

Hitachi Advanced Server HA800 G6 Series Compute Security

Reference Guide

Notices

The information provided here is subject to change without notice. Hitachi Vantara's products and services are covered only by the express warranty statements that come with them. This document does not constitute an additional warranty. Hitachi Vantara is not responsible for any technical or editorial errors or omissions in this document.

Confidential computer software. You must have a valid license from Hitachi Vantara to possess, use, or copy the software. In accordance with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under the vendor's standard commercial license.

Links to third-party websites will take you outside of the Hitachi Vantara website. Hitachi Vantara has no control over and is not responsible for the information outside the Hitachi Vantara website.

Acknowledgments

AMD is a trademark of Advanced Micro Devices, Inc.

Ampere[®] is a registered trademark of Ampere Computing.

Intel[®] is a trademark of Intel Corporation in the U.S. and other countries.

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

SAS[®] is a registered trademark or trademark of SAS Institute, Inc.

VMware[®] is a registered trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions.

All third-party marks are property of their respective owners.

Contents

- Compute security features..... 6**

- Supply chain security..... 7**
 - Trusted Supply Chain.....7
 - Trusted Supply Chain server configuration.....7
 - Server Security Optimized Service for Server.....8
 - Server Configuration Lock.....9
 - Chassis intrusion detection switch.....10
 - Platform certificates.....10
 - Platform Certificate Verification Tool.....10

- Zero trust security..... 11**
 - Silicon root of trust.....11
 - Secure boot.....13
 - SPDM authentication.....14
 - SPDM supported algorithms.....14
 - Server identity.....16
 - 802.1 X and iLO.....18
 - Trusted Platform Module.....18
 - Unauthorized access prevention.....18
 - Persistence-enabled attack protection.....19
 - iLO firewall for system ROM and iLO firmware.....20

- Physical access security.....21**
 - System maintenance switch.....21
 - Reasons to disable iLO security.....22
 - USB security.....23
 - iLO Service Port.....23
 - Rack and power security.....23
 - Bezel lock.....23

- Cloud-based management.....24**
 - Compute Ops Management security features.....24
 - Compute Ops Management security FAQ.....26
 - General.....27
 - Processing of personal data.....27
 - Data and data access.....29
 - Regulations compliance governance.....30
 - Business continuity.....31
 - Authentication.....32
 - Connectivity.....32

- iLO server management features.....34**

iLO security guidelines.....	34
Ports used by the iLO features	35
Access control for features, ports, and protocols.....	38
iLO network connection options	38
Virtual LAN	40
Network and management ports.....	40
SSH keys.....	40
SSL certificates	41
Guidelines for using iLO with IPMI or DCMI over LAN	41
Security dashboard.....	42
Causes of security risk status	42
Security audits.....	44
Security Log.....	44
Remote console security.....	44
iLO encryption settings	44
iLO security states	45
Connecting to iLO when using CNSA mode.....	47
iLO 5 SSH cipher, key exchange, and MAC support	47
iLO 6 SSH cipher, key exchange, and MAC support	48
iLO 7 SSH cipher, key exchange, and MAC support	49
iLO 5 and iLO 6 SSL cipher and MAC support.....	49
iLO 7 SSL cipher and MAC support.....	51
FIPS validation and Common Criteria certification	52
Kerberos authentication with iLO.....	53
Schema-free directory authentication.....	53
Extended Schema directory authentication	54
Directory services support.....	54
Firmware verification.....	54
System Recovery Set.....	55
iLO backup and restore	56

Security vulnerability scanners and iLO..... 57

UEFI System Utilities server management features 59

Power-on password.....	59
Administrator password.....	59
HTTPS boot.....	59
Trusted platform module options.....	59
Advanced BIOS and platform security options	60

Encryption and key management..... 61

Server lifecycle decommission or repurpose. 63

One-button secure erase.....	63
One-button secure erase FAQ.....	64
System Erase and Reset.....	67

Third-party security solutions. 70

Microsoft Secured-core server support.....	70
AMD memory encryption	70

Intel Software Guard Extensions.....	70
Intel Trusted Execution Technology.....	71
Intel processor AES-NI support	71
Pensando Distributed Services Platform	71
Recommended security settings.....	72
Password guidelines	72
Recommended security settings for iLO.....	72
UEFI System Utilities security setting recommendations.....	76

Compute security features

Compute security features are designed to meet security challenges by continually improving the hardware and firmware security of Hitachi Vantara servers and related hardware environments. The security features ensure that every link in the chain of security provides effective protection.

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 Hitachi Vantara 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.

