th>
<th>Scope operator</th>
<th>Server firmware operator</th>
<th>Server profile architect</th>
<th>Server profile admin</th>
<th>Server profile operator</th>
<th>Hardware setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC networks</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td></td>
</tr>
<tr>
<td>FCOE networks</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td></td>
</tr>
<tr>
<td>FC ports</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>FC providers</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>FC SANs</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>FC SAN services</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>FC switches</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>FC tasks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>FC zones</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>firmware drivers</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
</tr>
<tr>
<td>global settings</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>golden-images</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>golden-volumes</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>group or role mappings</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>hardware setup</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>CRUD</td>
</tr>
<tr>
<td>hosts</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>host clusters</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>i3s-maintenance services</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>i3s-volume services</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Action privileges for specialized user roles</td>
<td>IA=Infrastructure administrator, admin=administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(C=Create, R=Read, U=Update, D=Delete, Use)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Read only</td>
<td>Scope admin</td>
<td>Scope operator</td>
<td>Server firmware operator</td>
<td>Server profile architect</td>
<td>Server profile admin</td>
<td>Server profile operator</td>
<td>Hardware setup</td>
</tr>
<tr>
<td>ID range ipv4</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>ID range ipv4 subnet</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>ID range vmacs (MAC addresses)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>ID range vsns (serial numbers)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>ID range vwwn (World Wide Names)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>infrastructure vms</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>integrated tools</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>interconnects</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD, Use</td>
</tr>
<tr>
<td>interconnect types</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
</tr>
<tr>
<td>labels</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>CRUD</td>
<td>CRUD</td>
<td>R</td>
</tr>
<tr>
<td>licenses</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>CRUD</td>
<td>CRUD</td>
<td>CRUD</td>
<td>—</td>
</tr>
<tr>
<td>logical downlinks</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>logical enclosures</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>logical interconnects</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>logical interconnect groups</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>logical switch groups</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>—</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
<th>IA=Infrastructure administrator, admin=administrator</th>
<th>(C=Create, R=Read, U=Update, D=Delete, Use)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read only</td>
<td>Scope admin</td>
<td>Scope operator</td>
</tr>
<tr>
<td>login domains</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>login sessions</td>
<td>RU</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>managed SANs</td>
<td>R</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>migratable VC domains</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>networks</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>network sets</td>
<td>R</td>
<td>R, Use</td>
<td>R, Use</td>
</tr>
<tr>
<td>notifications</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>oe-build-plans</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>oe-deployment-plans</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>organizations</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>os-volumes</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>plan-scripts</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>ports</td>
<td>—</td>
<td>R</td>
<td>—</td>
</tr>
<tr>
<td>power devices</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>racks</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>reports</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>repository manager</td>
<td>—</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>restores</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>roles</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Category</th>
<th>Action privileges for specialized user roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IA=Infrastructure administrator, admin=administrator (C=Create, R=Read, U=Update, D=Delete, Use)</td>
</tr>
<tr>
<td></td>
<td><strong>Table Continued</strong></td>
</tr>
<tr>
<td>Read only</td>
<td>Scope admin, Scope operator, Server firmware operator, Server profile architect, Server profile admin, Server profile operator, Hardware setup</td>
</tr>
<tr>
<td>SANs</td>
<td>R — — R R R R —</td>
</tr>
<tr>
<td>SAN manager</td>
<td>R — — R R R R —</td>
</tr>
<tr>
<td>SAS interconnects</td>
<td>R R R R R R CRUD, Use</td>
</tr>
<tr>
<td>SAS logical interconnect groups</td>
<td>R R R R R R —</td>
</tr>
<tr>
<td>SAS logical interconnects</td>
<td>R R R R R R —</td>
</tr>
<tr>
<td>scopes</td>
<td>R CRUD RU R R R R R R</td>
</tr>
<tr>
<td>server hardware</td>
<td>R R, Use R, Use RU, Use RU, Use RU, Use RU, Use CRUD, Use</td>
</tr>
<tr>
<td>server hardware types</td>
<td>R R R R R R CRUD, Use</td>
</tr>
<tr>
<td>server profiles</td>
<td>R R, Use R, Use RU¹ CRUD CRUD RU, Use —</td>
</tr>
<tr>
<td>server profile templates</td>
<td>R R R R CRUD, Use R, Use R —</td>
</tr>
<tr>
<td>stateless-servers</td>
<td>R R R R R R R —</td>
</tr>
<tr>
<td>storage pools</td>
<td>R R, Use R, Use R, Use R, Use R, Use R, Use —</td>
</tr>
<tr>
<td>storage systems</td>
<td>R R R R R R R —</td>
</tr>
<tr>
<td>storage target ports</td>
<td>R R R R R R R —</td>
</tr>
<tr>
<td>storage volumes</td>
<td>R R, Use R, Use CRUD, Use CRUD, Use R, Use —</td>
</tr>
<tr>
<td>Category</td>
<td>Read only</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>storage volume attachments</td>
<td>R</td>
</tr>
<tr>
<td>storage volume templates</td>
<td>R</td>
</tr>
<tr>
<td>support</td>
<td>—</td>
</tr>
<tr>
<td>switches</td>
<td>R</td>
</tr>
<tr>
<td>switch domains</td>
<td>R</td>
</tr>
<tr>
<td>switch groups</td>
<td>R</td>
</tr>
<tr>
<td>tasks</td>
<td>R</td>
</tr>
<tr>
<td>trap forwarding</td>
<td>R</td>
</tr>
<tr>
<td>unmanaged devices</td>
<td>R</td>
</tr>
<tr>
<td>update</td>
<td>R</td>
</tr>
<tr>
<td>uplink sets</td>
<td>R</td>
</tr>
<tr>
<td>users</td>
<td>R</td>
</tr>
<tr>
<td>user preferences</td>
<td>R</td>
</tr>
</tbody>
</table>

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

**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 Servers

**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 are sent.

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.

