Hewlett Packard
Enterprise

HPE Compute Security Reference Guide

Part Number: 30-2905B658-009
Published: May 2024
Edition: 9

HPE Compute Security Reference Guide

Abstract

This document describes security features supported by Hewlett Packard Enterprise Gen10, Gen10 Plus, and Gen11 servers and compute modules with HPE iLO 5 and HPE iLO 6. This document is for individuals who are responsible for the secure configuration and operation of HPE servers and compute modules.

Part Number: 30-2905B658-009
Published: May 2024
Edition: 9

Notices

Acknowledgments

Revision history

Part number	Publication date	Edition	Summary of changes
30-2905B658-009	May 2024	9	• Added information about TLS 1.3 • Updated the One-button secure erase table.
30-2905B658-008	April 2024	8	• Updated the Server identity section.
30-2905B658-007	January 2024	7	Edited Chassis intrusion detection switch for clarity.

Table of contents

HPE Compute security features

Hewlett Packard Enterprise Compute security features are designed to meet security challenges by continually improving the hardware and firmware security of Gen10, Gen10 Plus, and Gen11 platforms and related hardware environments. The security features ensure that every link in the chain of security provides effective protection.

The features described in this guide might not be supported by every product. To verify feature support for your product, see the **product documentation** or **QuickSpecs**.

Compute Ops Management

Compute has evolved into a distributed service that enables digital transformation and is available everywhere. But legacy management tools are complex and error prone. Compute Ops Management helps you to secure, automate, and unify compute management.

You can use Compute Ops Management to manage the full lifecycle of your entire compute environment with a single, as-a-service experience.

For more information, see Cloud-based management.

iLO licensed features

iLO (Standard) is preconfigured on HPE servers without an additional cost or license. Some features that enhance security and productivity require an iLO Advanced license. In addition to features you can manage through the iLO web interface, command line, and scripting tools, an iLO Advanced license enables features such as Server Configuration Lock and Smart Array Secure Encryption. For more information, see the iLO licensing guide: **https://www.hpe.com/support/iLOLicenseGuide-en**.

Supply chain security

Hewlett Packard Enterprise server security starts with the supply chain and extends throughout the product life cycle.

Subtopics

HPE Trusted Supply Chain

Server Configuration Lock

Chassis intrusion detection switch

Platform certificates

HPE Platform Certificate Verification Tool

HPE Trusted Supply Chain

The HPE Trusted Supply Chain provides a first line of defense against cyber attackers with supported servers built to heightened security standards in secured facilities. HPE Trusted Supply Chain combines security, processes, and people to deliver protection for the most sensitive applications and data even before the server is deployed.

- HPE Trusted Supply Chain server configuration—Add this service to supported servers to ensure that your server is built with the highest security standards in a secured facility in the USA.
- HPE Server Security Optimized Service for HPE ProLiant—Add this service to supported servers to ensure that your server is hardened by turning on advanced safeguards against cyber-exploits throughout the server life cycle.

Subtopics

HPE Trusted Supply Chain server configuration

HPE Server Security Optimized Service for HPE ProLiant

HPE Trusted Supply Chain server configuration

Servers with the HPE Trusted Supply Chain configuration ship with the following characteristics:

Country of origin USA

Built in secure Hewlett Packard Enterprise facilities in the USA, with conformance requirements, each server is inspected and verified to be free from malicious microcode and counterfeit parts, safeguarding it against cyber exploits throughout its life cycle.

Hardened security built in

HPE Trusted Supply Chain hardens the protections designed into select HPE products with unrivaled supply chain visibility and standards compliance providing a 360° view and mitigation plan for current and emerging cyber threats.

Trusted authenticity

HPE Trusted Supply Chain provides protection with HPE employees assigned to the product build to manage the product manufacturing process that adheres to the strictest sourcing, inspection, and traceability standards.

Unique labeling

HPE Trusted Supply Chain products include a **T** in the server model name, for example, HPE ProLiant DL380T. A Trusted Supply Chain sticker is placed on the product hardware.

iLO security state: High Security

Configuring iLO to use High Security mode reduces the attack surface for cyber attackers, making it more difficult to insert compromised code or malware into the server firmware. This security state locks down the host and requires specific authentication through encryption before a user can log into the server.

UEFI Secure Boot feature: Enabled

For customers who ask Hewlett Packard Enterprise to load an OS at the factory, enabling UEFI 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. An industry-recognized feature, secure boot ensures that the genuine and authenticated OS is initialized by preventing the loading of unauthenticated BIOS components and OS bootloaders.

If a customer chooses to load the OS on their own, they can configure this feature when the HPE Trusted Supply Chain server is delivered to the end-user location.

HPE Server Configuration Lock: Enabled

This feature takes cryptographic measurements, or images, of the supported HPE Trusted Supply Chain server firmware, hardware components, and options. It creates a digital fingerprint of the server configuration. If any firmware, hardware, or options are altered, an alert is displayed at startup.

Enabling this feature at the factory essentially prevents all tampering or compromise to the server composition, no matter how slight. This feature uses a password, created by Hewlett Packard Enterprise, to lock down the server configuration at the factory. The password is securely transmitted to the customer, who unlocks the server when it arrives.

For customers who need to perform additional configuration steps, perhaps through a reseller or partner, the password can be used to unlock and then relock the server before it ships to the end-user location.

HPE chassis intrusion detection switch: Enabled

This mechanism protects the HPE Trusted Supply Chain server from physical intrusion. Complementing and reinforcing the protection from the Server Configuration Lock, the chassis intrusion detection switch registers an alert if the top of the server chassis is removed. It logs an event in the iLO firmware, even if the server is powered off. If any cyber attacker or unauthorized personnel open the server chassis, the customer will know that someone might have tampered with the server.

More information

Silicon root of trust
iLO security states
Server Configuration Lock
Chassis intrusion detection switch

Secure boot

HPE Server Security Optimized Service for HPE ProLiant

Servers with the HPE Server Security Optimized Service for HPE ProLiant option ship with the following characteristics:

iLO security state: High Security

Configuring iLO to use High Security mode reduces the attack surface for cyber attackers, making it more difficult to insert compromised code or malware into the server firmware. This security state locks down the host and requires specific authentication through encryption before a user can log into the server.

UEFI Secure Boot feature: Enabled

For customers who ask Hewlett Packard Enterprise to load an OS at the factory, enabling UEFI 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. An industry-recognized feature, secure boot ensures that the genuine and authenticated OS is initialized by preventing the loading of unauthenticated BIOS components and OS bootloaders.

If a customer chooses to load the OS on their own, they can configure this feature when the HPE Trusted Supply Chain server is delivered to the end-user location.

HPE Server Configuration Lock: Enabled

This feature takes cryptographic measurements, or images, of the supported HPE Trusted Supply Chain server firmware, hardware components, and options. It creates a digital fingerprint of the server configuration. If any firmware, hardware, or options are altered, an alert is displayed at startup.

Enabling this feature at the factory essentially prevents all tampering or compromise to the server composition, no matter how slight. This feature uses a password, created by Hewlett Packard Enterprise, to lock down the server configuration at the factory. The password is securely transmitted to the customer, who unlocks the server when it arrives.

For customers who need to perform additional configuration steps, perhaps through a reseller or partner, the password can be used to unlock and then relock the server before it ships to the end-user location.

HPE chassis intrusion detection switch: Enabled

If this feature is included in the configuration, it is enabled as part of this service option.

This mechanism protects the HPE Trusted Supply Chain server from physical intrusion. Complementing and reinforcing the protection from the Server Configuration Lock, the chassis intrusion detection switch registers an alert if the top of the server chassis is removed. It logs an event in the iLO firmware, even if the server is powered off. If any cyber attacker or unauthorized personnel open the server chassis, the customer will know that someone might have tampered with the server.

More information

Silicon root of trust
iLO security states
Server Configuration Lock
Chassis intrusion detection switch
Secure boot

Server Configuration Lock

Server Configuration Lock protects a server against tampering or compromise to the server composition. You can enable this feature when a server is in transit or use it all the time to monitor for configuration changes.

HPE Trusted Supply Chain servers ship with this feature enabled and the server is set to `in-transit` status. HPE creates the Server Configuration Lock password and it is securely transmitted to the customer. On first boot, the customer enters the password to disable the `in-transit` status. At this time, they can disable or modify the feature configuration.

Server Configuration Lock creates a digital fingerprint of the server configuration. The digital fingerprint is a securely stored log file on the server TPM 2.0 (if supported) or in the server nonvolatile memory.

Server Configuration Lock monitors the server for:

- DIMM changes
- CPU changes
- PCIe device changes
- Security configuration changes
- System firmware revisions
- Server Configuration Lock password authentication failures

If a configuration change is detected during POST, an administrator must enter the Server Configuration Lock password to review the issue and continue the startup process. The configuration change is recorded in the Integrated Management Log (IML). A count of the detected issues is available in the Server Configuration Lock detection log in the UEFI System Utilities.

You can configure Server Configuration Lock in the UEFI System Utilities or by using the iLO RESTful API.

IMPORTANT:

When you use Server Configuration Lock, remember to record the password securely. By design, this security feature prevents bypassing or resetting the password when it is lost or forgotten.

For configuration instructions, including the steps to disable `in-transit` status, see the Server Configuration Lock User Guide for HPE ProLiant servers and HPE Synergy at the following website: **https://www.hpe.com/info/server-config-lock-UG-en**.

More information

HPE Trusted Supply Chain server configuration
HPE Server Security Optimized Service for HPE ProLiant

Chassis intrusion detection switch

Supported products are available with a chassis intrusion detection switch. The chassis intrusion detection switch detects any physical intrusion into the chassis. iLO logs an event when the access panel is opened or closed. Chassis intrusion monitoring and iLO reporting activities occur regardless of the server power state.

You can configure various alerting mechanisms (Remote SysLog, SNMP, or AlertMail) to notify you when a chassis intrusion event occurs. For more information about configuring alerts, see the iLO or iLO RESTful API documentation in the Hewlett Packard Enterprise Support Center (**https://www.hpe.com/support/hpesc**).

To verify server support for this feature, check the server QuickSpecs document at the following website: **https://www.hpe.com/info/qs**.

Platform certificates

On supported Hewlett Packard Enterprise servers, HPE iLO can be provisioned with a **Trusted Computing Group** (TCG)-compliant platform certificate. A platform certificate is an attribute certificate that functions as a signed manifest of the detailed hardware and firmware configuration of the server as built by Hewlett Packard Enterprise.

Platform certificates are used to detect supply chain tampering. When a customer receives a server, they can use the HPE Platform Certificate Verification Tool (PCVT) to compare the server state to the platform certificate.

iLO does not allow you to update or delete the certificate. You can view the certificate by using the following iLO RESTful API GET command:

```
/redfish/v1/Managers/1/SecurityService/PlatformCert/Certificates/1
```

More information

Advanced BIOS and platform security options
HPE Platform Certificate Verification Tool

HPE Platform Certificate Verification Tool

On a server provisioned with a Trusted Computing Group (TCG)-compliant platform certificate, you can use the HPE Platform Certificate Verification Tool (PCVT) to verify the configuration.

Running PCVT allows you to independently compare the server state to the information stored in the platform certificate.

- If the measurement of a component matches the reference value, this result indicates that the configuration has not changed since the server left the Hewlett Packard Enterprise factory.
- If a measurement does not match the reference value, this result indicates that the configuration changed since the server left the HPE factory. When a change is detected, investigation is needed to determine whether the change is expected and approved, or whether supply chain tampering occurred.

You can download the HPE PCVT and view the documentation at the following website: **https://github.com/HewlettPackard/PCVT**.

More information

Platform certificates

Zero trust security

In a zero trust environment, security is monitored throughout the server life cycle to protect the hardware, firmware, hypervisor, OS, and applications.

