Hewlett Packard
Enterprise

HPE Gen10 Security Reference Guide

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.

Part Number: 882428-001
Published: July 2017
Edition: 1

Notices

Acknowledgments

Contents

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. SUM is security aware and offers only local updates when the HPE iLO HighSecurity mode is active.
- 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, CAC 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, that any potential vulnerabilities will be addressed quickly, and that you can return to authenticated settings quickly if needed.

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**

For more information, see the HPE iLO 5 User Guide available from the HPE Information Library at **http://www.hpe.com/info/enterprise/docs**.

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 code 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 and SSO.

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 comes 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.
- 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 programed 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 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.

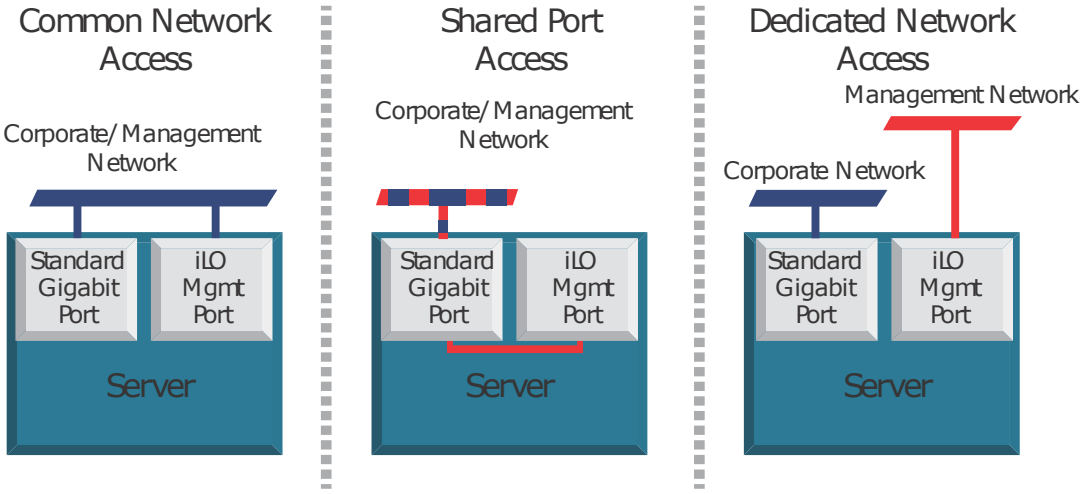

Figure 1: Traffic paths of shared and dedicated networks

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 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:

- **TPM 1.2**
- **TPM 2.0**
- **TM 1.0**
- **TPM Module 2.0 (Intel PTT)**
- **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. It usually has firewalls that restrict traffic flow between the corporate/Internet areas. This architecture lets you access servers that provide publicly available Internet services through a firewall, but 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 in the DMZ require a careful balance between critical security requirements and the need to effectively manage and maintain the systems.

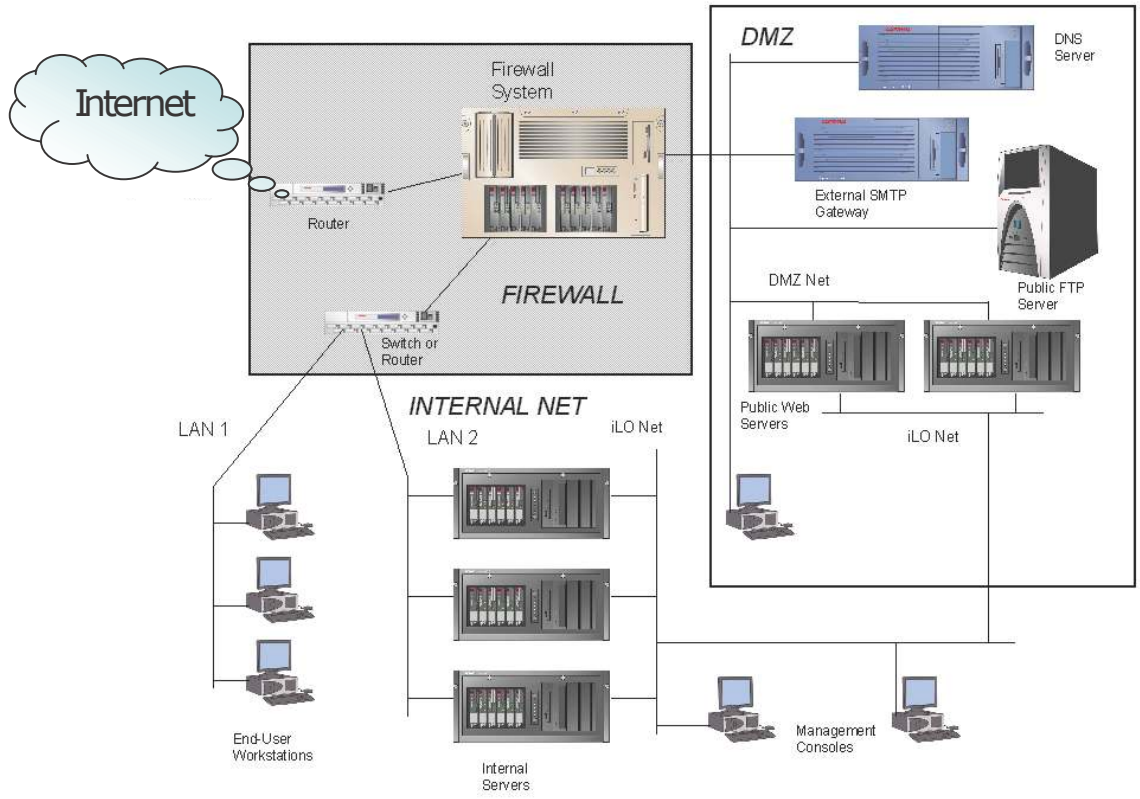

Figure 2: Example configuration of a DMZ

iLO can exist on a separate, secondary network (iLO Net in Figure 14) parallel to the primary or production network. This dual-network architecture segregates management traffic from production network traffic. It allows system-wide server management activities, including servers inside the DMZ, while maintaining maximum security by limiting access to the production network.