Supply chain security

Hitachi Vantara server security starts with the supply chain and extends throughout the product life cycle.

Trusted Supply Chain

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

- 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.
- Server Security Optimized Service for Hitachi Vantara—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.

Trusted Supply Chain server configuration

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

Country of origin USA

Built in secure Hitachi Vantara 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

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

Trusted authenticity

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

Unique labeling

Trusted Supply Chain products include a **T** in the server model name. A Trusted Supply Chain sticker is placed on the product hardware.

iLO security state: High Security (iLO 5, iLO 6), Secure Standard (iLO 7)

Configuring iLO to use High Security or Secure Standard 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 Hitachi Vantara to load an OS at the factory, enabling UEFI Secure Boot ensures that each component launched during the boot process is digitally signed. 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 Trusted Supply Chain server is delivered to the end-user location.

Server Configuration Lock: Enabled

This feature takes cryptographic measurements, or images, of the supported 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 Hitachi Vantara 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 re-lock the server before it ships to the end-user location.

Chassis intrusion detection switch: Enabled

This mechanism protects the 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](#)

[Server Configuration Lock](#)

[Chassis intrusion detection switch](#)

[Secure boot](#)

[iLO security states](#)

Server Security Optimized Service for Advanced Server

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

iLO security state: High Security (iLO 5, iLO 6), Secure Standard (iLO 7)

Configuring iLO to use High Security or Secure Standard 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 as Hitachi Vantara load an OS at the factory, enabling UEFI Secure Boot ensures that each component launched during the boot process is digitally signed. 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 Trusted Supply Chain server is delivered to the end-user location.

Server Configuration Lock: Enabled

This feature takes cryptographic measurements, or images, of the supported 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 Hitachi Vantara 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 re-lock the server before it ships to the end-user location.

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 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](#)

[Server Configuration Lock](#)

[Chassis intrusion detection switch](#)

[Secure boot](#)

[iLO security states](#)

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.

Trusted Supply Chain servers ship with this feature enabled and the server is set to `in-transit` status. Hitachi Vantara 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.

More information

[Server Security Optimized Service for Advanced Server
Trusted Supply Chain server configuration](#)

- _____ -
-

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 Hitachi Vantara website.

Platform certificates

On supported Hitachi Vantara servers, 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 Hitachi Vantara.

Platform certificates are used to detect supply chain tampering. When a customer receives a server, they can use the 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](#)

[Platform Certificate Verification Tool](#)

Platform Certificate Verification Tool

On a server provisioned with a Trusted Computing Group (TCG)-compliant platform certificate, you can use the Hitachi Vantara 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 Hitachi Vantara factory.
- If a measurement does not match the reference value, this result indicates that the configuration changed since the server left the Hitachi Vantara 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 PCVT and view the documentation at the Hitachi Vantara website.

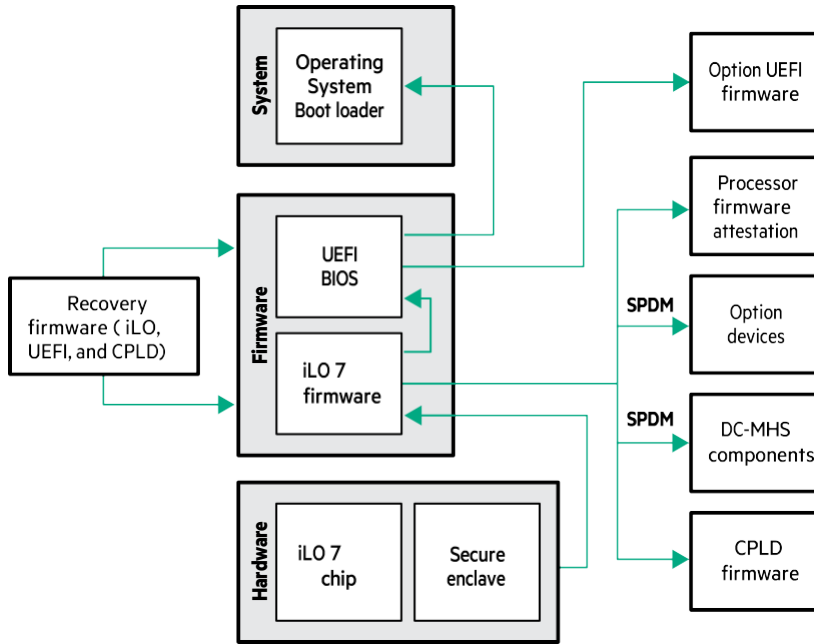
More information

[Platform certificates](#)