Subtopics

Silicon root of trust

Secure boot

SPDM authentication

Server identity

Trusted Platform Module

Unauthorized access prevention

Persistence-enabled attack protection

iLO firewall for system ROM and iLO firmware

Communication between iLO and server blades or compute modules

Silicon root of trust

Figure 1. iLO 5 Silicon root of trust

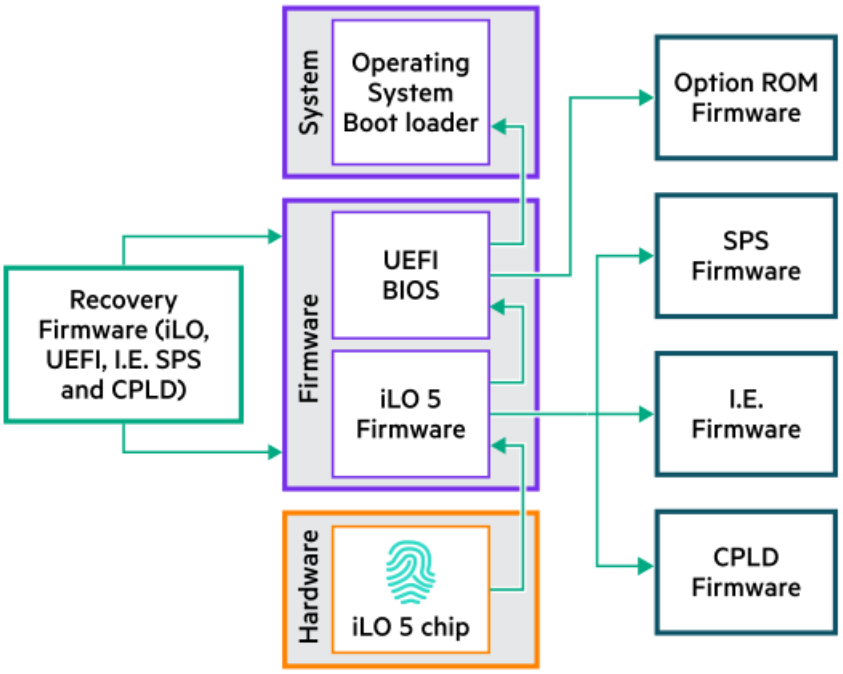
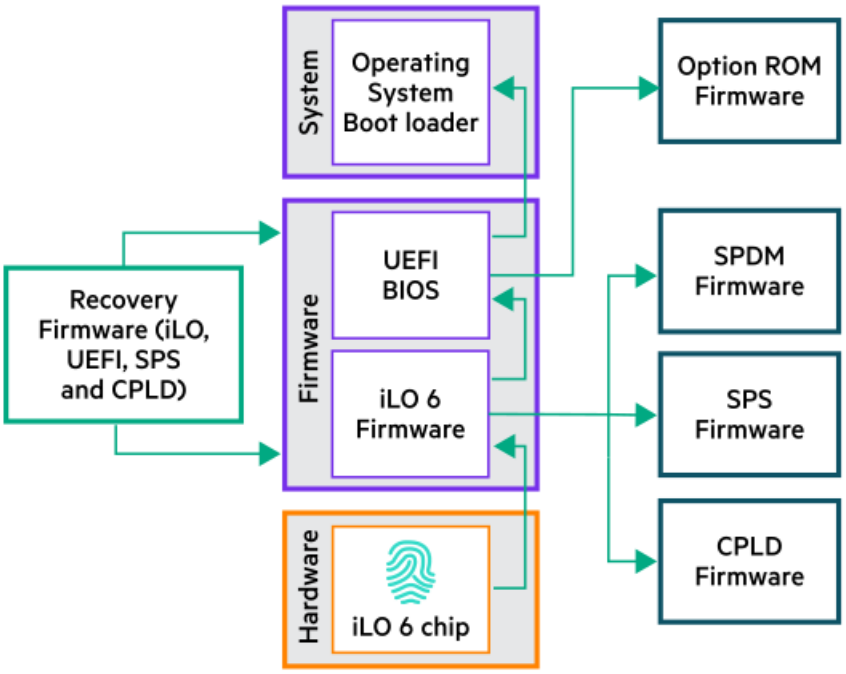


Figure 2. iLO 6 Silicon root of trust



The iLO chip acts as a silicon root of trust. The silicon root of trust makes it virtually impossible to insert any malware, virus, or compromised code that would corrupt the server boot process.

A digital fingerprint of the iLO firmware is embedded in the iLO chip at a trusted chip fabrication facility. At startup, the iLO chip verifies the iLO firmware integrity and determines if it is allowed to run. The decision is based on whether the iLO firmware matches the digital fingerprint. If the iLO firmware fails validation, the system automatically restores the iLO firmware from the System Recovery Set.

When the iLO firmware runs, it verifies the following components:

- UEFI BIOS (system ROM)
- CPLD (System Programmable Logic)
- Server Platform Services (SPS) firmware

  The SPS firmware runs on the management engine (ME).

- Innovation Engine (iLO 5 only)
- SPDM Firmware (Gen11 only)

If the active system ROM fails validation by iLO and an iLO Advanced license is installed, iLO will automatically recover it from the copy stored in the System Recovery Set. If an iLO Advanced license is not installed, the system firmware can still be recovered manually by using one of the available firmware update methods. For added redundancy on some systems, the system firmware is mirrored. This feature allows UEFI to check itself during server startup. If tampering is detected, it will fail over from the active side to the recovery side.

If the CPLD, SPS, or Innovation Engine (iLO 5 only), firmware fails validation, the system automatically restores them from the System Recovery Set if an iLO Advanced license is installed. If a license is not installed, the failure is logged and you must complete the repair manually.

Check the IML and the Security Log for information about the firmware validation activities and recovery actions.

After the firmware is verified and the server powers on, the secure boot feature verifies additional components during the boot process.

More information

Secure boot
Firmware verification
System Recovery Set

Secure boot

Secure boot 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:

- 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 run 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 **https://www.hpe.com/servers/ossupport**.

You can use a directly attached management console or the iLO remote console to customize the certificates embedded in the UEFI BIOS. For more information, see the UEFI System Utilities user guide for your platform (**https://www.hpe.com/info/UEFI-manuals**).

For information about using the iLO RESTful API to configure the secure boot settings, see the iLO RESTful API documentation (**https://servermanagementportal.ext.hpe.com/**).

SPDM authentication

HPE Gen 11 servers with iLO 6 use SPDM (Security Protocol and Data Model) to verify the integrity of components and authenticate supported option cards. Examples of supported hardware include PCIe option cards such as storage controllers and network adapters, and NVMe drives attached to the CPU.

This feature uses open DMTF standards to enable a zero trust configuration between the server management software and the supported server options.

NOTE:
HPE ProLiant RL3xx Gen 11 platforms do not support SPDM.

To enable this feature, configure the Global component integrity and Component integrity policy on the Access Settings page in iLO, or use the iLO RESTful API.

- **Global component integrity**—When enabled, iLO authenticates the server components and option cards by using SPDM authentication.
- **Component integrity policy**—When the **Global component integrity** option is enabled, use this option to control the system boot policy based on the SPDM authentication results.
  - Halt Boot On SPDM Failure —Stops system boot during SPDM authentication failure.
  - No Policy—Boot the system in normal mode, regardless of SPDM authentication failure.

If SPDM is enabled, an unsupported or nonauthentic component changes the iLO security status to Risk. When this happens, the device shows a failed status for the **Overall Component Integrity Result** on the **Device Inventory** page.

iLO supports SPDM v1.0 and v1.0.1. For devices that do not support an SPDM version, iLO logs Security Log events for SPDM failures.

You can check the status of individual component authentication in the Security Log.

The results of SPDM authentication are reported in the following iLO locations.

- IML
- Security Dashboard
- Security Log
- Device Inventory page
- SNMP traps and REST alerts

For information about option support, see the option QuickSpecs document at **https://www.hpe.com/info/qs**.

Subtopics

SPDM supported algorithms (Gen11 servers only)

More information

SPDM supported algorithms (Gen11 servers only)

SPDM supported algorithms (Gen11 servers only)

Based on the configured security state, iLO categorizes the SPDM algorithms as follows:

Production, FIPS, or High Security

BaseAsymAlgo(4)

- TPM_ALG_RSASSA_2048
- TPM_ALG_RSAPSS_2048
- TPM_ALG_RSASSA_3072
- TPM_ALG_RSAPSS_3072
- TPM_ALG_ECDSA_ECC_NIST_P256
- TPM_ALG_RSASSA_4096
- TPM_ALG_ECDSA_ECC_NIST_P384

BaseHashAlgo (4)

- TPM_ALG_SHA_256

- TPM_ALG_SHA_384
- TPM_ALG_SHA_512

CNSA

BaseAsymAlgo(4)

- TPM_ALG_RSASSA_3072
- TPM_ALG_RSAPSS_3072
- TPM_ALG_RSASSA_4096
- TPM_ALG_ECDSA_ECC_NIST_P384

BaseHashAlgo (4)

- TPM_ALG_SHA_384

Server identity

A server identity (DevID) provides a way to uniquely identify and authenticate a server across networks. It is based on the IEEE 802.1AR DevID standard and consists of an asymmetric cryptographic key pair and a digital certificate. A DevID is uniquely bound to a server. It enables a server to cryptographically prove its identity in various industry standards and protocols that authenticate, provision, and authorize communicating devices. Being a cryptographically strong credential protected by hardware, a DevID can serve as the foundation for server zero touch provisioning and zero trust operation.

HPE supports both factory-provisioned (IDevID) and field-provisioned (LDevID) server identities. For flexibility, these credentials are stored both in iLO (iLO IDevID and LDevID) and the TPM (System IDevID and System LDevID). Servers with TPMs are additionally provisioned with a related credential called a System IAK (Initial Attestation Key). To verify server identity support, see the product QuickSpecs document: **https://www.hpe.com/info/qs**.

For more information about the server identity features, see the iLO user guide and the Enablement for IEEE 802.1X-Based Server Onboarding **technical paper**.

iLO IDevID and iLO LDevID

iLO can be provisioned with a server identity (DevID) at the factory. The factory-provisioned server identity is called iLO IDevID on all servers except AMD-based Gen10 Plus servers, where it is called iLO LDevID. HPE servers can be securely onboarded into a customer network by using the iLO DevID for 802.1X authentication. iLO DevIDs have lifetime validity and are immutable.

iLO IDevID and iLO LDevID enable servers to make a zero-touch and zero-trust connection to cloud-based tools such as HPE GreenLake for Compute Ops Management. These features enable iLO to make a trusted outbound connection to begin provisioning without first completing the configuration steps in iLO. The outbound connection is enabled by TLS using the iLO IDevID/LDevID as the iLO TLS certificate.

System IDevID certificate

Systems with TPMs can be provisioned with a server identity that is available for use by the host OS and standards or protocols that are designed to interact with a TPM. This factory-provisioned identity is called System IDevID. The IDevID certificate can be accessed through iLO and the corresponding private key is stored in the TPM. System IDevID follows the Trusted Computing Group (TCG) TPM 2.0 Keys for Device Identity and Attestation specification.

You can view the certificate by using the following iLO RESTful API GET command:

```
/redfish/v1/Managers/1/SecurityService/SystemIDevID/Certificates/1
```

System IAK certificate

iLO can be provisioned with a System IAK certificate. This credential is similar to System IDevID, but it is used for TPM-based attestation. The IAK certificate can be accessed through iLO and the corresponding private key is stored in the TPM. System IAK complies with the TCG TPM 2.0 Keys for Device Identity and Attestation specification.

You can view the certificate by using the following iLO RESTful API GET command:

```
/redfish/v1/Managers/1/SecurityService/SystemIAK/Certificates/1
```

Subtopics

802.1X and iLO

802.1X and iLO

IEEE 802.1X is a mechanism for port-based network access control. It regulates access to the network and protects against unidentified and unauthorized network access.

802.1X uses the Extensible Authentication Protocol (EAP) for message exchange during the authentication process. EAP-Transport Layer Security (EAP-TLS) is an EAP type that uses certificates or smart cards for authentication.

HPE iLO supports EAP-TLS authentication for onboarding into an 802.1X access-controlled network. Using a factory-provisioned server identity (iLO IDevID), an HPE server can securely onboard and establish its identity with zero touch (unattended autonomous operation) for 802.1X authentication. iLO also supports a user-provisioned server identity (LDevID) for 802.1X authentication. When both iLO IDevID and LDevID are present in the system, LDevID is used for EAP-TLS authentication.

The default setting for 802.1X authentication is Enabled. iLO does not initiate EAP-TLS authentication or respond to authentication requests if the system does not have an iLO IDevID or LDevID.

More information

Server identity

Trusted Platform Module

Trusted Platform Modules (TPM) 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 OS to take measurements of all phases of the boot process.

TPM is an option on Gen10 and Gen10 Plus products and it is included in all Gen11 products. For TPM support information, see the server QuickSpecs at the following website: **https://www.hpe.com/info/qs**.

More information

Trusted platform module options

Unauthorized access prevention

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

Authentication

Determines who is at the other end of the network connection. Authentication can be performed locally or through directory services. Supported authentication methods include local accounts, Kerberos authentication, Directory integration, SSO, and smart cards.

Authorization

Determines whether the user attempting to perform an 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 remote consoles and mobile apps (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. When high encryption modes are not used, iLO might negotiate weaker keys or algorithms.

Persistence-enabled attack protection

A persistence-enabled attack occurs when unauthorized users gain and maintain long term system access without being detected. With this access, they might initiate activities such as a permanent denial of service attack or the installation of malware.

iLO offers the following protections:

Authorized firmware updates

All firmware types that can be flashed by iLO, including the iLO firmware, system BIOS, CPLD, and Innovation Engine (iLO 5 only) firmware, are digitally verified before installation. This verification prevents the insertion of compromised code by users without physical access.

The system BIOS, iLO firmware, and other essential firmware types are digitally verified at startup as part of the Silicon Root of Trust. This verification protects firmware from compromise even with physical access by the attacker.

Unencrypted ports

iLO clearly defines the port encryption status. You can disable access to any nonencrypted ports (such as IPMI). Access to iLO requires a password unless you 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 uses 2048-bit RSA keys. When the CNSA security state is used, iLO requires ECDSA 384-bit keys.

Unsuccessful Login delays

iLO captures all login activity. It uses a progressive timed delay during unsuccessful login attempts to impede brute force and dictionary attacks.

Restricted access and modification of critical security parameters

iLO logs security parameter changes such as user accounts, log changes, and certificates. This feature allows tracing of potential unauthorized information access attempts.

Daily firmware flash limit

To protect the iLO and server hardware from repeated flashing attacks, iLO limits the number of times per day that you can flash each supported firmware type. The limit is 20, which includes both successful and failed firmware flash activities. The firmware flash count is reset every 24 hours, or 24 hours after a successful firmware update. The firmware flash limit applies to firmware updates initiated through any application or interface.

The firmware flash count is stored in the nonvolatile memory. If the flash limit is exceeded, the firmware cannot be flashed, and the software notifies you that you must try again later.