---

**Security-hardened appliance**

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

• Some examples of best-practice security hardening used within HPE OneView on HPE Synergy Composer are:

  ◦ The appliance uses a customized operating system that eliminates all non-essential services in order 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 graphical user interface)
    – 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 completely 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 firmware image of the HPE Synergy Composer is digitally signed by Hewlett Packard Enterprise. When re-imaging the Composer in order to quickly bring it to a specific firmware revision level, the digital signature is verified by the re-imaging process. This ensures the authenticity and integrity of the image.

• 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.

• HPE OneView supports Service console access which enables an Hewlett Packard Enterprise. Support representative to obtain, with customer permission, a one-time password for privileged access to the appliance in order to perform advanced diagnostics.

• 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.
- Two-factor login: You can configure the appliance to perform smart card 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**.

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 card 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
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/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 is as follows:

1. The user types 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 set up 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.
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:

```
```

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 pass phrase. 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

\[
\text{CN}=(\ast), \text{E}=(\ast), \text{UID}=(\ast), \text{DN}=(\ast)
\]

Variations for the CN attribute: examples

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

**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 \(\text{DC}=(\ast)\) configuration extracts the first domain component from the field. The administrator can only specify \(\text{DC}=(\ast)\) 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=(\ast), Issuer.DC=(\ast), SubjectAlternativeName.DirName.DC=(\ast), 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

The appliance enables SSO (single sign-on) to iLO without storing user-created iLO credentials. The following table describes the mapping of roles between the appliance and iLO.

<table>
<thead>
<tr>
<th>Appliance role</th>
<th>SSO to iLO roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure administrator</td>
<td>Admin</td>
</tr>
<tr>
<td>Server administrator</td>
<td>Admin</td>
</tr>
<tr>
<td>Network administrator</td>
<td>User</td>
</tr>
<tr>
<td>Read only</td>
<td>User</td>
</tr>
<tr>
<td>Backup administrator</td>
<td>None</td>
</tr>
<tr>
<td>Storage administrator</td>
<td>User</td>
</tr>
<tr>
<td>Server firmware operator</td>
<td>Admin</td>
</tr>
</tbody>
</table>
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.

Mapping appliance interactions with iLO and iPDU

The appliance performs configurations on the iLO 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](#).

<table>
<thead>
<tr>
<th>Protocol or interaction</th>
<th>Description</th>
<th>iLO</th>
<th>iPDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>Configures NTP</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>Enables and configures SNMP to collect information</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>Enables and configures SNMP traps sent to appliance</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTTPS (RIBCL/SOAP/JSON)</td>
<td>Collects information (the specific protocol varies, but all use TLS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Console</td>
<td>Links from the UI to the iLO Remote Console</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>Not used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Not used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML reply</td>
<td>Collects generic system information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO</td>
<td>Enables and configures an SSO certificate for UI access. See <a href="#">Mapping of SSO roles for iLO</a> for the privileges that are granted.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Appliance user account</td>
<td>Configures and manages the system using an administrator-level user account (and randomly generated password)</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
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 appliance 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 the remote access to the appliance via SSH.

NOTE:
SSH access must be enabled to access the serial console CLI. The serial console CLI is used to access unmanaged interconnects.

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.

Understanding the 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:

<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/time</td>
<td>The date and time of the event</td>
</tr>
<tr>
<td>Internal component ID</td>
<td>The unique identifier of an internal component</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>The organization ID. Reserved for internal use</td>
</tr>
<tr>
<td>User domain</td>
<td>The login domain name of the user</td>
</tr>
<tr>
<td>User name/ID</td>
<td>The user name</td>
</tr>
<tr>
<td>Session ID</td>
<td>The user session ID associated with the message</td>
</tr>
<tr>
<td>Task ID</td>
<td>The URI of the task resource associated with the message</td>
</tr>
<tr>
<td>Client host/IP</td>
<td>The client (browser) IP address identifies the client machine that initiated the request</td>
</tr>
</tbody>
</table>
| Result          | The result of the action, which can be one of the following values:
|                 | • SUCCESS                                                                   |
|                 | • FAILURE                                                                   |
|                 | • SOME_FAILURES                                                             |
|                 | • CANCELED                                                                  |
|                 | • KILLED                                                                    |
| Action          | A description of the action, which can be one of the following values:      |
|                 | • ADD                                                                       |
|                 | • MODIFY                                                                    |
|                 | • DELETE                                                                    |
|                 | • ACCESS                                                                    |
|                 | • RUN                                                                       |
|                 | • LIST                                                                      |
|                 | • ENABLE                                                                    |
|                 | • DISABLE                                                                   |
|                 | • SAVE                                                                      |
|                 | • SETUP                                                                     |
|                 | • UNSETUP                                                                   |
|                 | • DEPLOY                                                                    |
|                 | • START                                                                     |
|                 | • DONE                                                                      |
|                 | • KILLED                                                                    |
|                 | • CANCELED                                                                  |
|                 | • LOGIN                                                                     |
|                 | • LOGOUT                                                                    |
|                 | • DOWNLOAD_START                                                           |
| Severity        | A description of the severity of the event, which can be one of the following values, listed in descending order of importance: |
|                 | • INFO                                                                      |
|                 | • NOTICE                                                                    |
|                 | • WARNING                                                                   |
|                 | • ERROR                                                                     |
|                 | • ALERT                                                                     |
|                 | • CRITICAL                                                                  |