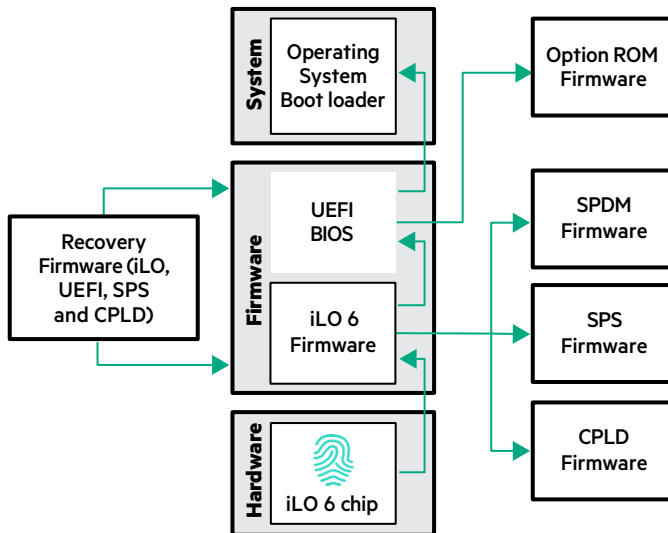
Zero trust security

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

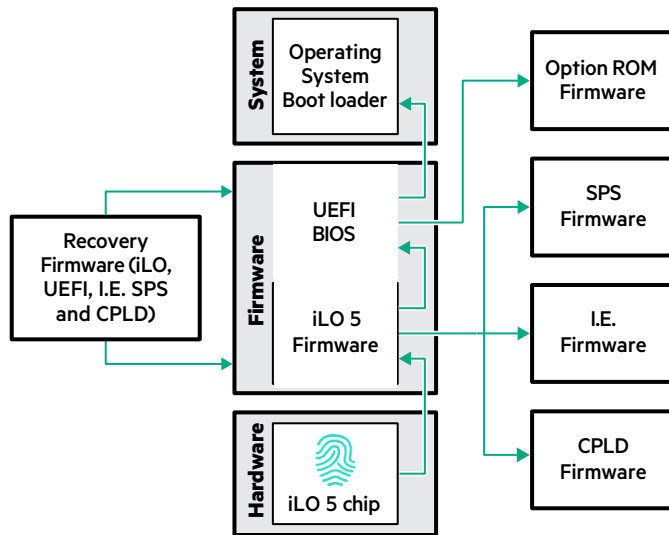
Silicon root of trust



iLO 7 silicon root of trust with secure enclave



iLO 6 silicon root of trust



iLO 5 silicon root of trust Silicon

root of trust and recovery

Depending on your server generation, the iLO 7 secure enclave, iLO 6 chip, or iLO 5 chip acts as a silicon root of trust. The silicon root of trust makes it impossible to insert any malware, virus, or compromised code that could corrupt the server boot process.

- **Secure enclave (iLO 7)**—An independent security processor embedded on the system boards of supported Hitachi Vantara servers. It provides comprehensive anti-tamper measures, side-channel resistance, and layered security. On servers with iLO 7, the iLO chip controls server management features and the secure enclave focuses on security. The iLO 7 secure enclave is designed to meet the FIPS 140-3 Level 3 standards.
- **iLO chip**—A remote server management processor embedded on the system boards of supported Hitachi Vantara servers. iLO enables the monitoring and controlling of servers from remote locations. On servers with iLO 6 and iLO 5, the iLO chip provides both server management and security features.

A digital fingerprint of the iLO firmware is embedded in the secure enclave (iLO 7) or the iLO chip (iLO 6 and iLO 5) at a trusted chip fabrication facility. At startup, the iLO firmware integrity is verified against the digital fingerprint to determine if it is allowed to run. If the iLO firmware fails the validation process, the system automatically restores the iLO firmware from the System Recovery Set.

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

- CPLD (System Programmable Logic)
- Innovation Engine (iLO 5 only)
- Server Platform Services (SPS) firmware (iLO 5 and iLO 6)
The SPS firmware runs on the management engine (ME).
- SPDM Firmware (iLO 6 and iLO 7)
- UEFI BIOS (system ROM)

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 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 a supported firmware type fails validation, the system automatically restores it 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.

Improved key storage in the secure enclave (iLO 7)

Protecting the keys used to encrypt business critical data should be an essential component of any business continuity plan. Keys for encrypting data at rest need to be protected against natural disasters, theft, ransomware, and even network outages.