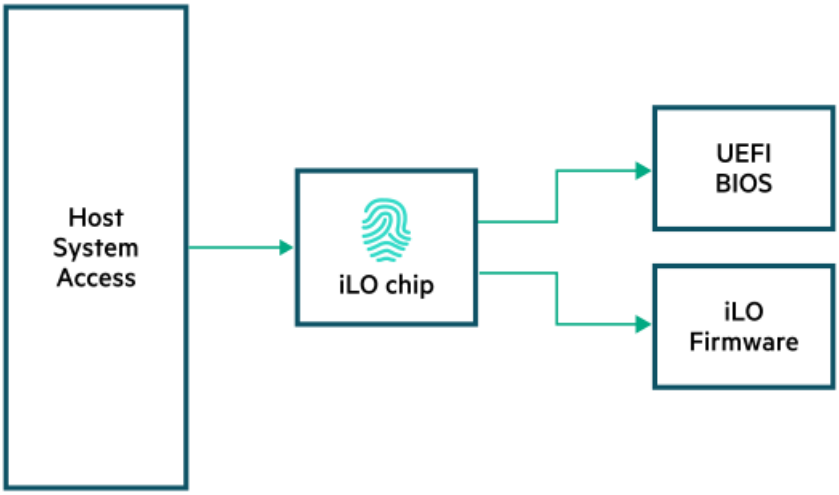
More information

Silicon root of trust

iLO firewall for system ROM and iLO firmware

HPE servers and compute modules are compliant with **NIST800-147B, BIOS Protection Guidelines for Servers**.

The system ROM and the iLO firmware reside on flash chips that are physically protected from host access by the iLO chip. Only the iLO firmware can write to these flash chips. This configuration prevents unauthorized access from the host system. The iLO firmware authenticates any images written to the BIOS flash chip.



Communication between iLO and server blades or compute modules

HPE ProLiant c-Class server blades

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

There is a strict communication hierarchy among ProLiant server blade components. The Onboard Administrator (OA) management module communicates with the iLO processor on each server blade. There is no connection from the iLO processor or OA module to the server NICs. The iLO processor only has information about the presence of other server blades in the infrastructure and whether enough amperage is available from the power subsystem to boot the server blades. Two ports on the rear of the BladeSystem enclosure provide access to the iLO network connections on the server blade.

HPE Synergy compute modules

The HPE Synergy 12000 Frame uses a single frame to hold multiple compute modules. A separate power subsystem provides power to all compute modules in the frame. iLO sends alerts and management information throughout the hardware infrastructure.

There is a strict communication hierarchy among the system components. The Frame Link Module communicates with the iLO processor on each HPE Synergy compute module. There is no connection from the iLO processor or Frame Link Module to the server NICs. The iLO processor only has information about the presence of other compute modules in the frame and whether enough amperage is available from the power subsystem to boot the compute modules. Two ports on the rear of the chassis provide access to the iLO network connections on the Synergy compute module.

Physical access security

Subtopics

System maintenance switch

USB security

Rack and power security

Bezel lock

More information

Chassis intrusion detection switch

System maintenance switch

Hewlett Packard Enterprise servers and compute modules have hardware system maintenance switches, which control different security functions and configurations.

The system maintenance switch is inside the chassis on the system board. To access the switch, you must take the device offline, power down, and remove the access cover.

The following system maintenance switches are off by default. You can set these switches to on when you want to change the product security behavior. The system maintenance switch settings are listed on the access panel label and in the product user guide.

iLO security (position 1)

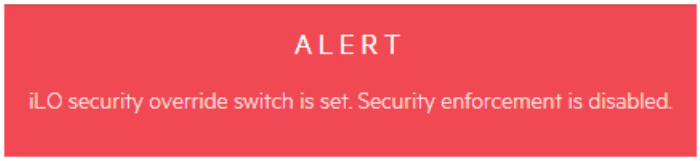
The iLO security setting on the system maintenance switch provides emergency access to an administrator who has physical control of the system board.

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

When this switch is off (default), iLO enforces the configured authentication settings.

Disabling this switch has the following effects:

- When iLO is configured to use the Production security state, all login credential verifications are disabled.
- When iLO is configured to use the High Security, FIPS, or CNSA security state, all login credential verifications are enforced.
- If the host server is reset, the UEFI System Utilities software runs.
- iLO networking, the iLO web interface, and the ROM-based system utility are accessible even if they were previously disabled.
- The System Recovery privilege is enforced. To perform an action that requires this privilege, you must authenticate with a user account that has the privilege enabled.
- 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 alert is sent when iLO starts after the iLO security configuration change.

BIOS password disabled (position 5)

When the switch is off (default), you can configure and use the Set Admin Password and Set Power On Password features in the UEFI System Utilities.

When the switch is on, configured BIOS administrator and power-on passwords are removed.

Reset configuration (position 6)

When the switch is off (default), the BIOS configuration is maintained.

When the switch is on, all BIOS factory defaults are restored.

You can view the system maintenance switch status on the System Information page in Intelligent Provisioning.

For more information, see the maintenance and service guide for your product.

Subtopics

Reasons to disable iLO security

More information

Power-on password
Administrator password

Reasons to disable iLO security

You might want to use the system maintenance switch to disable iLO security in the following situations:

- 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.
- iLO is unreachable over the network because the iLO NICs are turned off or the iLO network configuration is incorrect. It is not possible or convenient to use the UEFI System Utilities to correct the configuration.

  Disabling iLO security resets the iLO network configuration to the factory default settings.
  - On most servers, this action enables DHCP and the iLO Dedicated Network Port.
  - On servers where the iLO Dedicated Network Port is an optional add-on card, this action enables DHCP and the Shared Network Port.
  - On servers with the iLO network enablement module, this action enables DHCP and the iLO Dedicated Network Port.
- Only one user name is configured, and the password is forgotten.
- You want to erase the configuration information stored on the battery-powered SRAM memory device.

  When iLO starts, it backs up the configuration information stored in the battery-powered SRAM memory device to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored. When iLO security is disabled, the SRAM data is not restored automatically.

More information

System maintenance switch

USB security

UEFI System Utilities

You can configure the server USB port settings through the USB Options section of the UEFI System Utilities.

You can configure:

- USB port and embedded device startup behavior.
- The ability to boot from USB devices such as virtual media devices and embedded SD cards.
- Which USB or SD device to search first when enumerating boot devices.
- Availability of the internal SD card.

For more information, see the UEFI System Utilities user guide for your platform (https://www.hpe.com/info/UEFI-manuals).

iLO Service Port

The iLO Service Port is a USB port with the label iLO on supported servers.

You can use the iLO Service Port to download the Active Health System Log or to connect a client with a supported Ethernet adapter to access iLO.

The iLO Service Port has the following security characteristics:

- 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.

You can disable the feature, or choose whether to allow USB flash drive access, require credentials, or use an Ethernet adapter.

For more information, see:

- iLO security setting recommendations
- The iLO documentation (**iLO 5** or **iLO 6**).

Rack and power security

Hewlett Packard Enterprise offers solutions to enhance rack and power security, including racks with physical and electronic lock options and locking power cords to provide secure cable retention and power-related downtime.

For more information about these solutions, see **https://www.hpe.com/info/rackandpower**

Bezel lock

For protection against external access on supported products, you can install a bezel lock. For ordering information, see the product QuickSpecs at **https://www.hpe.com/info/qs**. For installation instructions, see the product user guide.

Cloud-based management

Subtopics

HPE GreenLake for Compute Ops Management security features

HPE GreenLake for Compute Ops Management security features

HPE GreenLake for Compute Ops Management simplifies and unifies operations across the server life cycle, for the whole environment, no matter where your compute infrastructure lives. It provides a consistent, secure cloud experience that scales elastically and unifies compute management.

Security is pervasive throughout the application.

Authentication

Users can use the following authentication methods:

- User name and password
- Multifactor authentication (MFA)
- Single Sign-On (SSO)

Device authentication

- Devices authenticate with a mutual TLS (mTLS) connection to ensure that they are connecting to a known entity.
- Devices are assigned to a single customer.

User roles

The tasks you can perform with Compute Ops Management depend on your assigned role (Observer, Operator, Administrator, or custom role).

Resource restriction policies

HPE GreenLake supports custom resource restriction policies (RRPs) that allow you to configure resource access control. You can use this feature with Compute Ops Management when you want to limit the servers that your administrators and operators can manage.

For example, you might have multiple administrators working in the same workspace or service instance. To prevent accidental or unauthorized changes, create RRPs and apply them to the administrator user account roles. Users with an RRP can perform management actions only on the servers specified by the Compute Ops Management filter associated with the RRP. All other servers in the affected service instance are read-only. If a user with restricted access initiates a management action on a read-only server, an authorization error occurs.

Resource restriction policies apply to servers that are managed directly by Compute Ops Management. They do not affect servers managed by HPE OneView.

Audit log

HPE GreenLake records information about all server actions initiated through the Compute Ops Management application. HPE GreenLake saves this information in the audit log.

iLO security risk monitoring

Compute Ops Management monitors the iLO security dashboard to alert you to potential security risks. The security risk status is calculated by comparing the server configuration to a predefined set of security recommendations.

A security risk means that the server configuration is different from the recommended configuration. If you want to configure a setting with a different value from the recommendation, you can configure that setting to be excluded from the risk status.

More information

- Cloud Security Alliance STAR Registry Listing for Compute Ops Management
- HPE GreenLake for Compute Ops Management Security Guide

iLO server management features

For information about performing tasks in the iLO web interface, see the online help or view the iLO user guide (iLO 5 or iLO 6).

You can use the iLO RESTful API to perform many of the tasks that are available through the iLO web interface. For more information, see https://servermanagementportal.ext.hpe.com/.

NOTE:
RIBCL and the scripting tools HPQLOCFG, LOCFG.PL, and HPONCFG have entered the sustenance stage. HPE will now provide only critical bugs and security fixes for RIBCL. Hewlett Packard Enterprise recommends using the iLOREST Tool or iLO RESTful API.

Subtopics

iLO security guidelines

Ports used by iLO features

Access control for features, ports, and protocols

iLO network connection options

Virtual LAN

Network and management ports

SSH keys

Supported authentication methods

SSL certificates

Guidelines for using iLO with IPMI or DCMI over LAN

Security dashboard

Security audits

Security Log

Remote console security

iLO encryption settings

Kerberos authentication with iLO

Schema-free directory authentication

HPE Extended Schema directory authentication

Secure firmware flash updates

Firmware verification

iLO backup and restore

More information

Recommended security settings

iLO security guidelines

When you set up and use iLO, consider the following guidelines for maximizing security. For information about configuring these options, see the iLO user guide (**iLO 5** or **iLO 6**).

Dedicated management network

Set up iLO on a dedicated management network.

Hewlett Packard Enterprise recommends establishing a private management network that is separate from your data network. Configure the management network so that it can be accessed only by administrators.

If you connect iLO devices to a shared network, consider the iLO devices as separate servers and include them in security and network audits.

Internet connection

To avoid security risks, do not connect iLO or other systems directly to the Internet.

The iLO processor is a management and administration tool, not an Internet gateway. Connect to the Internet by using a corporate VPN that provides firewall protection.

IMPORTANT:
Change the iLO user account passwords immediately if iLO has been connected directly to the Internet.

SSL certificate

Replace the default self-signed certificate by installing an SSL certificate that is signed by a Certificate Authority (CA).

Trusted CA certificates

Install trusted CA certificates to enable certificate validation for external services such as LDAP.

Passwords

Follow the Password guidelines.

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. Hewlett Packard Enterprise recommends using a Minimum Password Length of eight or more

characters. The default value is eight characters.

> **IMPORTANT:**
> Do not set 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.

User account privileges

Instead of creating user accounts with all privileges, create multiple accounts with fewer privileges.

Firmware updates

Keep your iLO and server firmware up to date.

Authentication

Use an authentication service (for example, Active Directory or OpenLDAP), preferably with two-factor authentication.

This feature allows authentication and authorization using the same login process throughout the network. It provides a way to control multiple iLO devices simultaneously. Directories provide role-based access to iLO with specific roles and privileges based on time and location.

Implement two-factor authentication to provide additional security, especially when you make connections remotely or outside the local network.

Protect SNMP traffic

Reset the community strings according to the same guidelines as the administrative passwords. Also set firewalls or routers to accept only specific source and destination addresses. Disable SNMP at the server if you do not need it.

Port and protocol settings

Disable ports and protocols that you do not use (for example, SNMP or IPMI/DCMI over LAN).

Use HTTPS for the .NET remote console

To configure this option, install a trusted SSL certificate that is signed by a Certificate Authority (CA) and enable the IRC requires a trusted certificate in iLO setting.

Unused features

Disable features that you do not use (for example, remote console).

Lock the server OS console

Configure the remote console to automatically lock the server OS console.

Security state

Configure a higher security state such as High Security, FIPS, or CNSA.

For information about configuring iLO to operating in FIPS-validated mode, see section 3.1.1 in the **FIPS 140-2 Non-Proprietary Security Policy** document.

Configuration utilities

Disable the iLO Configuration Utility in the UEFI System Utilities or configure iLO to require login credentials when users access it.

Log authentication failures

Configure iLO to log authentication failures.

Firmware verification

Enable firmware verification scans.

Security Dashboard and Security Log

Use the Security Dashboard and Security Log to monitor security risks and recommendations.

Host authentication

Enable the Require Host Authentication feature.

Firmware downgrade policy

Set the Downgrade Policy to Downgrade requires Recovery Set privilege.