The image above shows a packet-filtering router that acts as an initial line of defense. Behind this router is a firewall system. 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 system. 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 multi-targeted 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. There is no possibility for data to flow between the DMZ network and the iLO network because 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 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 10).

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.

The referenced documents, the *HPE iLO 5 User Guide*, and the *HPE iLO 5 Scripting and Command Line Guide*, are available in the HPE Information Library at **http://www.hpe.com/info/ilo/docs**.

Documentation for the iLO RESTful API can found at **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/**.

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.

- The Security Bulletin for this issue may be found at **http://www.hpe.com/support/iLO234-SB-CVE-2013-4786**
- 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** 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.

Running a firmware verification scan

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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.

Configuring the firmware verification settings

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

Procedure

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

An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

Procedure

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

Firmware health status details

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.

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
  - Secure Boot
  - SATA secure erase
  - UEFI Option ROM measurement

SUM security features

SUM is a tool for firmware, driver and software maintenance on ProLiant servers, BladeSystem enclosures, Moonshot systems, and other HPE devices. It provides a browser-based GUI or a command-line scripting interface for flexibility and adaptability.

SUM security features are a function of the environment in which it is installed. While SUM alone does not have specific configurable security functions, it can be blocked by the security settings of iLO.

SUM warns users when the iLO security settings require an approved login on any node which is chosen for updates. If HPE iLO 5 is set to a security mode other than Production mode, a local login is required before it can be updated with SUM. Any security mode other than Production mode will prevent SUM from successfully deploying updates to nodes, and cause SUM to show a warning to the remote user.

NOTE:

In higher security modes (any mode higher than production), you cannot use SUM to directly install secure flash components, TPM components, or NVDIMM components. To install these component types in a high security environment, use SUM to add files or install sets to the iLO installation queue, or install each update individually by using the **Firmware** or **Group Firmware Update** pages in iLO 5 and later.

Future releases of SUM will accommodate higher security modes.

Intelligent Provisioning Security Features

Intelligent Provisioning

Intelligent Provisioning is a single-server deployment tool embedded in ProLiant servers, Apollo systems, 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.

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.

In addition to accessing Intelligent Provisioning by pressing F10 from the POST screen, you can also access Intelligent Provisioning from the iLO web browser user interface using Always On. You can access Always On without having to reboot 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**.

HPE Gen10 recommended security settings

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

iLO 5 settings

Feature or function	Path	Setting	Suggested setting value
TPM or TM status	**Information** > **Overview**	TPM Status	Read only
		Module Type	Read only (displays only when a TPM or TM is present)
Local user account controls	**Administration** > **User Administration**	Add, edit, and delete local users	Up to 12 local accounts, with a range of individual user privilege settings to support the security principle of least access.
Directory group account controls	**Administration** > **Directory Groups**	Add, edit, and delete directory groups	
iLO service settings	**Security** > **Access Settings**	Secure Shell (SSH)	Enabled (also must set port)
		Web Server	Enabled (also must set Non-SSL and SSL ports)[1]
		Remote Console	Enabled (also must set port)
		Virtual Media	Enabled (also must set port)
		SNMP	Disabled
		IPMI/DCMI over LAN	Disabled
iLO access options	**Security** > **Access Settings**	iLO Functionality	Enabled
		iLO Web Interface	Enabled
		iLO RIBCL Interface	Enabled (although HPE recommends using the iLO RESTful API)
		iLO ROM-Based Setup Utility	Enabled
		Require Login for iLO RBSU	Enabled
		Show iLO IP during POST	Enabled
		Virtual Serial Port Log	Enabled

Table Continued

Feature or function	Path	Setting	Suggested setting value
		XML Reply	Disabled (Enable to have the iLO discoverable on your network)
		Serial Command Line Interface	Enabled-Authentication Required (Also must set speed)
		Minimum Password Length	8
		Server Name	Leave blank and let host OS assign
		Server FQDN/IP Address	Leave blank and let host OS assign
		Authentication Failure Logging	Enabled-Every Failure
		Authentication Failure Delay	10 seconds
		Authentication Failures Before Delay	1 Failure causes no delay
iLO Service Port	**Security** > **iLO Service Port**	iLO Service Port	Enabled
		USB flash drives	Disabled
		Require authentication	Enabled
		USB Ethernet adapters	Disabled
SSH key administration	**Security** > **Secure Shell Key**	Keys must be 2048-bit DSA or RSA	Using a smarcard with SSH keys provides better security than simple password authorization.
Certificate to user mapping	**Security** > **Certificate Mappings**	Each local user account must have an associated certificate.	
Smartcards	**Security** > **CAC/ Smartcard**	CAC Smartcard Authentication	Enabled (Requires an iLO Advanced license)
		CAC Strict Mode	(Optional) Enabled
		Import Trusted CA Certificates and revocation list	At least one trusted CA certificated must be installed, along with revocation list.
SSL certificate administration	**Security** > **SSL Certificate**	Customize Certificate	Create a trusted SSL certificate for each iLO. Default self-signed certificates are not secure.