Advanced Key Management in iLO 7 protects local keys by providing a secure repository for keys, certificates, and other server security assets. This feature is an improvement over using the TPM to encrypt local keys, because the keys are not stored in an exposed location.

PQC Code signing (iLO 7)

Post-quantum cryptographic (PQC) methods with Leighton-Micali Signatures (LMS) are used to sign the iLO 7 firmware with a quantum-resistant digital signature.

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.

You can use a directly attached management console or the iLO remote console to customize the certificates embedded in the UEFI BIOS.

For information about using the iLO RESTful API to configure the secure boot settings, see the iLO RESTful API documentation, contact Hitachi Vantara.

SPDM authentication

Hitachi Vantara servers with iLO 7 and 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.

To enable this feature, use the iLO web interface or the iLO RESTful API to configure the **Global Component Integrity** option and the **Component Integrity Policy**.

- **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, configure a policy 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 non-authentic component changes the iLO security status to **Risk**.

iLO supports the SPDM specification v1.0, v1.0.1, v1.1, and v1.2 for authentication. For devices with no supported 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

More information

[SPDM supported algorithms](#)

SPDM supported algorithms

Based on the configured security state, iLO categorizes the SPDM algorithms as described in **G3 servers**.

G3 servers

FIPS or Secure Standard

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

G4 servers

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 zero trust operation.

The iLO server identity features enable supported servers to make a zero-trust connection to cloud-based tools such as Hitachi Vantara 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 IDDevID/ LDevID as the iLO TLS certificate.

In addition to DevID identity credentials, Hitachi Vantara provisions servers with Attestation Key (AK) credentials. AK credentials are similar to their DevID counterparts and can be used for attestation use cases.

Hitachi Vantara supports both factory-provisioned and field-provisioned (customer-defined) server identity and attestation credentials. Factory-provisioned credentials have lifetime validity and are immutable. For flexibility, factory credentials are provisioned to the server iLO and the TPM. In each case, the private key component of each credential is protected by the iLO or the TPM chip it is bound to. Credentials bound to the TPM comply with the Trusted Computing Group (TCG) **TPM 2.0 Keys for Device Identity and Attestation** specification.

Terminology

The IEEE 802.1AR DevID standard defines a manufacturer-provided *Initial Device Identifier* (IDDevID). An IDDevID can be complemented by one or more *Locally Significant Device Identifiers* (LDevIDs) provided by a network administrator after manufacturing. The TCG has adopted the same designations for the Initial (IAK) and Locally significant (LAK) Attestation Key.

At the factory, Hitachi Vantara might provision more than one DevID and AK credential set to identify different elements of a system. To comply with the described naming scheme, Hitachi Vantara designates additional factory-provisioned DevID and AK credentials that complement the existing IDDevID and IAK credentials as *System LDevID* and *System LAK*.

NOTE: To avoid confusion and emphasize the distinction between permanent HV-issued IDDevIDs/IAKs and System LDevIDs/ System LAKs compared to customer-supplied LDevIDs and LAKs, this topic uses the terms factory-provisioned and field-provisioned.

Factory-provisioned DevID and AK credentials

Different generations of Hitachi Vantara servers carry a different complement of factory-provisioned DevID and AK credentials. The following list outlines the certificate types provisioned with each generation.

G3

- iLO PCA IDevID
- iLO PCA IAK
- iLO System LDevID
- iLO System LAK
- TPM System IDevID
- TPM System IAK

Credentials with *System* in their name identify the server as a whole and reference the chassis serial number. Later generations of servers contain additional *PCA* IDevID and IAK credentials. These credentials enable separate identification and attestation of the internal circuit board that hosts the iLO and TPM components. Hitachi Vantara recommends that all but a few specialized use cases should employ the credentials containing *System* in their title to ensure the highest levels of interoperability with authentication and attestation protocols and standards.

Field-provisioned LDevID credentials

Hitachi Vantara servers support provisioning of customer-supplied, field-provisioned LDevID credentials for the TPM. Field-provisioned LDevID certificates might contain customer-specific information to enable custom authentication and authorization scenarios and can be changed over the lifetime of the server. A customer can provision an arbitrary number of these credentials to the TPM (limited by TPM capacity), certified by their designated PKI (Public Key Infrastructure).

Hitachi Vantara servers can also be provisioned with one customer-supplied LDevID certificate on the iLO. Like its TPM counterparts, the field-provisioned iLO LDevID certificate is fully specified by the customer.