Recovery Set

Keep the Recovery Set up to date.

HTTP connections

Configure iLO to avoid access over an HTTP connection.

To configure this behavior, install a trusted SSL certificate that is signed by a Certificate Authority (CA) and enable the IRC requires a trusted certificate in iLO setting.

In this configuration, when you access the iLO web interface, iLO returns an HTTP Strict Transport Security (HSTS) flag in the response header, which enables the browser to automatically redirect any HTTP request to HTTPS.

Ports used by iLO features

Network settings and ports

The values listed in Network settings and ports configurable through iLO can be configured to comply with site requirements or security initiatives.

Table 1. Network settings and ports configurable through iLO

Description	Default Setting or Port	Protocol type
IPMI/DCMI over LAN port	623	UDP
IPMI/DCMI over LAN Specifies whether to allow IPMI/DCMI communications over the LAN with iLO.	Disabled	
IPMI over KCS [1]	Enabled	
Remote Console Port	17990	TCP
Remote Console Allows you to enable or disable access through the iLO remote consoles.	Enabled	
Secure Shell (SSH) Port	22	TCP
Secure Shell (SSH) Allows you to enable or disable the SSH feature. SSH provides encrypted access to the iLO command-line protocol (CLP).	Enabled	
SNMP Port	161	UDP
SNMP Trap Port	162 for SNMP alerts (outgoing only).	UDP
SNMP Specifies whether iLO responds to external SNMP requests.	Enabled	
Virtual Media Port	17988	TCP
Virtual Media Enables you to specify whether virtual media is enabled or disabled.	Enabled	
Web Server Non-SSL Port (HTTP)	80	TCP
Web Server SSL Port (HTTPS)	443	TCP
Web Server [2] Allows you to enable or disable access through the iLO web server.	Enabled	

1 Applies to iLO 6
2 Supports the iLO web interface, remote console, iLO RESTful API, iLO Federation, firmware updates, and RIBCL.

Other outgoing ports

Security administrators might need to know the ports listed in Other ports used by iLO. These ports are for outgoing third-party services.

Table 2. Other ports used by iLO

Description	Default port	Protocol type	Location in iLO web interface
DNS Resolution	53	UDP	N/A
iLO Federation/SSDP Multicast [1] SSDP Multicast [2]	1900	UDP	N/A
DHCPv4	67, 68	UDP	N/A
DHCPv6	547	UDP	N/A
NTP	123	UDP	N/A
NetBIOS Name Service/WINS	137	UDP	iLO Dedicated Network Port > IPv4 iLO Shared Network Port > IPv4
Kerberos KDC Server Port	88	TCP, UDP	Security > Directory
Directory Server LDAP SSL Port	636	TCP	Security > Directory
AlertMail SMTP Port	25	TCP	Management > Mail
Remote Syslog Port	514	UDP	Management > Remote Syslog
Key Manager Port	9000	TCP	Administration > Key Manager
Remote Support Port	7906	TCP	Remote Support > Registration

1 Applies to iLO 5
2 Applies to iLO 6

Ports not supported by iLO

iLO does not support the commonly used ports listed in Unsupported ports.

Table 3. Unsupported ports

Description	Port	Protocol type	Notes
LDAP-unsecured • Connection (TCP) • Connectionless (UDP)	389	TCP/UDP	iLO uses secure port 636 for outgoing LDAP connections.
Global Catalog LDAP-unsecured • Connection (TCP) • Connectionless (UDP)	3268	TCP/UDP	iLO uses secure LDAP connections.

Access control for features, ports, and protocols

The iLO Access Settings features allow you to disable unused features, ports, and protocols. For more information, see the Access Settings documentation in the iLO user guide (**iLO 5** or **iLO 6**).

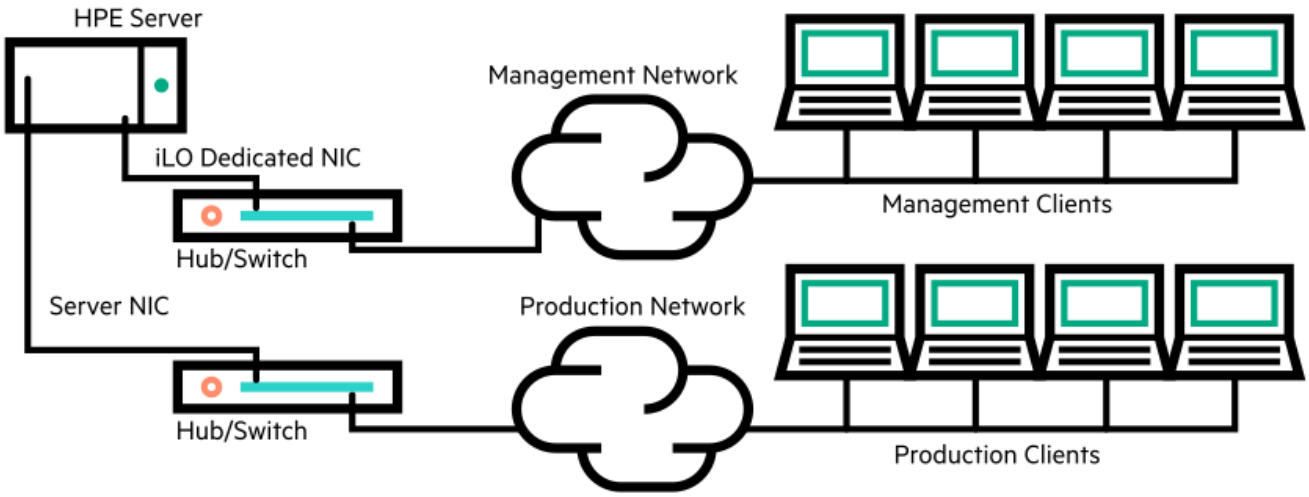
iLO network connection options

You can connect iLO to the network through a dedicated management network or a shared connection on the production network.

Dedicated management network

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

Figure 1. Dedicated management network



Production network

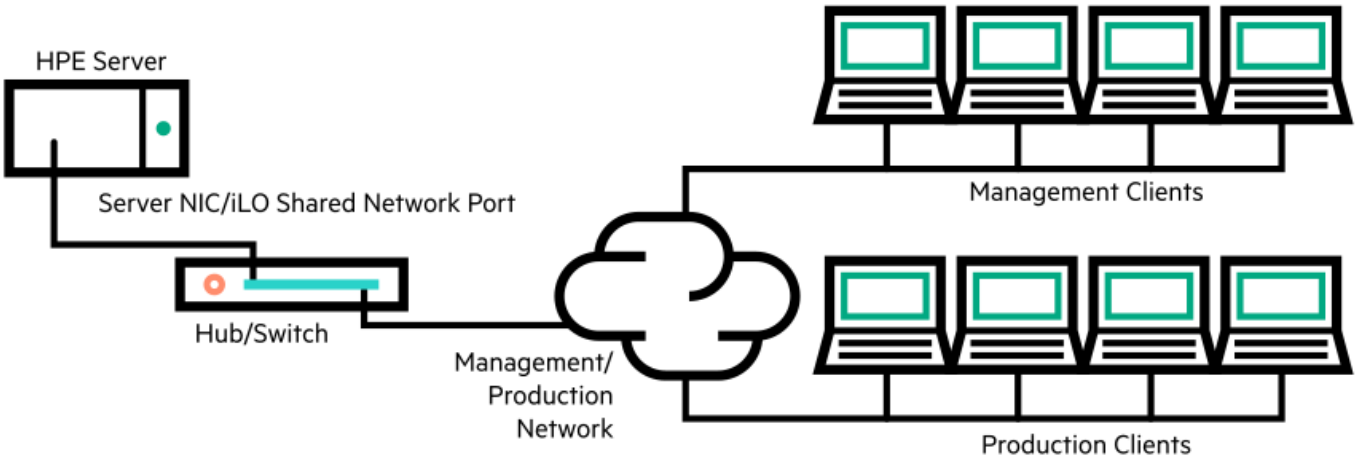
In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO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

There are some drawbacks to using this configuration.

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

  When this situation occurs, the Remote Console and connected iLO Virtual Media devices might be disconnected.
- Network controller firmware updates or resets can also cause iLO to be unreachable over the network for a brief period.
- The iLO Shared Network Port connection can operate up to a maximum speed of 100 Mbps. Network-intensive tasks such as data transfer through iLO virtual media might be slower than the same tasks performed in a configuration that uses the iLO Dedicated Network Port.

Figure 2. Shared network connection



iLO network enablement module

Some servers require an optional iLO network enablement module to add support for remote management through a dedicated management network (default) or a shared network connection. If an iLO network enablement module is not installed, iLO access is supported only through host-based (in-band) access methods. Some examples of the supported host-based access methods include the iLO RESTful API, UEFI System Utilities, iLO Service Port (if available), and the Virtual NIC.

To review the network connections that your server supports, see the server user guide.

More information

Virtual LAN
Network and management ports

Virtual LAN

iLO shared network port

Implementing VLAN tags enhances iLO shared network port security. When you enable VLAN tags, the iLO shared network port becomes part of a VLAN. 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 VLAN tag appear to be on a separate LAN even if they are physically connected to the same LAN. The shared network port NIC checks the Ethernet frame for a VLAN ID and compares it against its configured value. If they match, then the shared network port strips the frame of the VLAN tag and forwards it to iLO. If they do not match, the shared network port forwards the frame to the server. The shared network port NIC inserts a VLAN tag into any outgoing Ethernet frames.

iLO dedicated network port

You can use VLAN tagging to distinguish between properly configured and unconfigured devices. Using VLAN tagging allows you to keep unconfigured devices off the network, even if they are physically connected.

More information

iLO network connection options

Network and management ports

The iLO firewall and bridge logic prevents any connection between the iLO management port and the server Ethernet port. Even by using the shared network port, iLO cannot bridge traffic between its 10/100/1000 Ethernet port and the server Ethernet port. Therefore, attacks on the server network cannot compromise iLO.

SSH keys

When you add an SSH key to iLO, the iLO firmware associates the key with a local user account.

Supported SSH key formats

- RFC 4716
- OpenSSH key format
- iLO legacy format

For examples of these formats, see the iLO user guide.

Working with SSH keys

- The supported SSH key formats are supported with the iLO web interface and the CLI.
- Only the iLO legacy format is supported with RIBCL scripts.
- Any SSH connection authenticated through the corresponding private key is authenticated as the owner of the key and has the same privileges.
- The iLO firmware can import SSH keys with a maximum length of 1,366 bytes. If the key length exceeds 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.
- If a user is removed after an SSH key is authorized for that user, the SSH key is removed.

Supported authentication methods

CAC smart card authentication

A common access card (CAC) is a United States Department of Defense (DoD) smart card 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 smart card certificate that must be associated with your local user account in the iLO web interface. Upload and associate your smart card 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.

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 smart card must be configured to require a PIN.

Personal Identity Verification

Personal Identity Verification (PIV) credentials are supported.

Smart cards

Smart cards are supported.

SSL certificates

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

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

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

IMPORTANT:

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

Certificates are included when you use the iLO backup and restore feature.

More information

X.509 Certificate Subject CN Does Not Match the Entity Name
Untrusted TLS/SSL server X.509 certificate
Weak cryptographic key
iLO backup and restore

Guidelines for using iLO with IPMI or DCMI over LAN

iLO supports IPMI 2.0 and DCMI industry standard protocols. IPMI is an industry standard protocol developed by Intel. It is supported by over 200 vendors, including Hewlett Packard Enterprise.

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

iLO enables you to send industry-standard IPMI and DCMI commands over the LAN. The IPMI/DCMI port is set to 623 by default, but it is configurable. When enabled, the IPMI over LAN option allows you to send IPMI/DCMI commands over the LAN by using a client-side application. When this option is disabled, server-side IPMI/DCMI applications are still functional.

Observe the following guidelines when using IPMI or DCMI over LAN:

- Segment IPMI/DCMI traffic from the rest of the network. If you are using a shared NIC connection, a VLAN for iLO can be used to accomplish this separation. Isolate the IPMI/Management subnet by using a firewall, and limit access to authorized administrators.
- Do not allow IPMI/DCMI traffic from outside the network.
- iLO supports IPMI 2.0 which uses stronger encryption than IPMI 1.5.

Resolved vulnerabilities

In July 2013, the US-CERT issued an alert (TA13–207A) Risks of Using the Intelligent Platform Management Interface (IPMI). The alert is available at the following website: **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 issue 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 IDs are configured with user names and passwords. Often, this is preconfigured in manufacturing to well-known user IDs and passwords. iLO does not retain disabled user ID user names and passwords. iLO has one user name

preconfigured with a unique password during manufacturing. Hewlett Packard Enterprise recommends that customers 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. Since this requirement is part of the IPMI protocol, Hewlett Packard Enterprise recommends disabling IPMI over LAN (if not in use) or isolating the IPMI management subnet.

Security dashboard

The iLO Security Dashboard displays the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. Use the dashboard to evaluate your configuration for potential risks. When a risk is detected, you can view details and advice for how to improve system security.

Subtopics

Causes of security risk status

More information

Server Configuration Lock
iLO security states

Causes of security risk status

The following security features are monitored on the Security Dashboard page. If a server does not support a feature, it is not listed.

Access Panel Status

The chassis intrusion detection switch reported that the access panel status is Intrusion.

This feature is available only on servers that are configured for chassis intrusion detection.

Hewlett Packard Enterprise recommends auditing the events recorded in the IML and iLO Event log, and checking surveillance video for any physical intrusion activity on the server.