Table Continued

Feature or function	Path	Setting	Suggested setting value
Directory-based authentication	**Security** > **Directory**	LDAP Directory Authentication	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)
		Local User Accounts	Depending on environment, enabled or disabled.
		Kerberos Authentication	Enabled (Also must set Realm, Server Address, Server Port, and Keytab file)
Encryption	**Security** > **Encryption**	Security State	HighSecurity
HPE SSO	**Security** > **HPE SSO**	Single Sign-On Trust Mode	Trust by Certificate[2]
Login security banner	**Security** > **Login Security Banner**	Enable Login Security Banner	Enabled (Also must set a security message)

[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

Feature or function	Path	Setting	Suggested setting value
Security Settings	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security**	Set Power On Password	Password compliant with strong security standards.
		Set Admin Password	Set a password that is compliant with strong security standards.
		Intel TXT Support	Enabled, if available on your system
		One-Time Boot Menu (F11 Prompt)	Disabled
		Intelligent Provisioning (F10 Prompt)	Enabled
		Processor AES-NI Support	Enabled
		Backup ROM Image Authentication	Enabled

Table Continued

Feature or function	Path	Setting	Suggested setting value
		System Intrusion Detection	Enabled
Secure Boot Settings	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings**	Attempt Secure Boot	Enabled[1]
Advanced Secure Boot Options	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options**	Settings for PK, KEK, DB, DBX, and DBT. Also includes controls for deleting all keys, exporting all keys, or resetting all to defaults.	See the *UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HP Synergy*
TLS (HTTPS) Options	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options**	Settings for viewing, enrolling, deleting, and exporting certificates. Also includes controls for deleting, exporting, or resetting all certificates.	See the *UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HP Synergy*
Advanced Security Settings	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Advanced Security Settings**	Cipher suites allowed for TLS connections	Select the allowed ciphers for TLS connections
		Certificate validation for every TLS connection	Peer
		Strict Hostname checking	Enable
		TLS Protocol Version Support	Auto
Trusted Platform Module Options	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Trusted Platform Module Options**	Chipset-TPM	Enable[2]
		Current TPM Type	(Read only)
		Current TPM State	(Read only)
		TPM 2.0 Operation[3]	No Action
		TPM Mode Switch	TPM 2.0
		TPM 2.0 Visibility	Visible
		TPM UEFI Option ROM Measurement	Enabled
SATA Secure erase	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Storage Options** > **SATA Controller Options**	Embedded SATA Configuration	To support secure erase, this option must be set to SATA AHCI Support and the SATA drives installed must support the Secure Erase command.

Table Continued

Feature or function	Path	Setting	Suggested setting value
		SATA Secure Erase	Enable this to allow SATA secure erase functions to work. This control does not start the secure erase function.
UEFI iLO 5 Configuration Utility			
iLO 5 configuration options	**System Utilities** > **System Configuration** > **iLO 5 Configuration Utility**	iLO 5 Functionality	Enabled
		iLO 5 Configuration Utility	Enabled
		Require user login and configuration privilege for iLO 5 Configuration	Enabled
		Show iLO 5 IP Address during POST	Enabled
		Local Users	Enabled
		Serial CLI Status	Enabled
		Serial CLI Speed (bits/second)	As appropriate for your environment
		iLO Web Interface	Enabled

[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 or PTT 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)

Feature or function	Path	Setting	Suggested setting value
Erase devices	Press F10 during POST, or from iLO 5, click **Intelligent Provisioning** > **Always On**. Then click **Perform Maintenance** > **System Erase and Reset**	Erase all hard drives	Enable
		Secure erase of non-volatile storage	Enable
		Clear Intelligent Provisioning preferences	Enable

System Maintenance switch (normal operation)

Feature or function	Path	Setting	Suggested setting value
iLO security bypass	Remove the chassis cover	Position 1	Off
System configuration lock		Position 2	On (after configuration is complete)

Table Continued

Feature or function	Path	Setting	Suggested setting value
Power-on password control		Position 5	On (most secure)
Restore defaults		Position 6	Off

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 improvement 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.

CAUTION:

A TPM locks all data access if you do not follow proper procedures for modifying the server, including updating system or option firmware, replacing hardware such as the system board and hard drive, and modifying TPM OS settings.

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. Disabling iLO security allows login access with all privileges, without a user ID and password, provided that iLO is configured to use the **Production** security state.

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 maintenance and service guide for your server.

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:

- 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.

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 opened 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 the front of 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 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.
- 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 following options to help secure the servers:

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:

- Power on Password
- 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 configuration security

iLO has the following options for secure configuration:

- Local and directory user accounts with configurable privileges
- Separately accessible configuration utility in BIOS
- Password override control via system maintenance switch
- SSH key storage and access control
- HPE Single Sign On capability
- Login Security Banner

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**

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 settings is disabled, however, server-side IPMI/DCMI applications are still functional.

When using IPMI over LAN, the following guidelines are suggested:

- Segment IPMI 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 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

In July 2013, the US-CERT issued an alert (TA13–207A) Risks of Using the Intelligent Platform Management Interface (IPMI) (**https://www.us-cert.gov/ncas/alerts/TA13-207A**).

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

1. Go to **http://www.hpe.com/support/iLO5**.
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.

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.

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

Add SSH keys to iLO user accounts to provide stronger security.

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 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.

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

1. 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.

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. 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:

   - **Login**
   - **Remote Console**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Host BIOS**
   - **Configure iLO Settings**
   - **Administer User Accounts**
   - **Host NIC**
   - **Host Storage**
   - **Recovery Set**
6. To select all available user privileges, click the **select all** check box.
7. 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 Adminisration** 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 **OK**.