*Table Continued*
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.

**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 191

**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](#).
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 188.

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, Import an appliance certificate on page 190.

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 188.

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.
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:
   ```bash
   openssl genrsa -out cert.key 3072
   ```

2. Using the new key pair, create a Certificate Signing Request (CSR) for the client certificate.
   This command creates a CSR using data input via interactive prompts:
   ```bash
   openssl req -new -key cert.key -out cert.csr
   ```
   The Common Name for this command must be set to "rabbitmq_readonly", since the SCMB server is configured to accept connections from this user. Otherwise, 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:
      ```bash
      [ 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. Please 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.

    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

    Any active connections to the SCMB server will break and need to be reestablished 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 the troubleshooting steps in "Unable to connect to the SCMB server using a CA-signed client certificate" in the online help.

**Import an appliance certificate**

After sending a certificate signing request to the CA and receiving a certificate, you must import it.

**Prerequisites**

- Privileges: Infrastructure administrator.
- Ensure that no other users are logged in to the appliance.

**Procedure**

1. From the main menu, select **Settings**.
2. Click **Security**.
3. Select **Actions > Import certificate**.
4. Copy the certificate text and paste it into the box provided.
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.
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.

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 on **Yes, trust**.
The certificate is added to the appliance trust store. All communication from HPE OneView to the managed device/remote server henceforth will make use of the trusted certificate. The same capability is available via REST API for scripting users.

**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. An SSH connection using other authorized HPE OneView accounts can be used to access the command line interface (CLI) for connecting to serial consoles of Synergy devices.

**Ports required for HPE OneView**

HPE OneView requires specific ports to be available to the appliance to manage servers, enclosures, and interconnects.
Table 8: Ports required for HPE OneView

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Inbound and Outbound</td>
<td>Used for SSH and SFTP. SSH is required to communicate with interconnect modules. SFTP is required for actions such as firmware upgrades and support dumps.</td>
</tr>
<tr>
<td>53</td>
<td>UDP and TCP</td>
<td>Outbound</td>
<td>Used for DNS client queries.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Inbound</td>
<td>Used for the HTTP interface. Typically, this port redirects to port 443; this port provides the access required by the iLO.</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Inbound</td>
<td>HPE OneView acts as an NTP server, iLO requires access.</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Outbound</td>
<td>Used as an NTP client to synchronize the appliance time.</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>Outbound</td>
<td>Supports SNMP GET calls to obtain status data from a server through iLO. Also used for iPDU.</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>Inbound and Outbound for trap forwarding from HPE OneView</td>
<td>Used for SNMP trap support from the iLO, and iPDU devices. This port is also used to monitor the VC interconnects and trap forwarding.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Inbound</td>
<td>Used for the HTTPS interface to user interface and APIs.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Outbound</td>
<td>Used for secure SSL access to the iLO, Frame link module, remote support access to Hewlett Packard Enterprise, and other devices. Used for Redfish, RIBCL, SOAP, and iPDU communication.</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>Outbound</td>
<td>Secure LDAP. Used for enterprise directory integration (Microsoft Active Directory, OpenLDAP)</td>
</tr>
<tr>
<td>2162</td>
<td>UDP</td>
<td>Inbound</td>
<td>Used as an alternative SNMP trap port.</td>
</tr>
<tr>
<td>3269</td>
<td>TCP</td>
<td>Outbound</td>
<td>Used for Microsoft Active directory LDAP global catalog port.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>Inbound</td>
<td>Allows external scripts or applications to connect to and monitor messages from the SCMB (State-Change Message Bus).</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17988</td>
<td>TCP</td>
<td>iLO Integrated Remote Console to iLO</td>
<td>Integrated Remote Console initiating a connection to the iLO.</td>
</tr>
<tr>
<td>17990</td>
<td>TCP</td>
<td>Browser to iLO</td>
<td>Provides browser access to the integrated remote console.</td>
</tr>
<tr>
<td>63001 and 63002</td>
<td>TCP</td>
<td>Local, on host OS</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Controlling access to the appliance console**

Control physical access to the HPE Synergy frame. Unauthorized personnel cannot get physical access to the system console or computer components.

Typical legitimate uses for access to the console are:

- Performing initial hardware setup
- Troubleshooting network configuration issues
- Resetting an appliance administrator password
- Enabling service access by an on-site Authorized technical support representative

**Enable or disable authorized services access**

When you first start up the appliance, you can choose to enable or disable access by on-site Authorized technical support. By default, on-site Authorized technical support personnel are allowed to access your system through the appliance console and diagnose issues that you have reported.