Authentication Failure Logging

iLO is not configured to log authentication failures.

Hewlett Packard Enterprise recommends enabling this feature on the Access Settings page.

Default SSL Certificate In Use

The iLO default self-signed certificate is in use.

Hewlett Packard Enterprise recommends configuring a trusted certificate on the SSL Certificate Customization page.

IPMI/DCMI Over LAN

The IPMI/DCMI over LAN feature is enabled, which exposes the server to known IPMI security vulnerabilities.

Hewlett Packard Enterprise recommends disabling this feature on the Access Settings page.

Last Firmware Scan Result

The last firmware verification test failed. A firmware component is corrupted or its integrity is compromised.

Hewlett Packard Enterprise recommends updating the affected firmware component to a verified image.

For more information, see the iLO user guide.

To use this feature, you must install a license. For information about the available license types and the features they support, see the licensing guide (https://www.hpe.com/support/iLOLicenseGuide-en).

Minimum Password Length

The minimum password length is less than the recommended length, which makes the server vulnerable to dictionary attacks.

Hewlett Packard Enterprise recommends setting this value to 8 (default) or greater on the Access Settings page.

Password Complexity

iLO is not configured to enforce the password complexity guidelines, which makes the server vulnerable to dictionary attacks.

You can enable this feature on the Access Settings page.

Require Host Authentication

The Require Host Authentication feature is disabled and iLO is configured to use the High Security security state. When this feature is disabled, iLO credentials are not required when you use host-based configuration utilities to access the management processor.

Hewlett Packard Enterprise recommends enabling this feature on the Access Settings page.

Require Login for iLO RBSU

iLO is not configured to require login credentials to access the iLO configuration options in the UEFI System Utilities. This configuration allows unauthenticated access to the iLO configuration during system boot.

Hewlett Packard Enterprise recommends enabling this feature on the Access Settings page.

Secure Boot

The UEFI Secure Boot option is disabled. In this configuration, the UEFI system firmware skips validation for the boot loader, Option ROM firmware, and other system software executables for trusted signatures. It breaks the chain of trust established by iLO from power-on.

Hewlett Packard Enterprise recommends enabling this feature.

For more information, see the UEFI System Utilities documentation.

Security Override Switch

The server Security Override Switch (also called the System Maintenance Switch) is enabled. This configuration is a risk because login authentication is not required when the Security Override Switch is enabled.

Hewlett Packard Enterprise recommends disabling this feature.

For more information, see the iLO user guide (**iLO 5** or **iLO 6**).

SNMPv1 Request

SNMPv1 Request is enabled. This configuration allows iLO to receive SNMPv1 requests. Enabling SNMPv1 Request increases the system vulnerability to attack.

Hewlett Packard Enterprise recommends disabling this feature on the SNMP Settings page.

Global Component Integrity (iLO 6)

SPDM authentication is enabled. This configuration allows iLO to authenticate all applicable components in the server using SPDM. Disabling Global Component Integrity on the **Access Settings** page will change the iLO security status to risk.

If Global Component Integrity is disabled, iLO does not validate the components for SPDM authentication and SPDM supported cards are reported as `Not Supported`.

More information

Security dashboard

Security audits

Many companies have policies that mandate periodic security audits. iLO has event logs containing date- and time-stamped information about events that occurred in the iLO configuration and operation. You can access the logs in the iLO web interface. You can use the iLO RESTful API to set up an automated examination and extraction process that parses the logs by date, time, and authenticated user for accessing information about security events.

Security Log

The security log provides a record of the security events recorded by the iLO firmware.

Examples of the logged events include changes to the security configuration and security compliance issues. Other logged events include hardware intrusion, maintenance, and denial of service.

The security log provides a focused view of all recorded security events. Some of the same events are also included in the iLO event log or IML.

When the security log is full, each new event overwrites the oldest event in the log.

Remote console security

Remote console computer lock

Use this feature to automatically lock the OS or log out when a remote console session ends or the network link to iLO is lost. If you open a remote console window when this feature is enabled, the OS is locked when you close the window.

Integrated Remote Console trust settings

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 the 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, which is insecure. In this configuration, SSL is used after the .NET IRC starts to exchange encryption keys. If you cannot install a trusted SSL certificate, and you do not want to use a non-SSL connection, you can use the Standalone remote console (HPLOCONS) or the HTML 5 Integrated Remote Console.

iLO encryption settings

HPE iLO Standard, that comes with every Gen10 or later server, gives customers the ability to configure servers in one of three security states. With an iLO Advanced 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 web pages, SSH, and network communications. 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 following security states are available:

- Production
- High Security
- FIPS
- CNSA

Subtopics

iLO security states

iLO connections when higher security states are configured

iLO 5 SSH cipher, key exchange, and MAC support

iLO 6 SSH cipher, key exchange, and MAC support

SSL cipher and MAC support

FIPS validation and Common Criteria certification

iLO security states

Production (default)

When iLO is 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.
- Remote console data uses AES-128 bidirectional encryption.

High Security

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 following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

  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 the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- 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

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

HPE ProLiant RL3xx Gen 11 platforms do not support 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 that are 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.

- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

  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 the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

CNSA

The CNSA security state (also called SuiteB mode) is available only when the FIPS security state is enabled.

HPE ProLiant RL3xx Gen 11 platforms do not support CNSA.

When iLO is set to this security state:

- iLO operates in a mode intended to comply with the CNSA requirements defined by the NSA.
- iLO operates in a mode intended to secure systems that hold United States government top secret classified data.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- 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.
- Any software or utility that you use to connect to iLO must be CNSA-compliant.

  For example:
  - Firmware update utilities
  - SSH clients
  - HPE and third-party scripting and command-line tools
  - HPE and third-party management tools
  - AlertMail, syslog, LDAP, or key manager servers
  - Remote support software
- Use the HTML5 remote console, which enforces the use of AES-256 bit CNSA-compliant ciphers.

To verify compliance, check with your software vendor.

Look for updates about CNSA 2.0 in future editions of this document and in the iLO release notes.

Synergy Security Mode

A special security state used by Composer 2. You cannot change the security state on a device that uses this mode.

More information

System maintenance switch
iLO connections when higher security states are configured
iLO 5 SSH cipher, key exchange, and MAC support
iLO 6 SSH cipher, key exchange, and MAC support

iLO connections when higher security states are configured

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

When iLO is configured to use the CNSA security state, an AES 256 GCM cipher is required. AES is the only symmetric algorithm that is CNSA-compliant.

Web browser

Use the default browser settings or ensure that the browser is configured to support TLS 1.2, TLS 1.3 (or both) 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.

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 High Security, FIPS, or CNSA security states are enabled. If you are not assigned the required user privileges, an error message is displayed.

  The Require Host Authentication access setting has the following effects on host-based configuration utilities:

  - Enabled—Valid credentials are required for using the host-based configuration utilities with all iLO security states.
  - Disabled—Valid credentials are not required when iLO is configured to use the Production or High Security security state.

  The Require Host Authentication setting cannot be disabled when the FIPS or CNSA security state is used.

iLO RESTful API

Use a utility that supports TLS 1.2, TLS 1.3 (or both) and an AES cipher.

More information

iLO security states

iLO 5 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, AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
- diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1, and ecdh-sha2-nistp384 key exchange
- hmac-sha1, hmac-sha2-256, and AEAD_AES_256_GCM MACs

FIPS or High Security

- AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
- diffie-hellman-group-exchange-sha256 and ecdh-sha2-nistp384 key exchange
- hmac-sha2-256 or AEAD_AES_256_GCM MACs

CNSA

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

Synergy Security Mode

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

iLO 6 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, AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
- diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1 key exchange, and ecdh-sha2-nistp384 key exchange
- hmac-sha1, hmac-sha2-256, and AEAD_AES_256_GCM MACs

FIPS or High Security

- AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
- diffie-hellman-group-exchange-sha256 and ecdh-sha2-nistp384 key exchange
- hmac-sha2-256 or AEAD_AES_256_GCM MACs

CNSA

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

Synergy Security Mode

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

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.

The following lists of supported ciphers apply to all iLO SSL connections, including connections to LDAP servers, key manager servers, SSO servers, Insight Remote Support servers, https:// URLs used in virtual media, the iLO RESTful API, CLI commands, and iLO Federation group firmware updates.

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

Production

- 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES256-SHA)
- 256-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
- 256-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES256-SHA)
- 256-bit AES-GCM with RSA, and an AEAD MAC (AES256-GCM-SHA384)
- 256-bit AES with RSA, and a SHA256 MAC (AES256-SHA256)
- 256-bit AES with RSA, and a SHA1 MAC (AES256-SHA)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES128-SHA)
- 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)
- 128-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES128-SHA)
- 128-bit AES-GCM with RSA, and an AEAD MAC (AES128-GCM-SHA256)
- 128-bit AES with RSA, and a SHA256 MAC (AES128-SHA256)
- 128-bit AES with RSA, and a SHA1 MAC (AES128-SHA)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)
- TLS1.3 128 bits AES_GCM with AEAD MAC (TLS_AES_128_GCM_SHA256)

High Security

TLS 1.2 or TLS 1.3 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-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)
- TLS1.3 128 bits AES_GCM with AEAD MAC (TLS_AES_128_GCM_SHA256)

FIPS

TLS 1.2 or TLS 1.3 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)
- 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)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)
- TLS1.3 128 bits AES_GCM with AEAD MAC (TLS_AES_128_GCM_SHA256)

CNSA

TLS 1.2 or TLS 1.3 is required for this security state.

- 256-bit AES-GCM with ECDSA, ECDH, and an AEAD MAC (ECDHE-ECDSA-AES256-GCM-SHA384)
- Client only: 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)

Synergy Security Mode

- 256-bit AES-GCM with ECDSA, ECDH, and an AEAD MAC (ECDHE-ECDSA-AES256-GCM-SHA384)
- Client only: 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)

FIPS validation and Common Criteria certification

HPE iLO 5 v1.11 has attained the following:

- The cryptographic module for HPE iLO 5 v1.11 is FIPS 140.2 Level 1 validated. See the NIST Cryptographic Module Validation certificate at **https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3122**.
- HPE iLO 5 v1.11 has passed Common Criteria certification and was awarded a Common Criteria certificate for conformance to EAL 2+ (ALC_FLR.2). See the certification report at **https://www.commoncriteriaportal.org/files/epfiles/383-4-427%20CR%20v1.0e.pdf**.

Kerberos authentication with iLO

NOTE: HPE ProLiant RL3xx Gen 11 servers do not support Kerberos.

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 OS documentation.

Schema-free directory authentication

When you use schema-free directory authentication, 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 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 multiple iLO systems at the same time.

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=EXAMPLE,DC=COM` for Active Directory, or `UID=username,ou=People,dc=example,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=EXAMPLE,DC=COM`, is configured, iLO uses the following DN: `CN=JOHN.SMITH,CN=USERS,DC=EXAMPLE,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.

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.

Subtopics

Directory services support

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.

Secure firmware flash updates

Firmware images are hashed with SHA384 and signed using the Hewlett Packard Enterprise RSA 4096-bit private key. This signature block is prepended to the firmware binary image.

When performing a firmware update, the hash is decrypted by the currently executing iLO firmware with the Hewlett Packard Enterprise 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.

Firmware verification

The Firmware Verification feature allows you to view firmware scan results, set firmware scan policies, and run on-demand or scheduled system firmware scans.

System firmware scans detect invalid images and quarantine them when possible. Depending on the scan results, information is logged in the Active Health System Log and the Integrated Management Log.

To respond to detected issues, you can configure iLO to log the results, or log the results and attempt an automatic repair from the System Recovery Set.

Scans support several firmware types, depending on the system configuration. Some examples follow:

- iLO firmware
- System ROM (BIOS)
- System Programmable Logic Device (CPLD)
- Server Platform Services (SPS) firmware
- Innovation Engine (IE) firmware
- Server Platform Services Full Recovery Image
- Server Platform Services-IE Full Recovery Image
- Ampere System Control Processor

For more information, see the iLO user guide (iLO 5 or iLO 6).

Subtopics

System Recovery Set

By default, a System Recovery Set is included with every server. The components included in the recovery set depend on the server configuration.

User accounts with the **Recovery Set** privilege can configure this install set and only one System Recovery Set can exist at a time.

> **NOTE:**
> The Recovery Set privilege can be granted to iLO user accounts only from an active session that already possesses the Recovery Set privilege (such as the default iLO Administrator account). Only users with this privilege can update the System Recovery Set. If no user accounts possess the privilege, the Recovery Set cannot be altered without resetting iLO to the factory default settings.

If the default System Recovery Set is deleted, it can be recreated. Depending on the tools that the server supports, you can use the iLO RESTful API and the RESTful Interface Tool or SUM.

For more information, see the **SUM documentation** or the iLO user guide (**iLO 5** or **iLO 6**).

Table 1. Default System Recovery Set contents

Firmware	Servers with Intel processors	Servers with AMD processors	Servers with Ampere processors
System ROM (BIOS)	X	X	X
iLO firmware	X	X	X
System Programmable Logic Device (CPLD)	X	X	X
Server Platform Services (SPS) Firmware	X		
Server Platform Services Full Recovery Image	X [1]		
Innovation Engine (IE)	X [2]		
Server Platform Services-IE Full Recovery Image	X [2]		
Secondary System Programmable Logic Device			X

[1] Gen 11 only
[2] Gen10/Gen10 Plus only

More information

Firmware verification

iLO backup and restore

Automatic backup and restore

When iLO goes through the initialization process, it backs up the configuration information stored in the battery-powered SRAM memory device to the nonvolatile flash memory (NAND).