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 **iLO Overview** page, 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.

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 apply when you configure the BIOS, Storage, or Network settings through the iLO web interface or the iLO RESTful API. These 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 local user accounts

Procedure

1. Click **Administration** in the navigation tree.

   The **User Administration tab** is displayed.

   The **Local Users** table shows the login names, user names, and assigned privileges of each configured user.
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
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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 **OK**.

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. This value does not apply to OpenLDAP servers.

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 apply when you configure the BIOS, Storage, or Network settings through the iLO web interface or the iLO RESTful API. These 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.
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.
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 "oemhp_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.
   - `oemhp_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:

   ```
   oemhp_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 provides storage to accommodate 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. This protocol uses a key to encrypt and decrypt the data. Generally, the longer the key, the better the encryption.

A certificate is a small data file that connects an SSL key to a server. The certificate contains the server name and the server public key. Only the server has the corresponding private key, and this is how it is authenticated.

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 security of the iLO processor.

Viewing SSL certificate information

Procedure

1. 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)**

   For more information, see **CSR input details** on page 43.
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 use this input.

5. Click **Generate CSR**.

   A message notifies you that a certificate 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 (SAN). This information is typically included in the **Additional Attributes** box. If necessary, enter the iLO DNS short name and IP address in the **Additional Attributes** box by using the following syntax: `san:dns=<IP address>&dns=<server name>`.

   The CA generates a certificate in PKCS #10 format.
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.

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.

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.

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.

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 45 or **Importing a direct DNS name** on page 45.
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 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.

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

1. 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**.
4. The EULA confirmation opens.

   The EULA details are available in the License Pack option kit.
5. Click **OK**.

   The license key is now enabled.

Viewing license information

Procedure

1. 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 (**http://www.hpe.com/downloads/software**).
- Obtain access to software updates in the HPE Update Center (**http://www.hpe.com/downloads/software**).
- 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 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.
- A free iLO evaluation license key is available for download from the following website: **http://www.hpe.com/info/tryilo**.

UEFI configuration security

UEFI provides the following secure configuration options:

- Regular and advanced network options
- User management
- iLO 5 access and functionality controls
- Factory default reset
- Smart Array Controller configuration
- NIC and FCoE configuration

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. Additionally, Intel based platforms are compatible with a firmware based TPM 2.0 called Intel PTT (Platform Trust Technology).

  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 to 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** (active connections)
- **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 (for example, `ilo` instead of `ilo.example.com`).

  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, including:

New User iLO 5 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.

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 **New User iLO 5 Privileges**.
3. For each option, select one of the following settings.
   - **YES** (default)—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 name you want to edit or delete.
3. Select one of the following.
   - **Delete**—Deletes the user name.
   - **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 Configuration Utility.

  If this setting is **Enabled**, a login dialog box opens when you access the iLO 5 Configuration Utility.
- **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 processer 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.

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.

ESC	SCRL LCK	0	f
L_ALT	SYS RQ	1	g

Table Continued

R_ALT	PRINT SCREEN	2	h
L_SHIFT	F1	3	I
R_SHIFT	F2	4	j
L_CTRL	F3	5	k
R_CTRL	F4	6	l
L_GUI	F5	7	m
R_GUI	F6	8	n
INS	F7	9	o
DEL	F8	;	p
HOME	F9	=	q
END	F10	[	r
PG UP	F11	\	s
PG DN	F12	]	t
ENTER	SPACE	`	u
TAB	'	a	v
BREAK	,	b	w
BACKSPACE	-	c	x
NUM PLUS	.	d	y
NUM MINUS	/	e	z

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 use SUM to directly install iLO Secure Flash components, TPM components, or NVDIMM components. To install these component types, use SUM to add files or install sets to the iLO installation queue, or install each update individually by using the iLO **Firmware** or **Group Firmware Update** pages.
- 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 61.

- 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 use SUM to install iLO Secure Flash components, TPM components, or NVDIMM components. Use the iLO **Firmware** or **Group Firmware Update** pages to install these components.

  You cannot use SUM to directly install iLO Secure Flash components, TPM components, or NVDIMM components. To install these component types, use SUM to add files or install sets to the iLO installation queue, or install each update individually by using the iLO **Firmware** or **Group Firmware Update** pages.
- 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.

SuiteB

The SuiteB security state (also called CNSA 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 SuiteB requirements defined by the NSA, and intended to secure systems used to hold United States government top secret classified data.
- You cannot use SUM to directly install iLO Secure Flash components, TPM components, or NVDIMM components. To install these component types, use SUM to add files or install sets to the iLO installation queue, or install each update individually by using the iLO **Firmware** or **Group Firmware Update** pages.
- 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 **SuiteB** security states, see **Enabling the FIPS and SuiteB security states** on page 60.

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. To end your browser connection and restart iLO, click **Apply**.

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

5. After you select the **Production** or **HighSecurity** security state and click **Apply**, 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 SuiteB security states

Use this procedure to configure iLO to use the **FIPS** and **SuiteB** **security states**. To configure iLO to use the **Production** or **HighSecurity** security states, see **Enabling the Production or HighSecurity security state** on page 59.

To configure iLO in a FIPS-validated environment, see **Configuring a FIPS-validated environment with iLO** on page 61.

The FIPS security state might be required for Common Criteria compliance, Payment Card Industry compliance, or other standards.

Prerequisites

- Configure iLO Settings privilege
- If you plan to enable the optional SuiteB security state, an iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.
- The default iLO user credentials are available.