Support access is privileged, which enables the on-site authorized 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 UI.

**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 an /rest/appliance/settings/enableServiceAccess REST API to enable or disable services access.

⚠️ CAUTION:
Hewlett Packard Enterprise recommends that you enable access. Otherwise, the authorized support representative will not be able to access the appliance to correctly troubleshoot issues.

**Algorithms for securing the appliance**

This section covers the following information:

- **Local user passwords**
- **Backup files**
- **Managed device credentials**
- **Updates**
- **Support dumps**
- **Certificates**
- **Administrator password reset and Hewlett Packard Enterprise support access**
- **Supported SSL cipher suites**
- **Supported SSH cipher suites**
- **Supported RabbitMQ cipher suites**
- **Supported SNMP authentication protocols for interconnects**
- **Supported SNMP privacy protocols for interconnects**
- **Supported SNMP authentication protocols for trap forwarding**
- **Supported SNMP authentication protocols for trap forwarding**
- **SNMP server management**

**Local user passwords**
SHA-384 Hashing algorithm with 64-bit Salt and 1000 iterations are used to hash the password

**Backup files**
Backup files are encrypted with a simple symmetric key cryptography and the key is unique per appliance. This form of encryption helps prevent casual attempts at reading or tampering the backup files. Hewlett Packard Enterprise strongly recommends that you encrypt backup files on the backup server with an encryption key that you generate to ensure confidentiality and the integrity of the backup file.

**Managed device credentials**
Passwords of managed devices and external servers are encrypted with AES-256 algorithm.
Updates
HPE OneView Update binary (update.bin) and the Red Hat package managers (RPM) contained in the update.bin are signed using SHA-512 and 4096-bit RSA key.

Support dumps
Support dumps are encrypted using AES/CTR/No Padding:256 algorithm and the AES key is encrypted separately using 3072-bit RSA asymmetric key pair.

Certificates
By default, on a fresh installation of the HPE OneView appliance, the self-signed certificate is signed using SHA-256 digital signature algorithm with a 2048 bit RSA key. On an upgraded appliance any existing self-signed certificates are retained. If a user has a certificate authority-signed SHA1 certificate, then the SHA1 certificate is retained post upgrade. The user is notified with an alert to regenerate or re-import a higher strength certificate.

Administrator password reset and Hewlett Packard Enterprise support access
S/KEY: A one-time challenge-response password scheme

Supported SSL cipher suites

ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
ECDH-ECDSA-AES256-SHA384
ECDH-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
AES256-SHA256
DH-RSA-AES256-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
ECDH-ECDSA-AES128-SHA256
ECDH-RSA-AES128-SHA256
AES128-SHA256
DH-RSA-AES256-SHA
DH-RSA-AES128-SHA
DH-RSA-AES128-SHA256
ECDHE-RSA-AES256-SHA
DHE-RSA-AES256-SHA
AES256-SHA
ECDHE-RSA-AES128-SHA
ECDH-RSA-AES128-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DHE-DSS-AES128-SHA256
ECDHE-ECDSA-AES256-SHA
ECDH-ECDSA-AES256-SHA
ECDH-RSA-AES256-SHA
ECDHE-ECDSA-AES128-SHA
ECDH-ECDSA-AES128-SHA
DHE-DSS-SEED-SHA
DH-RSA-SEED-SHA
DHE-RSA-SEED-SHA
CAMELLIA128-SHA
CAMELLIA256-SHA
<table>
<thead>
<tr>
<th>SSH service</th>
<th>Algorithms and ciphers supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ciphers</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>aes256-ctr</td>
</tr>
<tr>
<td></td>
<td>aes256-cbc</td>
</tr>
<tr>
<td></td>
<td>aes192-cbc</td>
</tr>
<tr>
<td></td>
<td>aes192-ctr</td>
</tr>
<tr>
<td></td>
<td>aes128-ctr</td>
</tr>
<tr>
<td><strong>Message Authentication Code (MAC)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hmac-sha2-512</td>
</tr>
<tr>
<td></td>
<td>hmac-sha2-256</td>
</tr>
<tr>
<td></td>
<td>hmac-sha1</td>
</tr>
<tr>
<td></td>
<td>hmac-sha1-96</td>
</tr>
<tr>
<td></td>
<td>hmac-md5</td>
</tr>
<tr>
<td></td>
<td>hmac-md5-96</td>
</tr>
<tr>
<td><strong>Key Exchange</strong></td>
<td>ecdh-sha2-nistp384:384</td>
</tr>
</tbody>
</table>

*Table Continued*
### SSH service

<table>
<thead>
<tr>
<th>Algorithms and ciphers supported</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diffie-hellman-group-exchange-sha256</code></td>
</tr>
<tr>
<td><code>ecdh-sha2-nistp256</code></td>
</tr>
<tr>
<td><code>ecdh-sha2-nistp521</code></td>
</tr>
<tr>
<td><code>diffie-hellman-group-exchange-sha1</code></td>
</tr>
<tr>
<td><code>diffie-hellman-group14-sha1</code></td>
</tr>
<tr>
<td><code>diffie-hellman-group1-sha1</code></td>
</tr>
</tbody>
</table>