If the SRAM is erased or data corruption is detected, iLO tries to restore the configuration information from the backup file. Automatic restore operations are recorded in the IML.

When iLO security is disabled with the system maintenance switch, the SRAM data is not restored automatically.

The backup file created by the automatic backup and restore process is not user-accessible. It cannot be used to perform a manual restore operation.

Manual backup and restore

iLO supports manually restoring the configuration information stored in the battery-powered SRAM memory device. This feature is intended for use on a system with the same hardware configuration as the system that was backed up. It is not meant to duplicate a configuration and apply it to a different iLO system.

Hewlett Packard Enterprise does not expect that you will have a reason to perform a restore operation. However, there are cases in which having a backup of the configuration expedites the return to a normal operating environment.

As with any computer system, backing up your data is a recommended practice to minimize the impact from failures. Hewlett Packard Enterprise recommends performing a backup each time that you update the iLO firmware.

iLO firmware requirements for backup and restore

- iLO 5 firmware version 2.10 and later and iLO 6 support backup and restore operations in which the backup and restore tasks are performed on systems with the same or different iLO firmware versions.
- iLO 5 firmware versions earlier than 2.10 support backup and restore operations in which the backup and restore tasks are performed on systems with the same iLO firmware version.

Security vulnerability scanners and iLO

Security vulnerability scanners are used in server environments to probe for weaknesses that need to be investigated and addressed. The iLO team uses security vulnerability scanners in its quality labs for every iLO firmware release. 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 it is a security best practice to set the iLO security state to High Security or higher.

It is a best practice to test new versions of security vulnerability scanners in a lab environment before deploying them in a production environment. By definition, a security vulnerability scanner probes interfaces for known or suspected vulnerabilities. In effect, the scanner is attempting to hack the interface being tested. This operation might 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 identify. These items are described in the following sections, which include remediation recommendations. Many of these issues are resolved by setting the iLO security state to High Security or higher.

Subtopics

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 (CA). When iLO leaves the factory, the customer information and the server DNS name/IP address are unknown. Therefore, iLO uses a default self-signed certificate.

The iLO firmware provides the capability to create a Certificate Signing Request (CSR) that you can use to request a signed certificate from a CA. The signed certificate can then be imported into iLO.

- To complete this task by using the iLO web interface, see the iLO user guide (**iLO 5** or **iLO 6**).
- To complete this task by using RIBCL scripting, see the iLO scripting and command line guide (**https://www.hpe.com/support/ilo-docs**).
- To complete this task by using the RESTful Interface Tool and the iLO RESTful API, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.

More information

SSL certificates

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. For customers who are not actively using IPMI, Hewlett Packard Enterprise recommends leaving the IPMI over LAN interface disabled.

A Security Bulletin for this issue is available at the following website: **https://www.hpe.com/support/iLO234-SB-CVE-2013-4786**.

- To enable or disable IPMI over LAN by using the iLO web interface, see the iLO user guide (**iLO 5** or **iLO 6**).
- To enable and disable IPMI by using XML scripting, see the iLO scripting and command line guide (**https://www.hpe.com/support/ilo-docs**).
- To enable and disable IPMI by using the RESTful Interface Tool and the iLO RESTful API, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.

Hewlett Packard Enterprise recommends the iLO RESTful API as a replacement for the IPMI over LAN capabilities. For more information about the iLO RESTful API and the RESTful Interface Tool, see **https://www.hpe.com/info/redfish** or **https://www.hpe.com/support/restfulinterface/docs**.

If you require the use of IPMI, enabling it will expose this issue.

More information

Access control for features, ports, and protocols
Guidelines for using iLO with IPMI or DCMI over LAN

Untrusted TLS/SSL server X.509 certificate

Replace the default, self-signed SSL certificate with a certificate signed by a Certificate Authority (CA). When iLO leaves the factory, the customer information and the server DNS name/IP address are unknown. Therefore, iLO uses a default self-signed certificate.

The iLO firmware provides the capability to create a Certificate Signing Request (CSR) that you can use to request a signed certificate from a CA. The signed certificate can then be imported into iLO.

- To complete this task by using the iLO web interface, see the iLO user guide (**iLO 5** or **iLO 6**).
- To complete this task by using RIBCL scripting, see the iLO scripting and command line guide (**https://www.hpe.com/support/ilo-docs**).
- To complete this task by using the RESTful Interface Tool and the iLO RESTful API, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.

More information

SSL certificates

IPMI 1.5 GetChannelAuth Response Information Disclosure

This is an assumed vulnerability based on Hewlett Packard Enterprise support of the IPMI protocol. iLO itself is not susceptible to this vulnerability. This vulnerability report can be suppressed by disabling IPMI.

- To enable or disable IPMI over LAN by using the iLO web interface, see the iLO user guide (**iLO 5** or **iLO 6**).
- To enable and disable IPMI by using XML scripting, see the iLO scripting and command line guide (**https://www.hpe.com/support/ilo-docs**).
- To enable and disable IPMI by using the RESTful Interface Tool and the iLO RESTful API, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.

More information

Access control for features, ports, and protocols
Guidelines for using iLO with IPMI or DCMI over LAN

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 preauthenticated client to confirm the existence of a configured username. Hewlett Packard Enterprise recommends changing the default username.

If you are not actively using IPMI, Hewlett Packard Enterprise recommends disabling the interface.

- To enable or disable IPMI over LAN by using the iLO web interface, see the iLO user guide (**iLO 5** or **iLO 6**).
- To enable and disable IPMI by using XML scripting, see the iLO scripting and command line guide (**https://www.hpe.com/support/ilo-docs**).
- To enable and disable IPMI by using the RESTful Interface Tool and the iLO RESTful API, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.

More information

Access control for features, ports, and protocols
Guidelines for using iLO with IPMI or DCMI over LAN

Weak cryptographic key

This vulnerability can be addressed by setting the iLO security state to **High Security**. This action requires iLO to use higher grade ciphers.

This vulnerability will also be reported if the default SSL certificate is used.

The iLO firmware provides the capability to create a Certificate Signing Request (CSR) that you can use to request a signed certificate from a CA. The signed certificate can then be imported into iLO.

- To complete this task by using the iLO web interface, see the iLO user guide (**iLO 5** or **iLO 6**).
- To complete this task by using RIBCL scripting, see the iLO scripting and command line guide (**https://www.hpe.com/support/ilo-docs**).
- To complete this task by using the RESTful Interface Tool and the iLO RESTful API, see the following website:

https://www.hpe.com/support/restfulinterface/docs.

More information

SSL certificates
iLO encryption settings

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.

Missing HTTPOnly Flag from Cookie

When a security scanner reports `Missing HTTPOnly Flag from Cookie` as a vulnerability, it refers to a client-side defense mechanism that prevents client-side script attacks (XSS) from accessing HTTP-only cookies. HTTP-only cookies do not prevent all XSS exploits, and using them is not a substitute for eliminating XSS vulnerabilities. This setting cannot be relied on because some browsers do not support it. The version of the browser will be different in each iLO configuration.

Hewlett Packard Enterprise has implemented ways of defending against XSS attacks. Refer to the iLO firmware download page for the latest available security enhancements. In addition, replace default self-signed certificates with trusted certificates signed by a Certificate Authority.

iLO does not use externally provided content such as trackers, scripts, or HTML from other servers. There is no page content within iLO that did not come from administrators. Therefore, the reported vulnerability `Missing HTTPOnly Flag from Cookie` is not a true vulnerability.

When scanning iLO products, ignore this error or disable scanning for `Missing HTTPOnly Flag from Cookie`.

More information

SSL certificates

UEFI System Utilities server management features

You can use the UEFI System Utilities to configure the Server Configuration Lock feature, manage server settings and behavior, and configure supported third-party solutions. For information about performing tasks with the UEFI System Utilities, see the online help or view the user guide for your platform (https://www.hpe.com/info/UEFI-manuals).

Subtopics

Power-on password

Administrator password

HTTPS boot

Trusted platform module options

Advanced BIOS and platform security options

More information

HPE and third-party security solutions
Server Configuration Lock

Power-on password

Enabling the Set Power On Password feature causes a password prompt to display when you power on the server. The boot process will not continue until you enter the password.

To disable or clear the password, you can enter the password followed by a forward slash character (/).

NOTE:

If an Automatic Server Recovery (ASR) reboot occurs, the power-on password prompt is not displayed and the server boots normally.

The default setting is **Disabled**.

When this feature is enabled, you can use the System Maintenance Switch to disable the password requirement.

More information

System maintenance switch

Administrator password

Enabling the Set Admin Password feature causes a password prompt to display when you try to access the UEFI System Utilities or UEFI Shell. The password is required before you can continue to the UEFI System Utilities or UEFI Shell. Three password attempts are allowed.

When this feature is enabled, you can use the System Maintenance Switch to disable the password requirement.

More information

System maintenance switch

HTTPS boot

You can configure the HTTP support and TLS (HTTPS) Options settings in the UEFI System Utilities to enable a server to use a TLS session to boot to an HTTPS URI. This option provides a more secure alternative to PXE booting. To enable HTTPS boot, you must enroll the HTTPS server TLS certificate.

When configured, HTTPS boot options are added to the UEFI boot order list for network ports that are enabled for network boot.

In addition to managing HTTPS server certificates, you can configure advanced security settings for this feature. The options include the cipher suite, certificate validation type, strict hostname checking, and TLS protocol version.

Trusted platform module options

You can view the current Trusted Platform Module (TPM) configuration and update the settings with the UEFI System Utilities.

- By default, the TPM is enabled as TPM 2.0 when the server is powered on after installing it.
- In UEFI Mode, the TPM can be configured to operate as TPM 2.0 or TPM 1.2.
- In Legacy Boot Mode, the TPM configuration can be changed between TPM 1.2 and TPM 2.0, but only TPM 1.2 operation is supported.

CAUTION:

An OS that is using the TPM might lock all data access if you do not follow the proper procedures for modifying the server and suspending or disabling TPM in the OS. Following recommended procedures is important when updating system or option firmware, replacing hardware such as the system board and hard drive, and modifying TPM OS settings. Changing the TPM mode after installing an OS might cause issues, including data loss.

More information

Trusted Platform Module

Advanced BIOS and platform security options

Consider the following advanced options to enhance server security:

Platform Certificate Support

Enable or disable platform certificate support on Gen10 Plus and later products.

Allow login with iLO accounts

Allow users to log in to the ROM-based setup utility by using an iLO account with the Host BIOS privilege.

Backup ROM Image Authentication

Enable cryptographic authentication of the redundant ROM image at startup.

One-Time Boot Menu (F11 Prompt)

Enable or disable the F11 prompt during POST.

Intelligent Provisioning (F10 Prompt)

Enable or disable Intelligent Provisioning access.

UEFI Variable Access Firmware Control

Allow the system BIOS to control certain variables from being overwritten by other software such as the OS.

No-Execute Protection

Enable or disable data section non-execution protection.

Data security

Subtopics

Encryption and key management

Encryption and key management

UEFI-managed encryption

UEFI-managed encryption allows data-at-rest encryption for supported system devices such as persistent memory modules and NVMe drives.

Self-encrypting drives

For storage devices that support the Opal Storage Specification, security is enhanced by making the storage device self-encrypting (SED). Self-encrypting drives encrypt stored data so that it cannot be read by an unauthorized user. The encryption keys are protected by a local master key (LMK) or through the use of a random master key (RMK).

For more information about self-encrypting drives, see **Self-encrypting drives**.

To view the HPE self-encrypting drive offerings, see the HPE ProLiant Compute SSD Selector Tool: **https://ssd.hpe.com/**.

HPE SR storage controllers

HPE SR controllers support controller-based encryption (CBE) and Self encrypting drives (SED).

CBE

HPE Smart Array SR Secure Encryption is a controller-based, enterprise-class data encryption solution that protects data at rest on RAID volumes. HPE Secure Encryption is compatible with all hard disk drives (HDDs) or solid-state drives (SSDs).

HPE Smart Array SR Secure Encryption is a FIPS 140-2 Level 1 enterprise-class encryption solution that complies with regulations for sensitive data, such as HIPPA and Sarbanes-Oxley.

For more information, see the **HPE Smart Array SR Encryption Quickspecs** .

SED

SED is another choice for data-at-rest encryption. It is an HDD or SSD that contains an Advanced Encryption Standard (AES) hardware encryption engine, which encrypts data at line rate as it is written to the storage media, and provides access control by locking the drive when power is lost. The media encryption key (MEK) encrypts all the user data on the drive. It is stored encrypted on the drive and it cannot be accessed by the user. The MEK is encrypted with a user password, also called a key encrypting key (KEK), which is used to unlock the drive. The KEK can be stored and managed by Host key management (HKM), Local key management (LKM), and Remote key management (RKM).

SED is ideal for customers who need their data protected with encryption. SEDs provide data-at-rest protection, which means that when power is lost (for example, when the server is turned off), the drive is locked. If someone steals a drive from a server, they cannot read any of the data from that drive. SED performs at line rate, so it does not impact overall server performance, which is critical for customers in the financial service industry (FSI), healthcare, and the U.S. government sectors.

Secure Encryption is available for both local and remote key management methodologies. The remote key management mode requires an iLO Advanced license, an HPE Smart Array SR Secure Encryption LTU, and a supported key management application.