Accessing the certificates using Redfish

You can view the Identity and Attestation certificates provisioned to a server (both iLO and TPM-based) by using the following iLO RESTful API GET commands:

```
/redfish/v1/CertificateService/
```

or:

/redfish/v1/Managers/1/SecurityService/

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.

iLO supports EAP-TLS authentication for onboarding into an 802.1X access-controlled network.

- Using a factory-provisioned server identity, an Hitachi Vantera server can securely onboard and establish its identity for unattended autonomous operation. Depending on your iLO version, iLO IDevID, iLO IDevIDPCA, or both types are supported.
- iLO also supports a user-provisioned server identity (LDevID) for 802.1X authentication.

When a factory-provisioned and a user-provisioned server identity are present on a system, the user-provisioned LDevID is used for EAP-TLS authentication.

802.1X authentication is enabled by default. iLO does not initiate EAP-TLS authentication or respond to authentication requests if the system does not have an iLO DevID.

To use 802.1X on a server with a preinstalled secure device identity, configure your Authentication, Authorization, and Accounting (AAA) server to accept the iLO DevID certificate. For example, configure the AAA server to support EAP-TLS and install the DevID issuer certificate in the RADIUS server.

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.

More information

[Trusted platform module options](#)

Unauthorized access prevention

Access to iLO 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.

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 (iLO 5 and iLO 6) or the **User Management > Users** page (iLO 7).

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

Two-factor authentication

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

Personal Identity Verification

Personal Identity Verification (PIV) credentials are supported.

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.

Security keys

Manages the 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 iLO can flash, including the iLO firmware, UEFI BIOS (system ROM), and CPLD, 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 5 and iLO 6 use 2048-bit RSA keys and iLO 7 uses ED25519 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 time 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.

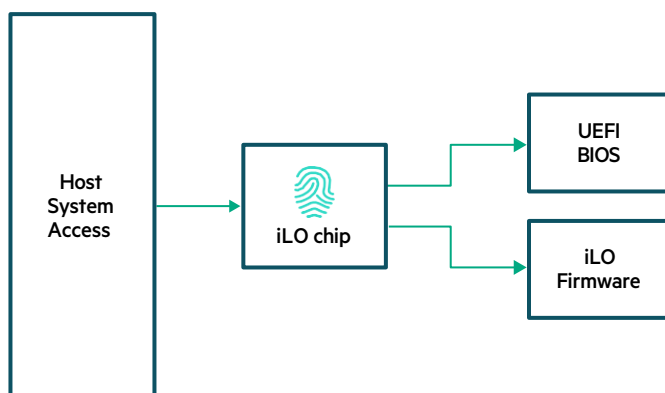
More information

[Silicon root of trust](#)

iLO firewall for system ROM and iLO firmware

Hitachi Vantara servers 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.



Physical access security

More information

[Chassis intrusion detection switch](#)

System maintenance switch

Hitachi Vantara 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 it down, and remove the access cover.

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

iLO security (position 1) for G6 servers

On G6 servers, the iLO security setting on the system maintenance switch enables the process for recovering the default iLO password.

iLO security (position 1) for G4 servers

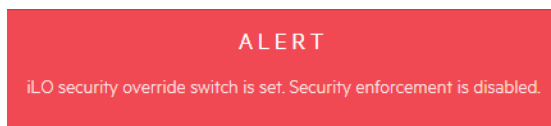
The iLO security setting on the system maintenance switch provides emergency access to an administrator who has physical control of the system board.

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.

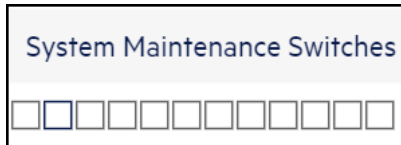
When the switch is on, configured BIOS administrator and power-on passwords are removed.

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.

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:

G3 servers

All user accounts that have the Administer User Accounts privilege are locked out and the default password is misplaced or forgotten.

G4 servers

- 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

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.

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 for iLO access.

- Connect to the iLO Service Port on a server with iLO 7 by using a standard USB Type A to Type C cable or a USB Type C to Type C cable.
- Connect to the iLO Service Port on servers with iLO 5 or iLO 6 by using a supported Ethernet adapter.

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.

More information

[Recommended security settings for iLO](#)

Rack and power security

Hitachi Vantara 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.