### Host Key algorithms (for clients)

<table>
<thead>
<tr>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssh-rsa:3072</code></td>
</tr>
<tr>
<td><code>ssh-rsa:2048</code></td>
</tr>
<tr>
<td><code>ssh-rsa:4096</code></td>
</tr>
<tr>
<td><code>ssh-dss:1024</code></td>
</tr>
<tr>
<td><code>ecdsa-sha2-nistp384:384</code></td>
</tr>
<tr>
<td><code>ecdsa-sha2-nistp256:256</code></td>
</tr>
<tr>
<td><code>ecdsa-sha2-nistp521:521</code></td>
</tr>
</tbody>
</table>

### Host Key algorithms (HPE OneView host key algorithms)

<table>
<thead>
<tr>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssh-rsa:2048</code></td>
</tr>
<tr>
<td><code>ssh-dsa:1024</code></td>
</tr>
</tbody>
</table>

### HPE OneView Key-based authentication

<table>
<thead>
<tr>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rsa:2048</code></td>
</tr>
</tbody>
</table>

### Supported RabbitMQ cipher suites

```
ecdh_ecdsa, aes_256_cbc, sha384, sha384
dhe_rsa, aes_256_cbc, sha384, sha384
ecdhe_ecdsa, aes_256_cbc, sha256,
rsa, aes_256_cbc, sha256
ecdhe_rsa, aes_128_cbc, sha256, sha256
ecdh_rsa, aes_128_cbc, sha256, sha256
dhe_rsa, aes_128_cbc, sha256
ecdh_ecdsa, aes_128_cbc, sha256, sha256
ecdhe_rsa, aes_128_cbc, sha256, sha256
dhe_rsa, aes_128_cbc, sha256
```
Supported SNMP authentication protocols for interconnects

MD5
SHA1
SHA-256
SHA-384
SHA-512

Supported SNMP privacy protocols for interconnects

MD5
DES
3DES
AES-128
AES-192
AES-256

Supported SNMP authentication protocols for trap forwarding

MD5
SHA1
SHA-256
SHA-384
SHA-512

Supported SNMP privacy protocols for trap forwarding

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

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.

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**

### Modeling scope-based access control in HPE OneView

<table>
<thead>
<tr>
<th>I want to ...</th>
<th>Learn more</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Implement scope-based access control</td>
<td>• About user accounts</td>
</tr>
<tr>
<td>• &quot;Troubleshoot authorization failures&quot; in the Online help</td>
<td>• About permissions</td>
</tr>
<tr>
<td>• &quot;See more tasks&quot; in the Online help</td>
<td>• About user roles</td>
</tr>
</tbody>
</table>

#### 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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Action semantic</th>
<th>Authorization check semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Controls the right to create a resource.</td>
<td>A permission must grant the user Create rights on the resource category. If a single scope-restricted permission grants Create, the resource is assigned to the permission scope. If multiple scoped permissions grant Create, the desired scope must be specified.</td>
<td>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.</td>
</tr>
<tr>
<td>Delete</td>
<td>Controls the right to delete a resource.</td>
<td>A permission must grant the user Delete 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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

**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 HPE OneView API Reference for more information.
<table>
<thead>
<tr>
<th>Action</th>
<th>Action semantic</th>
<th>Authorization check semantics</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Controls the right to modify a resource. This includes changing the state of a resource.</td>
<td>A permission must grant the user Update 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.</td>
<td>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.</td>
</tr>
<tr>
<td>Read</td>
<td>Controls the right to view a resource.</td>
<td>A permission must grant the user Read rights on the resource category. Read rights are not restricted by scope.</td>
<td></td>
</tr>
</tbody>
</table>
| Use      | 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. **Exception:** Use rights are required to unassign a template (for example, server profile template or volume template) from its associated resource. | A permission must grant the user the following rights:  
• 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. | 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. However, no Use checks are performed when you set the server hardware to unassigned in a server profile or remove a SAN storage volume. |

**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**.

---

**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

Click on the icon for the procedure

Design

1. Describe users and groups who need HPE OneView access
2. Determine the role that best aligns with the desired rights
3. Determine resource to include in scopes to restrict rights

Configure

4. Create permission scopes
5. Assign resources to scopes
6. Create user/group accounts and assign permission
7. Verify user rights

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:

<table>
<thead>
<tr>
<th>HPE OneView main menu</th>
<th>Related role category names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Bundles</td>
<td>firmware-drivers</td>
</tr>
<tr>
<td>Interconnects</td>
<td>interconnects, sas-interconnects</td>
</tr>
<tr>
<td>Logical Interconnect Groups</td>
<td>logical-interconnect-groups, sas-logical-interconnect-groups</td>
</tr>
<tr>
<td>Logical Interconnects</td>
<td>logical-interconnects, sas-logical-interconnects</td>
</tr>
<tr>
<td>Networks</td>
<td>ethernet-networks, fcoe-networks, fc-networks</td>
</tr>
<tr>
<td>Power Delivery Devices</td>
<td>power-devices</td>
</tr>
<tr>
<td>SAN Managers</td>
<td>fc-device-managers</td>
</tr>
<tr>
<td>SANs</td>
<td>fc-sans</td>
</tr>
<tr>
<td>Settings</td>
<td>appliance</td>
</tr>
<tr>
<td>Users and Groups</td>
<td>users, grouptorolemappings</td>
</tr>
<tr>
<td>Volume Templates</td>
<td>storage-volume-templates</td>
</tr>
<tr>
<td>Volumes</td>
<td>storage-volumes</td>
</tr>
</tbody>
</table>