For more information, see the HPE Storage controllers and server: data encryption overview at the following website: **https://www.hpe.com/info/SCEO**.

HPE MR storage controllers

HPE MR storage controllers support Self-Encrypting Drives (SED) that secure the drive data from unauthorized access or modification. Because the data on the drive is encrypted, it cannot be accessed without appropriate security authorization, even if an SED drive is removed from the storage system.

The following key management types are supported:

- **Host Key Management (HKM)**—Manage SEDs by using third-party key management such as SEDutil. SED monitoring is available in HPE MR Storage Administrator, the Storage Command Line Interface (StorCLI) tool, and the UEFI System Utilities.
- **Local Key Management (LKM)**—Enable SED drive security for local key management by using HPE MR Storage Administrator, the StorCLI tool, or the UEFI System Utilities. During setup, you provide a security key identifier and security key. At startup, the security key stored in the controller unlocks the drive. When the drive is powered off, the security-enabled drive data encryption key is locked.
- **Remote Key Management (RKM)**—The UEFI System Utilities works with the iLO key manager configuration to create the security key identifier and security key in the remote key manager server. When the drive is powered off, the security-enabled drive data encryption key is locked. At startup, the security key is retrieved from the remote key manager server to unlock the drive.

To view the controllers a server or compute module supports, see the QuickSpecs document at the following website: **https://www.hpe.com/info/quickspecs**.

Remote key management

A remote key manager generates, stores, serves, controls, and audits access to data encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys.

iLO manages the key exchange between the key manager and the other products. iLO uses a unique user account based on its own MAC address for communicating with the key manager. For the initial creation of this account, iLO uses a deployment user account that pre-exists on the key manager with administrator privileges. For more information about the deployment user account, see the key manager documentation.

The following key managers are supported. For version information, see the iLO user guide.

- Utimaco Enterprise Secure Key Manager (ESKM)

  Click here to read more about the **HPE security for data at rest with Utimaco ESKM** solution.

- Thales products:
  - Thales TCT KeySecure for Government G350v (previously known as SafeNet AT KeySecure G350v)
  - Thales KeySecure k150v (previously known as SafeNet KeySecure 150v)
  - Thales CipherTrust Manager 2.2.0 virtual (k170v) and physical (k570) appliances.

    Click here to read more about the partnership between HPE and Thales.

Product decommission or repurpose

When you decommission a product or decide to use it for a different purpose, you can protect your data by using the One-button secure erase or System Erase and Reset features.

Subtopics

One-button secure erase

System Erase and Reset

One-button secure erase

If you want to decommission a server or prepare it for a different use, you can use the One-button secure erase feature.

One-button secure erase follows the NIST Special Publication 800-88 Revision 1 in the Guidelines for Media Sanitization guide. The appendix recommends minimum sanitization levels for media. For more information about the specification, see Section 2.5 **Guidelines for Media Sanitization**.

One-button secure erase implements the NIST SP 800-88 Revision 1 Sanitization Recommendations for **Purging** user data and returns the server and supported components to the default state. This feature automates many of the tasks that you follow in the Statement of Volatility document for a server.

One-button secure erase for DevIDs and System IAK

iLO IDevID, LDevID, System IDevID, and System IAK certificates are removed during the One-button secure erase process.

When you use the One-button secure erase process, Hewlett Packard Enterprise recommends performing a manual iLO backup to minimize the impact of losing the iLO IDevID, LDevID, System IDevID, and System IAK certificates. iLO includes all the certificates in its backup service and you can restore the certificates from the backup file.

Supported products

You can initiate the One-button secure erase process from the following products:

- iLO
- Intelligent Provisioning
- The iLO RESTful API
- iLOREST (iLO 6)

For details about the effects of using this feature, see the iLO user guide for your platform:

- **iLO 5 user guide**
- **iLO 6 user guide**

Subtopics

One-button secure erase FAQ

Does One-button secure erase purge USB devices and internal SD cards?

No. One-button secure erase does not erase USB devices and internal SD cards.

If an HDD does not support the Purge function, does One-button secure erase attempt to purge it?

No. One-button secure erase skips a drive that does not support the purge function.

Does One-button secure erase support HPE Storage controllers?

HPE SR controllers, MR controllers, and NS controllers are supported for One-button secure erase.

Does One-button secure erase erase drives that do not support Purge?

RAID controllers can wipe drives (overwrite with a pattern) that do not support the purge operation. One-button secure erase does not request the controller to perform this nonsecure wipe. To wipe data on such drives, use the Intelligent Provisioning System Erase and Reset feature.

Does One-button secure erase erase battery-backed cache?

See the following table for more information.

How does One-button secure erase process the erase commands?

See the following table for information on how One-button secure erase purges or overwrites data.

What privileges are required to launch One-button secure erase?

Users need all iLO privileges to launch One-button secure erase.

Does One-button secure erase remove the serial number and product ID?

No, these items are not erased by One-button secure erase.

How long does the process take?

The duration depends on the hardware. Sanitization of HDDs takes longer than SSDs.

How One-button secure erase affects supported drives

Device	Operation requested	Result
NVRAM	3-pass write: 0x5a, 0xa5, 0xff	All battery-backed iLO SRAM memory is overwritten.
Embedded Flash (NAND)	eMMC 5.1 (JEDEC 84-B51) Secure Erase command with SECURE_REMOVAL_TYPE in Extended CSD register set to physical memory erase, if supported by the device.	Data in physical memory is erased.
Intel Optane DC PMM	Secure Erase + Overwrite DIMM	Cryptographic keys are removed and data in all physical memory blocks (both user-accessible and in spare blocks) is overwritten with zeros. PCD regions containing all configuration and metadata is also overwritten.
NVDIMM-N [1]	JEDEC JESD245B Factory Default	Data in all physical memory blocks is erased except warranty information. All readable registers are reset to defaults.
UEFI configuration store	3-pass: Chip erase (0xff), 0x00, Chip erase (0xff)	All physical sectors are overwritten.
RTC	Reset time to 01-01-2001 00:00:00	Date, Time, Time zone, and DST are reset to defaults.

Device	Operation requested	Result
TPM	TPM Clear + Clear NV indices + Delete Platform Symmetric key	All data in TPM is cleared including any nonvolatile information.
HPE Smart Array SR controllers	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize **Note:** Before initiating the One-button secure erase, the Security reset function must be performed manually through the Smart Storage Administrator, if Smart Array Secure Encryption was enabled.	• The security reset function removes the drive keys that are stored on the key manager for remote key management. All secrets, keys, and passwords from the controller and drives are cleared. This operation does not remove the controller key on the key manager. • All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. • Flash backup is cleared and data in the DRAM write-back cache is lost when the power is removed. All attached drives are requested to be sanitized. See below for operations requested on the drives.
HPE Smart Array MR controllers [2], [3]	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	• All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. Encryption keys are cleared. • Flash backup is cleared and data in the DRAM write-back cache is lost when the power is removed. All attached drives are requested to be sanitized. See below for operations requested on the drives.
HPE NS204i-p Gen10 Plus Boot Controller [1]	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	• All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. All attached drives are requested to be sanitized. See below for operations requested on the drives.
HPE NS Boot Controller [4]	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	• All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. All attached drives are requested to be sanitized. See below for operations requested on the drives.
HPE Smart Array S100i and SR100i Software RAID [1]	Reset to SATA AHCI mode + Physical drive sanitize	The controller is reset to the default SATA AHCI mode. All attached SATA drives are requested to be sanitized as below.
SATA HDD [5]	ATA SANITIZE with CRYPTO SCRAMBLE EXT if supported.	The CRYPTO SCRAMBLE EXT command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of ATA SANITIZE with OVERWRITE EXT option	All physical sectors are overwritten with zeros, including physical sectors that are not user accessible. Any previous data in caches are also made inaccessible.

Device	Operation requested	Result
SATA SSD [5]	ATA SANITIZE with CRYPTO SCRAMBLE EXT if supported.	The CRYPTO SCRAMBLE EXT command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of ATA SANITIZE with BLOCK ERASE option	Previous data in all physical memory blocks, including physical memory blocks that are not user accessible, becomes irretrievable. Any previous data in caches are also made inaccessible.
SAS HDD [2], [6]	CRYPTOGRAPHIC ERASE (if supported)	The CRYPTOGRAPHIC ERASE command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of SCSI SANITIZE with OVERWRITE EXT option	All physical sectors are overwritten, including physical sectors that are not user accessible. Any data in caches are also sanitized.
SAS SSD [2]	CRYPTOGRAPHIC ERASE (if supported)	The CRYPTOGRAPHIC ERASE command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of SCSI SANITIZE with BLOCK ERASE option	All physical memory blocks, including physical memory blocks that are not user accessible, are set to a vendor-specific value. Any data in caches are also sanitized.
NVM Express	NVM Express FORMAT with Secure Erase Setting (SES) = 2, if supported.	This is a cryptographic erase accomplished by deleting the encryption key.
	NVM Express SANITIZE if supported (for drives supporting NVM Express version 1.3 or later) A single pass of NVM Express FORMAT with SES = 1. This option is used if the drive does not support the SANITIZE.	All data and metadata associated with all namespaces is destroyed. All user content present in the NVM subsystem is erased.

1 Applies to iLO 5
2 HPE Smart Array MR controllers do not support one-button secure erase on Gen 10 servers.
3 HPE Smart Array MR Gen 10 Plus and Gen 11 controllers support one-button secure erase only for drives that support Crypto Erase (CRYTO SCRAMBLE EXT for SATA, CRYPTOGRAPHIC ERASE for SAS, and Crypto Erase for NVMe).
4 Applies to iLO 6
5 These drives might be connected to HPE SR controllers and MR controllers or the Chipset SATA controller.
6 HPE MR controllers support only CRYPTOGRAPHIC ERASE.

Supported devices that fail the erase process and unsupported devices are not erased securely. These devices might contain sensitive data. Isolate devices that are not erased and use other methods to delete the data, or securely dispose of the devices according to your organization security policies.

System Erase and Reset

System Erase and Reset is initiated from Intelligent Provisioning. It clears hard drives and Intelligent Provisioning preferences.

When you use this feature, Intelligent Provisioning overwrites data on the drives using the guidelines from DoD 5220.22-M, which is similar to the NIST description of clearing data. All block devices attached to the system are overwritten by applying random patterns in a three-pass process. These block devices include drives attached to the server. Depending on the amount of storage installed on a system, the overwrite process can take many hours or even days to complete. Use this method to select and erase drives on the system that do not support the native sanitize methods used by the One-button secure erase process.

For more information, see the **Intelligent Provisioning user guide**.

Other management tools

Subtopics

Intelligent Provisioning security

You can access Intelligent Provisioning by rebooting a server and pressing the correct key during the boot process, or by using the Always On Intelligent Provisioning feature in iLO.

Some iLO and BIOS settings can be configured through Intelligent Provisioning.

Intelligent Provisioning security through iLO

Some Intelligent Provisioning security features depend on the iLO security settings.

- iLO controls remote access with required credentials and configurable encryption levels. Users must have the iLO **Host BIOS** and **Remote Console** privileges to launch Always On Intelligent Provisioning.
- Intelligent Provisioning is not supported on systems that use the High Security, FIPS, or CNSA security states. You can view and configure the security state on the Encryption Settings page in iLO.
- If you use a remote console to access Always On Intelligent Provisioning, credentials are required if the iLO Require Host Authentication access setting is enabled.
- Physical access to the server is determined by the physical security mechanisms set by your organization.

Intelligent Provisioning adheres to TPM requirements.

Intelligent Provisioning security through UEFI

You can disable Intelligent Provisioning access in the Advanced Security Options in the UEFI System Utilities.

HPE OneView security features

HPE OneView is a single integrated platform, packaged as an appliance, that implements a software-defined approach to managing your physical infrastructure through its entire life cycle.

HPE OneView has the following security features:

- Mandatory access control through:
  - Local or network/LDAP accounts
  - Passwords
  - Granular permissions (role and scope)
  - Audit logs
  - Two-factor authentication
- Uses certificates to authenticate and establish trust relationships.
- Is supported with regular updates from HPE.

Additionally, HPE OneView is delivered as a security-hardened appliance with the following features:

- The appliance uses a customized operating system that eliminates all nonessential services to reduce its attack surface.
- Minimizes vulnerabilities by running only the services required to provide functionality.
- Password protected OS boot loader.
- An IP firewall that only allows access to the ports required by HPE OneView services.
- Key services do not run as privileged OS uses.
- No users are allowed at the OS level. Users can interact with HPE OneView strictly through RESTful APIs, the state change message bus (AMPQ interface), SSH or appliance console for maintenance, or through the web interface.

For more information, see the documentation at **http://www.hpe.com/info/OneView/docs**.

HPE InfoSight for Servers security

The HPE InfoSight portal is a secure web interface hosted by HPE that allows you to monitor supported devices through a graphical interface.

HPE InfoSight for Servers:

- Combines the machine learning and predictive analytics of HPE InfoSight with the health and performance monitoring of Active Health System (AHS) and HPE iLO to optimize performance and predict and prevent problems.
- Provides automatic collection and analysis of the sensor and telemetry data from AHS to derive insights from the behaviors of the install base to provide recommendations to resolve problems and improve performance.