Procedure

1. Optional: Capture the current iLO configuration by using HPONCFG.

   For more information, see 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**.

   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.

   iLO prompts you to confirm the request.
5. To confirm the request to enable the FIPS security state, click **OK**.

   iLO reboots with the FIPS security state enabled. Wait at least 90 seconds before attempting to re-establish a connection.
6. Optional: Enable the **SuiteB** security state.
   a. Log in to iLO by using the default iLO credentials.
   b. Click **Security** in the navigation tree, and then click the **Encryption** tab.
   c. Select **SuiteB** in the **Security State** menu, and then click **Apply**.

      iLO prompts you to confirm the request.
   d. To confirm the request to enable **SuiteB**, click **OK**.

      iLO reboots with the SuiteB 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 in FIPS mode. 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: Edit and restore the iLO configuration by using HPONCFG for Linux.

   User credentials are required when you restore the configuration.

   HPONCFG for Windows is not supported when iLO is configured to use the FIPS or SuiteB security state.

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 a system is using FIPS mode.

Connecting to iLO when using the HighSecurity, FIPS, or SuiteB security states

After you change security states, iLO requires that you connect through secure channels by using an AES cipher.

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 SuiteB security states are enabled.
- Only HPONCFG for Linux is supported. HPONCFG for Windows is not currently supported.

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 SuiteB security states** on page 60.

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

1. 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.

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

FIPS or HighSecurity

- AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
- diffie-hellman-group14-sha1 key exchange
- hmac-sha2-256 or AEAD_AES_256_GCM MACs

SuiteB

- AEAD_AES_256_GCM and AES256-GCM ciphers
- ecdh-sha2-nistp384 key exchange
- AEAD_AES_256_GCM MAC

SSL cipher and MAC support

SSL cipher and MAC support

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.

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

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)

SuiteB

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)

Encryption protocols, directory integration, access control, and auditing

HPE iLO allows administrators to choose the type of directory integration and it's associate access control, the encryption for it, 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.

   For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.
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.
2. Select **Use Directory Default 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. 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** 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**.
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. Optional: 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 FQDN or IP address of a directory server in the **Directory Server Address** box.
5. Enter the directory server port number in the **Directory Server LDAP Port** box.
6. Enter the location of this iLO instance in the directory tree in the **iLO Object Distinguished Name/CAC LDAP Service Account** box.
7. Enter valid search contexts in one or more of the **Directory User Context** boxes.
8. Click **Apply Settings**.
9. 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**.
10. 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**.
11. To test the communication between the directory server and iLO, click **Test Settings**.
12. Optional: To configure directory groups, click **Administer Groups** to navigate to the **Directory Groups** page.

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.

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 Smartcard Authentication settings

Prerequisites

- Install an iLO license that supports this feature. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.
- 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**.
4. Optional (for directory integration): Select an option in the **Directory User Certificate Name Mapping** section.

   This setting identifies which portion of your user certificate will be used to identify your user name. Use the identified portion as your user name when accessing iLO.
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. **Upload and map a smartcard certificate** to a local iLO user account (when using iLO with local user authentication only).

CAC smartcard authentication settings

Authentication Options

- **CAC Smartcard Authentication**—Enables and disables authentication through a common access smartcard.

  When CAC Smartcard Authentication is enabled, you cannot use SUM to install iLO Secure Flash components, TPM components, or NVDIMM components. To install these component types, install each update individually by using the iLO **Firmware** or **Group Firmware Update** pages.
- **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.

Directory User Certificate Name Mapping

- **For Directory Username**—Allows you to select the portion of the installed directory user certificate to use for your 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.

Managing trusted certificates for CAC Smartcard Authentication

Importing a trusted CA certificate

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

Procedure

1. Click **Security** in the navigation tree, and then click the **CAC/Smartcard** tab.
2. Scroll down the page 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

Import a CRL to invalidate previously issued certificates that have been revoked.

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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 **Manage 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 certificate revocation list

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

Procedure

1. Click **Security** in the navigation tree, and then click the **CAC/Smartcard** tab.
2. Scroll down the page to the **Manage 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. If no certificate is mapped to a local user account, the system displays all zeroes for that user. Use the controls on this page to add or delete a certificate.

In a smartcard or CAC environment (enabled on the **CAC/Smartcard** tab), 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.
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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.

   The **Certificate Thumbprint** column displays all zeroes when a user account does not have a saved certificate.
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.
- An iLO license that supports this feature is installed. For more information, see the following website: **http://www.hpe.com/info/ilo/licensing**.

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.

   The **Certificate Thumbprint** column displays all zeroes when a user account does not have a saved certificate.
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 SuiteB security state, you must use an AES or 3DES Kerberos key type.

kvno

Override key version number.

> **IMPORTANT:**
>
> Do not use this parameter. This option causes the `knvo` 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
keysize 69 HTTP/iloname.example.net@EXAMPLE.NET ptype 3
(KRB5 _NT_SRV_HST) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x5a5c7c18ae23559acc2 9d95e0524bf23)
```

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.
4. Double-click `network.negotiate-auth.trusted-uris`.
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 79.

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.

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. For more information, see **Tools for configuring multiple iLO systems at a time** on page 91.

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

1. Download the Directories Support for ProLiant Management Processors package from the following website: **http://www.hpe.com/support/ilo5**.
2. Install the .NET Framework 2.0 or later on the target server.

   The .NET Framework 2.0 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.