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.
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:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate IT</td>
<td>Senior technologists</td>
<td>HPE OneView appliance and all managed resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Server administrators</td>
<td>All server resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Network administrators</td>
<td>All network resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Storage administrators</td>
<td>All storage resources</td>
</tr>
<tr>
<td>Finance</td>
<td>OS and Application administrators</td>
<td>OS and applications operating on servers assigned to the Finance department</td>
</tr>
<tr>
<td>Human Resources</td>
<td>OS and Application administrators</td>
<td>OS and applications operating on servers assigned to the Human Resources department</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>SRV Cloud provisioning and allocation process</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Cloud IT</td>
<td>Server administrators</td>
<td>All VM Cloud server resources</td>
</tr>
<tr>
<td>VM Cloud IT</td>
<td>Network administrators</td>
<td>All VM Cloud network resources</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate IT</td>
<td>Senior technologists</td>
<td>Infrastructure administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Storage administrators</td>
<td>Storage Administrator</td>
<td>All resources</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Cloud IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>VM Cloud</td>
</tr>
<tr>
<td>VM Cloud IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>VM Cloud</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Rights</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labels</td>
<td>Create, Read, Update, Delete</td>
<td>Allows SRV IT users to assign labels to any resource in a category granted Update 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.</td>
</tr>
<tr>
<td>Network Sets</td>
<td>Create, Read, Update, Delete</td>
<td>Allows SRV IT to create network sets in the SRV Cloud scope.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Server profile architect</td>
<td>SRV Cloud</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Scope operator</td>
<td>SRV Cloud</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Rights</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labels</td>
<td>Create, Read, Update, Delete</td>
<td>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.</td>
</tr>
<tr>
<td>Server Hardware</td>
<td>Read, Update</td>
<td>Aligned with desired privileges.</td>
</tr>
<tr>
<td>Server Profiles</td>
<td>Read, Update</td>
<td>Aligned with desired privileges.</td>
</tr>
</tbody>
</table>

Human Resources and Finance users are granted the following permissions:

<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Finance</td>
</tr>
<tr>
<td>Human Resources</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Human Resources</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Department</th>
<th>Function</th>
<th>Permission Role</th>
<th>Permission Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate IT</td>
<td>Senior technologists</td>
<td>Infrastructure administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Corporate IT</td>
<td>Storage administrators</td>
<td>Storage administrator</td>
<td>All resources</td>
</tr>
<tr>
<td>Finance</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Finance</td>
</tr>
<tr>
<td>Human Resources</td>
<td>OS/Application administrators</td>
<td>Server profile operator</td>
<td>Human Resources</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Server profile architect</td>
<td>SRV Cloud</td>
</tr>
<tr>
<td>SRV Cloud IT</td>
<td>Server Cloud administrators</td>
<td>Scope operator</td>
<td>SRV Cloud</td>
</tr>
<tr>
<td>VM Cloud IT</td>
<td>Server administrators</td>
<td>Server administrator</td>
<td>VM Cloud</td>
</tr>
<tr>
<td>VM Cloud IT</td>
<td>Network administrators</td>
<td>Network administrator</td>
<td>VM Cloud</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create networks</td>
<td>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.</td>
</tr>
<tr>
<td>Create network sets</td>
<td>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.</td>
</tr>
<tr>
<td>Create logical interconnect groups</td>
<td>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.</td>
</tr>
<tr>
<td>Create enclosure groups</td>
<td>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.</td>
</tr>
<tr>
<td>Create logical enclosures</td>
<td>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.</td>
</tr>
<tr>
<td>Power on/off/Refresh interconnects</td>
<td>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.</td>
</tr>
<tr>
<td>Power on/off/Refresh drive enclosures</td>
<td>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.</td>
</tr>
<tr>
<td>Operation</td>
<td>Analysis</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Launch console/Power on/off/Reset/Refresh server hardware</td>
<td>Corporate IT must assign the blades in the VM Cloud enclosures to the VM Cloud scope.</td>
</tr>
<tr>
<td>Create server profile templates</td>
<td>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.</td>
</tr>
<tr>
<td>Create server profiles</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch console/Power on/off/Reset/Refresh server hardware</td>
<td>Corporate IT needs to assign the blades in the SRV Cloud enclosures to the SRV Cloud scope.</td>
</tr>
<tr>
<td>Create server profile templates</td>
<td>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.</td>
</tr>
<tr>
<td>Create server profiles</td>
<td>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.</td>
</tr>
<tr>
<td>Assign SRV Cloud resources to Human Resources and Finance scopes</td>
<td>Both an Update and Use 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 Update rights on the Human Resources scope and Use 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.</td>
</tr>
</tbody>
</table>

Finally, Corporate IT completes the analysis of the Human Resources and Finance scopes.
## Operation Analysis

<table>
<thead>
<tr>
<th>Operation</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch console/Power on/off/Reset/Refresh server hardware</td>
<td>SRV Cloud IT is responsible for assigning SRV Cloud server hardware to the Human Resources and Finance scopes.</td>
</tr>
<tr>
<td>Update server profiles</td>
<td>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.</td>
</tr>
</tbody>
</table>

To summarize, the authentication model for the pilot defines four permission scopes and nine directory group accounts with associated permissions.