For more information about HPE InfoSight and security, see the following documents:

- **HPE InfoSight for Servers Security**
- **HPE Nimble Storage dHCI Solution Security Guide**

HPE and third-party security solutions

Subtopics

Microsoft Secured-core server support

AMD memory encryption

Intel Software Guard Extensions

Intel Trusted Execution Technology

Intel processor AES-NI support

Pensando Distributed Services Platform

Microsoft Secured-core server support

Microsoft Secured-core servers use a combination of hardware features, firmware enablement, and Windows Server OS capabilities to protect against malware and rootkit security exploits.

In general, Secured-core server provides:

- Comprehensive security—A suite of protection in a single enablement designed to work from boot to OS protection.
  - Hardware root-of-trust using Trusted Platform Module 2.0 (TPM 2.0).
  - Firmware protection enabled by processor support for Dynamic Root of Trust of Measurement (DRTM) technology and DMA protection.
  - Virtualization-based security (VBS) and hypervisor-based code integrity (HVCI).
- Preventative defense designed to prevent future exploits and attacks.

The Secured-core server AQ (Additional Qualification) defines an additional set of requirements to support and enable the Secured-core features with Windows Server 2022. Systems that meet the requirements are listed in the **Windows Server Catalog**.

This feature requires configuration in both the UEFI System Utilities and in the Windows OS. For more information, see the Implementing Microsoft Windows Server 2022 using HPE ProLiant Servers, Storage, and Networking Options **technical paper**.

AMD memory encryption

HPE servers with AMD processors support different types of memory encryption:

- Secure Memory Encryption (SME)—Full system memory encryption that helps defend data against certain cold boot and physical attacks. It transparently encrypts all physical memory and requires no software intervention or support. Memory pages are automatically decrypted and encrypted upon any reads or writes.
- Transparent SME (TSME)—A stricter subset of SME, TSME transparently encrypts all physical memory and requires no software intervention. Memory pages are automatically decrypted and encrypted upon any reads or writes. The ephemeral encryption key is created during each boot and it is not accessible by software.
- Secure Encrypted Virtualization (SEV)—A set of AMD technologies that help protect virtual machines with one of up to 509 unique encryption keys known only to the processor.

Intel Software Guard Extensions

The Intel Software Guard Extensions (SGX) protect platforms against privileged malware. This solution allows applications to partition data and code into protected memory regions called enclaves. The enclave cannot be read or written to by code running outside of the enclave environment. This feature allows an application to protect sensitive code and data from a compromised operating system, virtual machine manager, or another virtual machine. SGX is used with Intel SGX drivers installed in the OS.

You can configure this feature with the UEFI System Utilities on Gen10 Plus servers with Intel processors that support it.

Intel Trusted Execution Technology

Intel Trusted Execution Technology (TXT) uses a TPM and cryptographic techniques to measure software and platform components to prevent malfunctioning or compromised components from running. It protects against software-based attacks that would modify the system configuration. You can configure this feature with the UEFI System Utilities on supported servers with Intel processors.

For support information, check the product QuickSpecs document: **https://www.hpe.com/info/qs**.

Intel processor AES-NI support

Intel AES-NI is an encryption instruction set that improves on the Advanced Encryption Standard (AES) algorithm. It accelerates data encryption and decryption on supported processors. AES-NI provides faster data protection and greater security, and it makes pervasive encryption possible in new areas.

For support information, check the product QuickSpecs document: **https://www.hpe.com/info/qs**.

Pensando Distributed Services Platform

The Pensando Distributed Services Platform (DSP) for supported Hewlett Packard Enterprise servers provides a powerful suite of software-defined services—like firewall, micro-segmentation, and telemetry—directly to the server. It boosts network and security performance by moving those services to the server edge, where the transition between network and server occurs. This solution replaces multiple appliances and reduces cost and complexity while improving security.

For more information, see **https://www.hpe.com/solutions/Pensando**.

Recommended security settings

This section provides recommended security practices related to passwords, iLO, and the UEFI System Utilities. For information about using the security features, see the product documentation.

Subtopics

Password guidelines

iLO security setting recommendations

UEFI System Utilities security setting recommendations

Password guidelines

Hewlett Packard Enterprise recommends that you follow these password guidelines when you create and update 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. Examples include the company name, product name, user name, or login name.
  - Change passwords regularly.
  - Keep the iLO default credentials in a safe place.
- Use strong passwords with at least three of the following characteristics:
  - At least one uppercase ASCII character
  - At least one lowercase ASCII character
  - At least one ASCII digit
  - At least one other type of character (for example, a symbol, special character, or punctuation).

  If you enable the Password complexity setting on the iLO Access Settings page, iLO enforces these password characteristics when you

create or edit an iLO user account.

iLO security setting recommendations

Hewlett Packard Enterprise recommends the following iLO security settings. For details about these settings, see the iLO online help or the iLO user guide. If a setting is not listed with a recommendation, determine the appropriate value based on your environment and security priorities.

Security Dashboard

Monitor all the security parameters without setting the Ignore option (default).

Remote Console security

- Enable Remote Console Computer Lock and, optionally, configure a custom computer lock key sequence.
- Enable IRC requires a trusted certificate in iLO to launch the .NET IRC by using an HTTPS connection.

Local user account controls

Configure up to 12 local user accounts, with a range of individual user privilege settings to support the security principle of least access.

Directory group account controls

Configure up to six directory groups to use with Kerberos authentication or schema-free directory integration.

Key management

Use an optional key manager to generate, store, serve, control, and audit access to data encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys.

Firmware verification

Configure the Enable Background Scan option and choose the Integrity Failure Action.

Server access settings

- Server Name—Leave this value blank and let the host OS assign it.
- Server FQDN/IP Address—Leave this value blank and let the host OS assign it.

Account Service access settings

- Authentication Failures Before Delay—One failure causes no delay (default)
- Authentication Failure Delay Time—Ten seconds (default)
- Authentication Failure Logging—Enabled-Every Failure
- Minimum Password Length—Eight characters (default)
- Password Complexity—Enabled

iLO access settings

- Downloadable Virtual Serial Port Log—Disabled (default)
- Idle Connection Timeout (minutes)—30 minutes (default)
- iLO Functionality—Enabled (default)
- iLO RIBCL Interface—Enabled (default)

  Hewlett Packard Enterprise recommends using the iLO RESTful API.
- iLO ROM-Based Setup Utility—Enabled (default)
- iLO Web Interface—Enabled (default)

- Remote Console Thumbnail—Disabled
- Require Host Authentication—Enabled

  The default value depends on the configured security state:

  - Production mode—Disabled by default.
  - High Security—Enabled by default.
  - FIPS or CNSA—Enabled by default and cannot be disabled.
- Require Login for iLO RBSU—Enabled
- Serial Command Line Interface Status —Enabled-Authentication Required (default)

  You must also set the Serial Command Line Interface Speed.
- Show iLO IP during POST —Enabled (default)
- Show Server Health on External Monitor —Enabled (default)
- VGA Port Detect Override—Enabled (default)
- **Virtual NIC**—Disabled

  The default setting in most versions of iLO is Disabled. In iLO 5 v2.10, the default setting is Enabled. When you reset iLO to the factory default settings, the Virtual NIC setting returns to the default setting for the installed version of iLO. Firmware upgrades or downgrades do not affect this setting.

Network access settings

- Anonymous Data—Enabled (default)
- IPMI/DCMI over LAN—Disabled (default, includes port setting)
- Remote Console—Enabled (default, includes port setting)
- Secure Shell (SSH)—Enabled (default, includes port setting)
- SNMP—Disabled (includes port settings)

  This setting is disabled automatically when you enable a security state higher than Production or High Security.
- Virtual Media—Enabled (default, includes port setting)
- Virtual Serial Port Log Over CLI —Disabled (default)
- Web Server—Enabled (default, must set non-SSL and SSL ports)

  If disabled, access is removed for RIBCL, iLO RESTful API, remote console, iLO Federation, and the iLO web interface.
- 802.1X Support—Enabled

Update service settings

- Downgrade Policy—Allow downgrades (default)

  CAUTION:

  Review the options in the iLO user guide before you modify this setting.
- Accept 3rd Party Firmware Update Packages —Disabled

iLO Service Port

- iLO Service Port—Enabled (default)
- USB flash drives—Disabled
- Require authentication—Enabled

- USB Ethernet adapters—Disabled

Secure Shell Key

Using SSH keys provides better security than simple password authorization.

Keys must be 2048-bit DSA or RSA (or ECDSA 384-bit keys in CNSA security state)

Authorized certificates for smart card or CAC environment

Each local user account must have an associated certificate.

Using a smart card with certificates provides better security than simple password authentication.

CAC/Smartcard settings:

- CAC Smartcard Authentication—Enabled (requires an iLO Advanced license)
- CAC Strict Mode—(Optional) Enabled
- Directory User Certificate Name Mapping —When using directory integration, select the correct option according to your user certificate.
- Import Trusted CA Certificates and revocation list —At least one trusted CA certificate must be installed, along with a revocation list.
- OCSP Settings—Enter the URL of an accepted OCSP provider to check user certificates for authentication.

SSL certificates

Install a trusted SSL certificate for each iLO. Default self-signed certificates are not secure.

Security State

High Security (minimum)

Single sign-on

SSO Trust Mode—Trust by Certificate

Some HPE applications may not successfully use SSO when the iLO security state is set to High Security and above. See your application documentation for more information.

UEFI System Utilities security setting recommendations

Hewlett Packard Enterprise recommends the following UEFI System Utilities settings. For details about these settings, see the UEFI System Utilities online help or user guide for your platform (**https://www.hpe.com/info/UEFI-manuals**. If a setting is not listed with a recommendation, determine the appropriate value based on your environment and security priorities.

Set Power On Password

Set a password that is compliant with strong security standards.

Set Admin Password

Set a password that is compliant with strong security standards.

Secure Boot settings

Attempt Secure Boot—Enabled

Secure Boot requires UEFI boot mode.

TLS (HTTPS) 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

Processor AES-NI Support

Enabled

Trusted Platform Module Options

- TPM 2.0 Operation—No Action
- TPM Mode Switch Operation—TPM 2.0
- TPM 2.0 Visibility—Visible
- TPM UEFI Option ROM Measurement—Enabled

SATA Controller Options

- Embedded SATA Configuration—To support SATA secure erase, this option must be set to SATA AHCI Support and the installed SATA drives must support the secure erase command.
- SATA Secure Erase— Enable this option to allow SATA secure erase functions to work. This control does not start the secure erase function.

Intel Security Options

- Intel TXT Support—Enabled, if available.

Advanced Security Options

- One-Time Boot Menu (F11 Prompt) —Disabled
- Intelligent Provisioning (F10 Prompt)—Enabled
- Backup ROM Image Authentication—Enabled

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

iLO 6 Configuration Utility

- iLO 6 Functionality—Enabled
- iLO 6 Configuration Utility—Enabled
- Require user login and configuration privilege for iLO 6 Configuration —Enabled
- Show iLO 6 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

Security resources

Critical product security vulnerability alerts

https://www.hpe.com/info/security-alerts

This website provides detailed information about the latest critical security vulnerability alerts.

Security bulletins

To view the HPE Security Bulletin Library, click Security Bulletin Library on the following website: **https://support.hpe.com/hpesc/public/home**.

To report a security vulnerability, click the Report a security vulnerability link on the HPE Security Bulletin Library webpage.

Product alerts

To sign up for email updates, click Sign up for Product Alerts on the following website: **https://support.hpe.com/hpesc/public/home**.

Server Security Solutions

https://www.hpe.com/us/en/solutions/infrastructure-security.html

This website provides information about server security, including articles, press releases, videos, and technical papers.

InfusionPoints reports

- **How HPE is Leading Supply Chain Security**
- **Device Identity and Component Attestation comes to HPE Gen10 Plus servers**

Ponemon Institute report

Closing the IT Security Gaps 2020 Global Study by the Ponemon Institute

Moor Insights & Strategy technical paper

Zero Trust - Five Steps For Enterprise IT

Project Aurora

https://www.hpe.com/security/ProjectAurora

HPE and Thales CipherTrust Data Security Platform

HPE servers and storage with Thales CipherTrust Data Security Platform

Licensing

For information about security feature licensing requirements, see the HPE iLO Licensing Guide (**https://www.hpe.com/support/iLOLicenseGuide-en**).

iLO 5 Cryptographic Module FIPS 140-2 Non-Proprietary Security Policy

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3122

HPE Resource Library

https://www.hpe.com/us/en/resource-library.html

Support and other resources

Subtopics

Accessing Hewlett Packard Enterprise Support

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  https://www.hpe.com/info/assistance

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

  https://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

HPE product registration

To gain the full benefits of the Hewlett Packard Enterprise Support Center and your purchased support services, add your contracts and products to your account on the HPESC.

- When you add your contracts and products, you receive enhanced personalization, workspace alerts, insights through the dashboards, and easier management of your environment.
- You will also receive recommendations and tailored product knowledge to self-solve any issues, as well as streamlined case creation for faster time to resolution when you must create a case.

To learn how to add your contracts and products, see https://www.hpe.com/info/add-products-contracts.

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

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

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter

- To subscribe to eNewsletters and alerts:

  https://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:

  https://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 Account set up with relevant entitlements.

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 initiates a fast and accurate resolution based on the service level of your product. 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.

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Tech Care Service

https://www.hpe.com/services/techcare

HPE Complete Care Service

https://www.hpe.com/services/completecare

Warranty information

To view the warranty information for your product, see the **warranty check tool**.

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:

https://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:

https://www.hpe.com/info/reach

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

https://www.hpe.com/info/ecodata

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

https://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, use the Feedback button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. This process captures all document information.