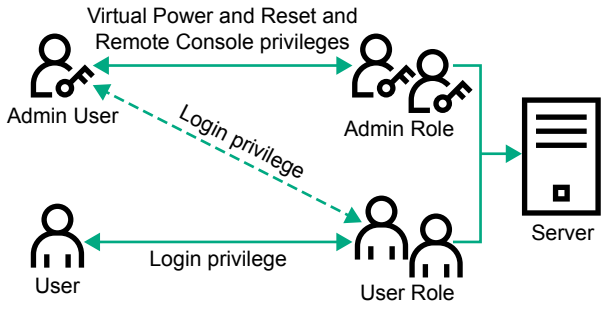

Figure 3: Multiple roles (overlapping)

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)**.

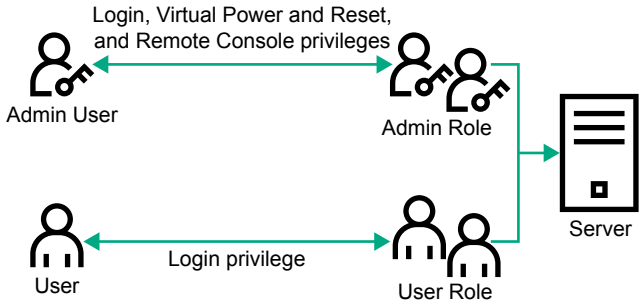

Figure 4: Multiple roles (separate)

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.

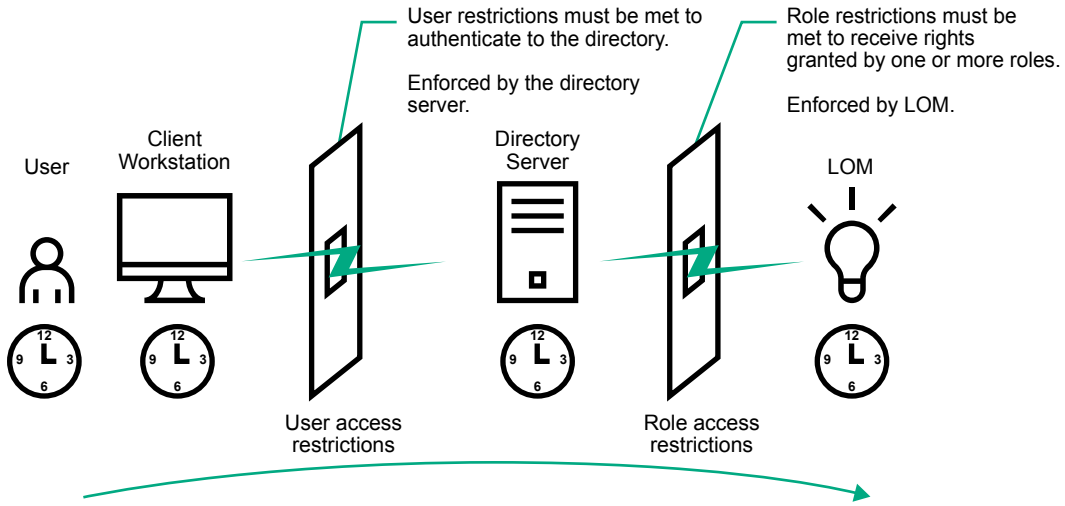

Figure 5: Directory login restrictions

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.

IP 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.

IP 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.

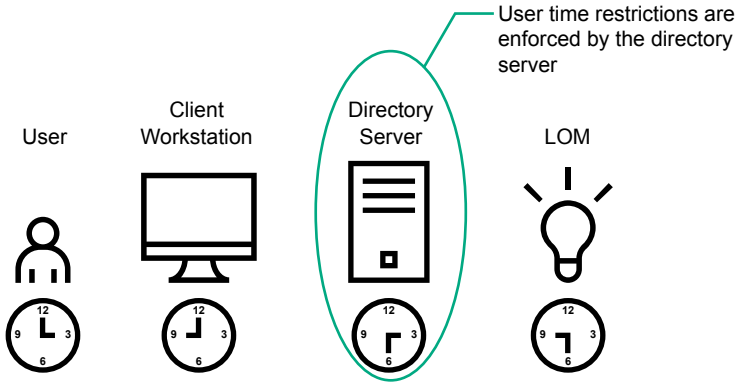

Figure 6: User time restrictions

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.

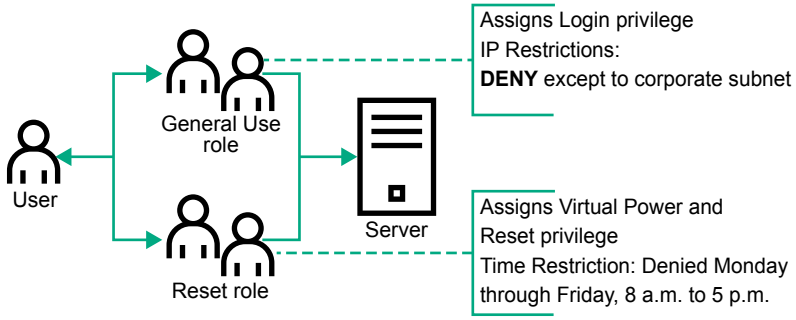

Figure 7: Creating restrictions and roles

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**.