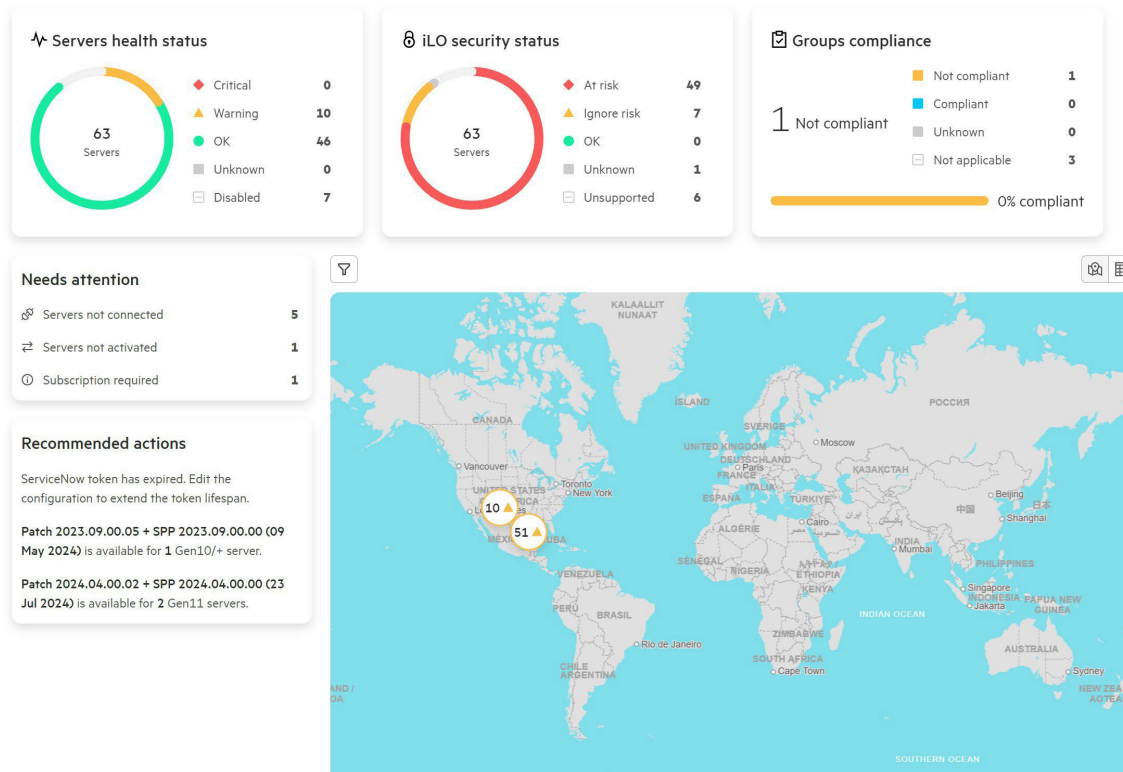
For more information about these solutions, contact Hitachi Vantara.

Bezel lock

For protection against external access on supported products, you can install a bezel lock.

Cloud-based management

Overview



Compute Ops Management security features

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).

Scope-based access control

GreenLake resource restriction policies (RRPs) and scope groups can be used with Compute Ops Management when you want to limit the servers 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, apply an RRP or scope group to the administrator user account roles. User accounts that are configured for scope based access control can perform management actions only on the servers specified by the Compute Ops Management filter associated with the RRP or scope group. All other servers in the affected service instance are read-only. If a user with restricted access starts a management action on a read-only server, an authorization error occurs.

When a user account is configured with scope based access control, the user:

- Can view all servers and server groups in a workspace.
- Can perform management actions on servers and server group members that are included in the Compute Ops Management filter associated with the configured RRP or scope group.

On servers that are not included in the Compute Ops Management filter associated with the configured RRP or scope group, users can perform the **Configure email notification preference** action.

On server group members that are not included in the Compute Ops Management filter associated with the configured RRP or scope group, users can perform compliance checking actions.

- Can manage server groups, but cannot configure the **Automate adding servers** option.
- Can run reports.
- Cannot manage saved filters or disable the scope based access control feature on a saved filter.

The available scope based access control features depend on your workspace configuration.

- Use RRP when using a workspace that is not configured with the enhanced GreenLake Identity and Access Management (IAM) features.
- Use scope groups when using a workspace that is configured with the GreenLake enhanced IAM features.

For more information about the GreenLake IAM features, contact Hitachi Vantara.