### Permission Scope

<table>
<thead>
<tr>
<th>Permission Scope</th>
<th>Resources explicitly assigned to the scope by Corporate IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>None</td>
</tr>
<tr>
<td>Human Resources</td>
<td>None</td>
</tr>
<tr>
<td>SRV Cloud</td>
<td>The blades contained in the two enclosures dedicated to the SRV Cloud pilot. The firmware bundles approved for use by SRV Cloud IT. The networks approved for use by SRV Cloud IT. 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.</td>
</tr>
<tr>
<td>VM Cloud</td>
<td>The three enclosures dedicated to the VM Cloud pilot. The blades contained in the three enclosures. The interconnects contained in the three enclosures. The drive enclosures contained in the three enclosures. The firmware bundles approved for use by VM Cloud IT. The volume templates approved for use by VM Cloud IT.</td>
</tr>
</tbody>
</table>

### Directory Group

<table>
<thead>
<tr>
<th>Directory Group</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CorpIT-FULL</td>
<td>(Infrastructure administrator, All resources)</td>
</tr>
<tr>
<td>CorpIT-NA</td>
<td>(Network administrator, All resources)</td>
</tr>
<tr>
<td>CorpIT-SA</td>
<td>(Server administrator, All resources)</td>
</tr>
<tr>
<td>CorpIT-StA</td>
<td>(Storage administrator, All resources)</td>
</tr>
<tr>
<td>Finance-Admins</td>
<td>(Server profile operator, Finance)</td>
</tr>
<tr>
<td>HR-Admins</td>
<td>(Server profile operator, Human Resources)</td>
</tr>
<tr>
<td>SRVCloudIT-Admins</td>
<td>(Server profile architect, SRV Cloud); (Scope operator, SRV Cloud)</td>
</tr>
<tr>
<td>VMCloudIT-SA</td>
<td>(Server administrator, VM Cloud)</td>
</tr>
<tr>
<td>VMCloudIT-NA</td>
<td>(Network administrator, VM Cloud)</td>
</tr>
</tbody>
</table>
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 offers 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.

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 and the allowed usage of that key (for example, digital signatures, certificate signing, encryption, and so on).

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**
- "Two-factor Authentication using Client Certificates" in the online help

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 access the appliance console and view the appliance self-signed certificate without using HTTPS, connect a laptop or a keyboard, monitor, and mouse to the Synergy frame.

- **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.

In an HPE Synergy environment, securely connecting to the composer, frame link modules, and compute module iLOs is most easily achieved before the initial frame link topology is wired to the management LAN. Also, when you add a new frame or compute module to an existing frame link topology, you need not disconnect from the management LAN. Instead, use the automatic initial trust approach for establishing trust for the new devices.

**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, frame link modules, and the appliance all provide REST APIs for generating CSRs and uploading the resulting CA-signed certificates and CRLs.

See the REST API online help for more information about REST APIs.

**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 frame link modules 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:**

Automatic additions of certificates happens only during discovery. The automatic initial trust approach is used only 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 sections below.

• 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-middle-attack.

Cited below are a few examples:

• **Synergy frame link topology**
  To establish initial trust in an HPE Synergy system using only self-signed certificate, perform hardware discovery of the initial frame link topology before connecting the frame link modules to the management network. When all the devices are isolated from the management network, there is no possibility of a man-in-the-middle attack and all the self-signed certificates are stored securely in the HPE OneView trust store.

  **NOTE:**
  This approach is only applicable during setup of the original frame link topology. As additional frames, remote frame link topologies, or additional compute modules are inserted, the self-signed certificates for those devices must be individually validated using the automatic initial trust approach.

• **For Synergy Gen10 compute modules**
  SSH to HPE OneView and use the following command to connect serially to each of the iLOs and obtain the certificate fingerprint:

  ```
  cd /map1/sslcert1/hpiLO
  show
  ```

  In order for the SSH connection itself to be trusted, the HP OneView SSH host key must be saved during the initial Synergy configuration, before the frame link topology is connected to the management network. This approach only works for compute modules in the 'Production' security mode of the iLO. Alternate approaches require that the iLO be isolated from the management network as described in the Gen9 compute modules section.

• **For Synergy Gen9 compute modules**
  For the Gen9 compute module, the only way to securely obtain a self-signed certificate is to connect to the iLO when the frame is isolated from the frame link topology and is disconnected from the management network. Connect a device with a web browser (such as a laptop) to the management network port of the iLO and browse each iLO to view its certificate fingerprint.

• **Frame Link Modules**
  The console user interface of the Frame Link Module displays its certificate's fingerprint. Frame Link Modules are automatically trusted initially and also after a factory reset of the Frame Link Module.
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 pre-bundled 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 are 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 communication to the remote support server to be trusted and secure:

- 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

**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.

**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 file 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 CRL files downloaded from a CA to the appliance. HPE OneView then validates all certificates signed by the CA against this CRL. CRLs themselves have an expiration date and must be uploaded into the appliance before their expiration.