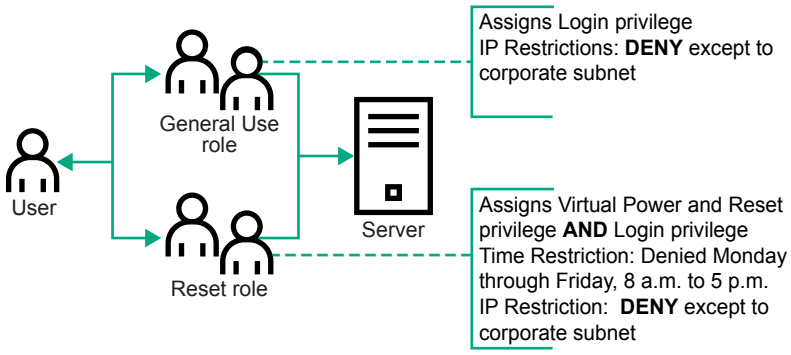

Figure 8: Restricting the Reset and General Use roles

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\user name` 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)
- Processor AES-NI Support
- 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

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Set Power On Password**.
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:

A TPM locks all data access if you do not follow proper procedures for modifying the server, including updating system or option firmware, replacing hardware such as the system board and hard drive, and modifying TPM OS settings.

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 1.2, FIPS**
     - **TPM 2.0**
   - **TPM 2.0 Visibility**—Sets whether TPM is hidden form 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**
  - **Chipset-TPM**—This option is visible only when there is no physical TPM chip installed. This option sets the state of a virtual TPM, for example the Intel PTT. 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.

   A File Explorer screen shows attached media devices.
5. 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.

Example: Exporting an Allowed Signatures Database signature

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Secure Boot Settings** > **Advanced Secure Boot Options** > **DB - Allowed Signatures Database** > **Export Signature** > **HPE UEFI Secure Boot 2016 DB Key**.
2. Select the entry you want to export.

   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 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**.

   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 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

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **TLS (HTTPS) Options** > **Advanced Security Settings**.
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:
  a. Select **TLS Protocol Version Support**.
  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.

Prerequisites

Before you can enable Intel (R) 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. A virtual TPM is not on by default and must be enabled manually.

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.

Firmware updates

HPE Gen10 ProLiant server firmware can be updated from:

- iLO web interface - Recommended for smaller updates, such as for a single system.
- Intelligent Provisioning - Ideal for initial firmware updates when provisioning new systems.
- Smart Update Manager (SUM) - Recommend for one-to-many updates, such as updating groups of servers in a data center. HPE recommends the use of SUM for all firmware updates.

Updated firmware installation requires specific procedures, based on the firmware type, when you use the HPE iLO 5 web interface to set a security state that is higher than production mode.

Available firmware update methods with iLO 5 security states engaged

HPE recommends that you update all firmware before raising the iLO security state. While the iLO 5 security state HighSecurity can be rolled back to Production state to facilitate embedded firmware updates (other states require resetting iLO to defaults), firmware updates when iLO 5 security is set to a state higher than Production or HighSecurity require some planning. The first step is separating single-system updates (one to one) from multi-system updates (one to many).

- For single component updates, load the smart component files into the iLO 5 repository and apply them using the tools available in the iLO 5 web interface.
- For one to many iLO updates, use an SPP and SUM.

You cannot use iLO 5 to update operating system device drivers and other OS software when iLO 5 is set to a higher security state than Production. While iLO 5 security states higher than Production do not block OS updates, neither does it support them. All OS device driver and software updates must be done separately from the tools available in iLO 5.

Note that CAC/Smartcard mode runs optionally in addition to other security modes. SUM does not support local or remote OS driver and software updates when smartcard mode is enabled, regardless of the iLO 5 security state.

Upgrading firmware with iLO security enabled

Procedure

1. **Single-system firmware updates with iLO 5 security enabled**.
2. **Updating firmware at scale with SUM and SPP when iLO security is enabled**.

Single-system firmware updates with iLO 5 security enabled

Prerequisites

- Downloaded the smart component/RPM firmware from HPE.com, and extracted the flashable binary file
- Configure iLO Settings privilege

Procedure

1. Extract the archived download using standard tools in the operating system.

   If you are extracting files from an SPP, you can search a catalog of the included files. Open the bp#.xml catalog file and run a search for your component.
2. In iLO, click **Firmware & OS Software** in the navigation tree, and then click the **iLO Repository** tab.
3. Click **Upload to iLO Repository**.
   a. Select **Local** file.
   b. Click **Browse...**
   c. Choose the local file that you extracted from the download and then click **Open**.

Remember to select both the component files and their associated .compsig (signature) files. Either cpxxxxx.exe files (for Windows) or .rpm files (for Linux) may be selected. Signature files are required when uploading to the repository so that iLO can validate the component.

d. Click **Upload**.

iLO notifies you that uploading a component with the same name as an existing component will replace the existing component. Components that are part of the recovery install set are locked and cannot be replaced by uploading a new component with the same name. To replace a component in the recovery install set, log in with an account that has the System Recovery privilege, and then delete the recovery install set.

e. Click **OK**.

The upload starts. The upload status is displayed at the top of the iLO web interface.

4. Click the install component icon () next to the component you want to install.

Depending on the secure flash component being updated, you may have to reboot either the system or iLO when finished installing updates.

Updating firmware on multiple systems with SUM and SPP when iLO security is enabled

This procedure includes using SUM and an SPP to upload firmware files to an iLO repository.

Prerequisites

- Downloaded a Service Pack for ProLiant from HPE.com
- Configure iLO Settings privilege
- iLO security set to HighSecurity, FIPS, or higher

Procedure

1. Uncompress or mount the downloaded SPP.

Use third party OS tools as needed.

2. Run the included version of SUM.

When you run the included version of SUM, the SPP is automatically added to the baseline. If it is not, or you are running SUM but not the included version, **see the instructions here**.