Audit log

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

iLO security risk monitoring

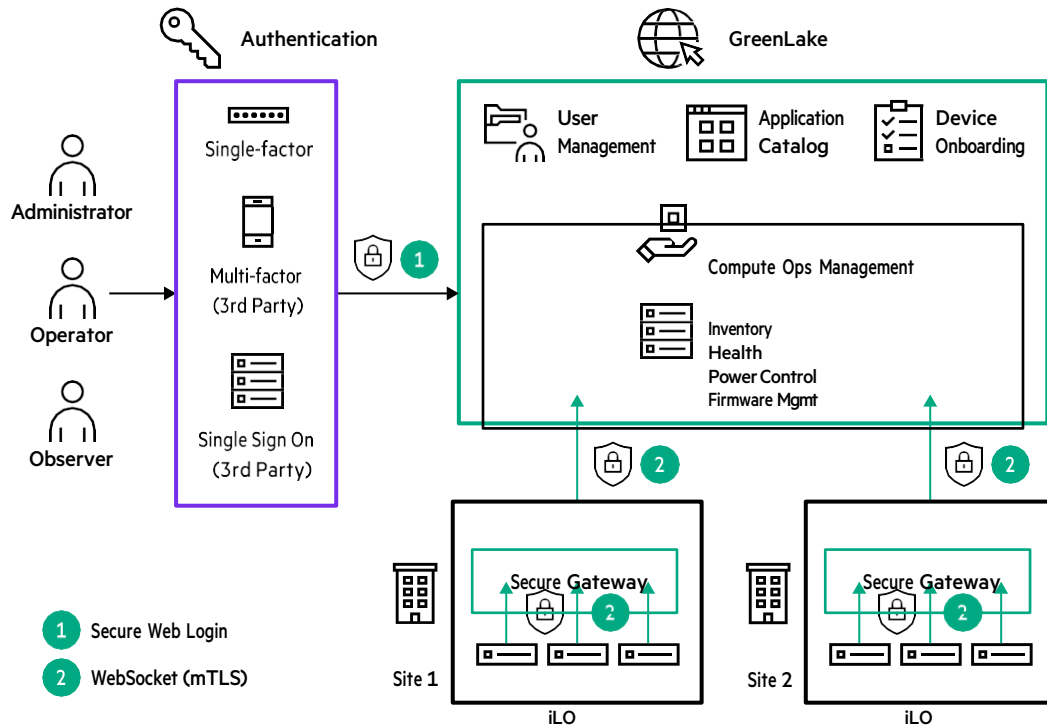
Compute Ops Management monitors the iLO security dashboard to alert you to potential security risks. The security risk status is calculated by comparing the server configuration to a predefined set of security recommendations.

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.

Secure gateway

Compute Ops Management secure gateway allows Compute Ops Management customers to aggregate their on-premise iLO connections from the data center over a single outbound connection to Compute Ops Management. This feature eliminates the need to have each iLO connected individually over the internet to Compute Ops Management.

Secure gateway is an on-premise appliance deployed as a virtual machine.



Secure gateway features include:

- Virtual machine-based appliance delivered as a VMware ESXi (7 and 8) Open Virtual Appliance (OVA)
- Automatic secure gateway appliance software updates through Compute Ops Management
- iLO connection aggregation sends data over a secure connection to Compute Ops Management
- Automatic recovery from service and cloud connection failures
- Efficient firmware updates
The secure gateway supports optimized component downloads by caching server firmware components. This feature decreases the internet-facing network resources used for firmware updates, which reduces costs and improves firmware update reliability. The secure gateway ensures that any component that is already downloaded and cached will not be downloaded from Hitachi Vantara again to perform a subsequent firmware update.

Compute Ops Management security FAQ

The following sections provide answers to frequently asked questions about Compute Ops Management.

General

Can Compute Ops Management features be disabled to prevent unauthorized changes?

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 administrators and operators can manage.

You can also use custom roles to allow or prevent the use of certain features. For example, performing an operating system image deployment requires the Server Edit permission that is included by default in the Operator and Administrator roles.

What certifications does Compute Ops Management have?

CAIQ STAR level1 and SOC2 Type2 certified.

Does Compute Ops Management have a OneTrust ADQ number?

No.

Who is responsible for the physical security of the solution?

- The cloud providers for GreenLake are responsible for the physical security of the software-as-a-service (SaaS) application hosted infrastructure.
- The customer is responsible for the physical security of the customer-owned managed devices.

How is change management handled?

The change management process is documented.

System and user changes to managed devices are saved in the GreenLake Audit Log for more than six months.

Processing of personal data

Does Hitachi Vantara handle data according to a records retention policy?

Hitachi Vantara records retention policies focus on legal retention requirements and align with current global principles and recognized industry standards. Hitachi Vantara maintains a records retention policy that defines "records" and how long they must be retained.

Does Hitachi Vantara have a Data Protection or Privacy officer?

The Data Protection Officer is available, contact Hitachi Vantara.

For more information, see the [Information Commissioner's Office \(ico.\) documentation](#).