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.

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
Locate CRL Distribution Points in the HPE OneView Online Help provides details on how to locate the CRL DPs for these certificates.

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.

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

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.

iLO3 and iLO4 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 or not 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 also occur on iLO4-based Synergy Gen9 compute modules in addition to the 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.

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.
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  http://www.hpe.com/support/hpesc

Information to collect

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

Accessing updates

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

- To download product updates:
  Hewlett Packard Enterprise Support Center
  www.hpe.com/support/hpesc
  Hewlett Packard Enterprise Support Center: Software downloads
  www.hpe.com/support/downloads
  Software Depot
  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:
  www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:
  www.hpe.com/support/AccessToSupportMaterials
IMPORTANT:
Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

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

For more information about CSR, contact your local service provider or go to the CSR website:
http://www.hpe.com/support/selfrepair

Remote support

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

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

Remote support and Proactive Care information
HPE Get Connected
www.hpe.com/services/getconnected
HPE Proactive Care services
www.hpe.com/services/proactivecare
HPE Proactive Care service: Supported products list
www.hpe.com/services/proactivecaresupportedproducts
HPE Proactive Care advanced service: Supported products list
www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information
Proactive Care central
www.hpe.com/services/proactivecarecentral
Proactive Care service activation
www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products reference document, go to the Enterprise Safety and Compliance website:
www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information
HPE ProLiant and x86 Servers and Options
www.hpe.com/support/ProLiantServers-Warranties
Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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

Q: Why silicon root of trust? Why not just write-protect the boot block in flash memory?
   A: Flash memory can be replaced and the management processor will attempt to boot off of whatever replaces it. It also provided very little protection against supply chain attacks. Silicon root of trust will only load a boot block that it trusts, regardless of what happens to the physical flash memory.

Q: What is silicon root of trust?
   A: It is a SHA512 hash of the iLO startup code that is permanently part of the silicon. The silicon validates this code before it is fetched and executed.

Q: What is scanned during runtime?
   A: iLO flash memory is scanned. This is analogous to virus scanning your hard drive, only much better. The contents of the flash memory must be exactly right down to the bit, or else the contents are flagged as compromised - which automatically starts the recovery process. The UEFI startup code is also scanned.

Q: I understand that the startup code is protected by a SHA512 in silicon. What about the rest of the iLO firmware?
   A: The individual pieces are signed using CNSA-grade cryptography. Once a firmware module is checked, the modules is loaded and executed.

Q: What is FIPS and how is it important?
   A: For several generations (including the current one), iLO has been FIPS 140-2 level one validated. This means iLO has been tested by an independent lab and verified to meet the security requirements. Things like the random number generator, use of secure algorithms and protocols, keys, and other areas related to security are tested and found to meet the standards. iLO is also tested for Common Criteria and PCI/DSS.

Q: What is ‘FIPS Inside’?
   A: This commonly means that something within a device may have been FIPS validated. In most cases, it means that a chosen set of cryptographic elements contained within has been tested and certified.

Q: Where does iLO keep its private keys?
   A: Keys and other security parameters are kept inside the iLO security boundary. The keys are inaccessible from any interface. The security boundary is protected internally by a security manager. Since iLO does not support accounts with root access, there is no path from the host or any other interface to the inside of the security boundary, regardless of user identity or credentials.

Q: How does CNSA mode work?
   A: In iLO, CNSA mode is a subset of FIPS mode. FIPS restricts cryptography to what is allowed by FIPS. CNSA further restricts it to what is allowed by the US Government for Top Secret installations. CNSA-grade cryptography is available in all iLO security modes.

Q: What kind of performance penalty will I suffer when iLO is in CNSA mode?
   A: Actually, performance is much better! ECDH is faster than conventional Diffie-Hellman. AES is fast because it is hardware accelerated by iLO. For this and security reasons, iLO is set up to prefer these ciphers even in the lower security modes.

Q: Why does iLO have security states? Why not have a lot of security settings instead?
   A: Security states help simplify security, and thus make systems less expensive to operate, and allow customers to know at a glance the true security state of the iLO. Having security states instead of many security settings also simplifies the internal design, reducing the likelihood of security vulnerabilities.
Q: With all of this security, is it possible for me to lock myself out?

A: No, but you can create major difficulties for yourself. If you lose your password, it is possible to put yourself into a situation where recovery is only possible by removing power from the server and then removing the coin battery for an extended period of time. 20-30 minutes with the battery removed is typically required.

Q: The iLO USB Service Port seems like a liability. Can I introduce malware into iLO or the server this way?

A: No. The service port only supports USB keys that are set up to receive AHS logs or USB Ethernet dongles. Anything else is ignored. In the case of Ethernet, the security is the same as with the regular iLO Ethernet port or the iLO sideband Ethernet port. It is encrypted and requires authentication and authorization. If a higher security state is in effect, then the same rules apply. There is no way to boot anything from the iLO service port.

Q: What exactly is secure wipe?

A: Devices that store security parameters or customer identifiable parameters are erased following the NIST 800-88r1 standard. This is invoked through Intelligent Provisioning. Doing this should not be taken lightly because it typically takes about 26 hours to complete. Almost all of this is what it takes to wipe the NAND flash.

Q: Are there any back doors through iLO security?

A: No.