3. Add an iLO as a node, assign a baseline and perform an inventory.

The credentials you provide when you add the iLO node to SUM makes it possible for SUM to add firmware files to the iLO repository.

For detailed instructions see **Adding a single node by IP or DNS name**.

4. Click **Actions** > **Review/Deploy**

a. Click the **Installation Options** tab.

b. Select **Upgrade Firmware** from the **Options** menu.

This selection is important because you cannot upgrade operating system software using this method when iLO is in a higher security mode.

c. Click the **iLO Repository Options** tab, and then select **Save Components as in Install Set on iLO Drive**.

5. Click **Deploy**.

SUM sends the firmware files for the components identified as needing updates to the iLO Repository. Both SUM and iLO will show the progress of the upload.

6. In iLO, go to the **Install Sets** page and click the install icon for the install set that was just created.

7. Reboot the server.

Adding a baseline

Procedure

1. On the Baseline Library screen, click **Add Baseline**.

   NOTE:

   If you want to clear the Add baselines screen, click **Start Over**.

   SUM opens the add baseline screen.
2. Select **Add Baseline** or **Create Custom**.
3. Select the type of baseline you want to add and include the required information:

   Browse SUM Server Path

   A directory or file share that the system running SUM can access.

   Enter the directory path to the baseline, or click **Browse** and use the menu to navigate to the directory.

   NOTE:

   If you are adding an SPP, navigate to the `/packages` directory.

   UNC path (for example \\host\dir)

   This location uses UNC paths that the system can access. In the **Enter URI for the baseline** field, enter the UNC address for the source baseline. Enter the username and password.

   NOTE:

   UNC path is only supported in Windows systems.

   SUM does not support mapped UNC drives.

   Download from http share

   Enter directory path: Enter, or browse to, the directory where you want to save the baseline. If required, create a directory.

   Enter HTTP URL: Enter an HTTP URL where a bundle file is saved. The server can be local or remote, and you can use an Apache, Tomcat, or IIS server. Provide the complete URL, including the bundle XML. The components must reside in the same directory as the bundle XML. Make sure that you have enough local free space for the baseline.

   If you want to download components only for specific operating systems, select the operating systems in the **OS Filter Options**.

   NOTE:

   SUM adds all baselines it finds in a directory.
4. Click **Add**.

   To see the status of the baseline, check the activity log. If the baseline does not appear in the baseline list, make sure that there are updates in the directory.

   NOTE:

   SUM begins to inventory a baseline as soon as you finish adding the baseline. Wait until the baseline inventory finishes before adding another baseline.

Adding a single node by IP or DNS name

Procedure

1. From the Nodes screen, click **+Add Node**.
2. Select **Add a single node or known range of nodes**.
3. Enter the IP address, DNS name, range of IP addresses, or multiple addresses separated by comma. For example, entering 10.0.1.1–10.0.1.20 adds 20 nodes. 10.0.1.1, 10.0.1.2, 10.0.1.7 adds three nodes. If the nodes use the same credentials, SUM adds the nodes.

   NOTE:

   If you are adding a VC node, use the IP address of the primary Enet module. All VC modules installed, including FC modules, are updated through the primary Enet module.

4. Enter a description for the node.
5. In the **Type of node to add** field, select the node type. If you do not know the node type, select **Unknown** . During the inventory process, SUM determines the node type. If you are adding a node from a Deployment Type screen, SUM automatically selects the node type.

   Some nodes allow SUM to discover and add associated nodes automatically.

   NOTE:

   Selecting the correct node type might help SUM complete adding the node faster.

6. (Optional) Select the baseline, additional package, or both to apply to this node.
7. (Optional) Select a group from the list.
8. Select one of the following:
   - **Use current credentials (requires existing trust relationship with the node)** : This option is for Windows nodes only.
   - **Enter administrator credentials**: Enter the username and password for a user with administrator privileges on the node. Windows users can use `domain\username` if the user has administrator permission.
9. Linux nodes allow you to use sudo credentials to deploy updates without logging in to the node with root credentials. To use sudo commands, you have to install sudo capabilities on the node.

   NOTE:

   Super user and sudo are not available for all nodes.

   If you want to use sudo, in the **Access Level** field, select one of the following:
   - Click **Use sudo to update components** if you want to use sudo credentials.
   - Click **Enter super user credentials to update components** if you want to enter super user credentials.

   NOTE:

   If you are using super user credentials, enter normal user credentials in the **Credentials** field, and then add super user credentials in the **Access Level** field. SUM first logs in using the normal user credentials, and then uses the super user credentials to log in to the super user account.

10. Click **Add**.

    In the **Added Nodes** section, SUM displays the nodes you selected.

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.

  See complete instructions for using Intelligent Provisioning to install an operating system in the *Intelligent Provisioning User Guide for HPE ProLiant Gen10 Servers and HPE Synergy* on the HPE Information Library at **http://www.hpe.com/info/intelligentprovisioning/docs**.
- 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**.

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.

Option	Description
All hard drives	Erase all hard drives on this server.
Wipe hard drives	Displays if **All Hard Drives** is selected. Writes a data pattern over all sectors. This will take several hours per hard drive.
Secure Erase of Non-Volatile Storage[1]	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. **IMPORTANT:** The Secure Erase of Non-Volatile Storage feature needs an iLO Advanced Secure License in order to be displayed and functioning in the GUI. See the *HPE iLO Licensing Guide* for more information.
Intelligent Provisioning Preferences	Clear Intelligent Provisioning preferences.

[1] *Erases using the guidelines from DoD 5220.22-M Date Wipe.*

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

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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