Where is customer data located? Are there international data transfers or restrictions?

Hitachi Vantara is a global company and many of our business processes utilize a global operational model. Personal data given to HV might be transferred across state and country borders for the purposes of data consolidation, storage, and simplified customer information management. Any access or transfer of personal information across state or country boundaries must comply with applicable local laws and contractual requirements.

Hitachi Vantara has Binding Corporate Rules (BCRs) for controllers to address the transfer of personal data it controls from the EU, EEA, and Switzerland to its non-EU operations.

Hitachi Vantara is not certified under the EU-US Privacy Shield program.

If a customer has special requirements or restrictions on the movement or transfer of data, these requirements are agreed to in the contract. To the extent agreed upon in the contract, these requirements or restrictions are incorporated into the HV business processes used to deliver the services.

If the transfer of personal customer data from the EU, EEA, and Switzerland to Hitachi Vantara non-EU operations is required in connection with any service, Hitachi Vantara will sign controller to processor EU Model contracts with the customer.

Does Hitachi Vantara comply with individual rights requests?

Hitachi Vantara has a process for managing requests by individuals to exercise their rights under the General Data Protection Regulation (GDPR).

Any requests received for personal data controlled by a customer are forwarded to the customer for the customer to process.

Does Hitachi Vantara routinely assess third parties who process data on its behalf?

Yes.

Does Hitachi Vantara have policies, processes, and procedures in place for assessing compliance with legal and contract requirements?

Hitachi Vantara requires that service providers who handle or process personal data sign appropriate privacy and security contract terms which specify the required data-protection measures.

Hitachi Vantara reserves the right to audit service providers on a regular basis for compliance with applicable laws and contractual requirements.

For more information see the GreenLake [SaaS data sheet](#).

Does Hitachi Vantara maintain contracts with third parties to ensure the availability, integrity, and confidentiality of data?

Yes. These contracts typically include provisions to ensure that data is handled securely and that the third parties follow Hitachi Vantara's stringent security standards and compliance and auditing requirements.

How long does it take Hitachi Vantara to notify a customer about an incident?

The Hitachi Vantara incident response process requires notification to a customer “without undue delay” when their EU personal data has been involved in a “personal data breach” as defined by the GDPR (no later than 72 hours after having become aware of it).

Does Hitachi Vantara have policies and procedures to ensure that response and recovery plans are established, in place, and managed?

Yes.

For more information, contact Hitachi Vantara for the Global Privacy Policy.

Does Hitachi Vantara train its workforce on privacy policies, procedures, laws, and other requirements?

All Hitachi Vantara employees are required to take the Standards of Business Conduct training on an annual basis. This training includes modules on data privacy, security, and information handling.

Depending on job responsibilities, employees might be required to take additional training courses customized to meet the needs of their job.

Hitachi Vantara has other privacy and security training modules available to employees through our training catalog, and also conducts on-demand security awareness campaigns.

How does Hitachi Vantara ensure Privacy by Design?

The Hitachi Vantara privacy program is designed to help ensure that it complies with all applicable data protection laws in its role as a controller or processor of customer data, including the requirements of the GDPR.

The Privacy Office is responsible for monitoring developments in privacy laws globally. The Privacy Office attorneys review new laws or changes to existing laws to assess the impact on the business and identify required changes to Hitachi Vantara privacy policies, programs, or other business practices.

Legally, the customer is responsible for determining whether their use of Hitachi Vantara products and services to process their personal data is compliant with the data protection and other laws to which they are subject.

Hitachi Vantara has three main privacy policies:

- The **Global Master Privacy Policy** governs the handling of personal data of both employees and business contacts.
- An online **privacy statement** governing online privacy and other data collection activities, which is accessible from all Hitachi Vantara webpages.
- An Employee Data Privacy Policy governing the processing of personal data related to current, past, and prospective employees, which is accessible to internal users.

Has Hitachi Vantara introduced measures to prevent unauthorized sharing and to protect data that is transferred to a third country?

Hitachi Vantara is a global company and many of our business processes utilize a global operational model. Personal data given to HV might be transferred across state and country borders for the purposes of data consolidation, storage, and simplified customer information management. Any access or transfer of personal information across state or country boundaries must comply with applicable local laws and contractual requirements.

Hitachi Vantara has Binding Corporate Rules (BCRs) for controllers to address the transfer of personal data it controls from the EU, EEA, and Switzerland to its non-EU operations.

It is not certified under the EU-US Privacy Shield program.

If a customer has special requirements or restrictions on the movement or transfer of data, these requirements are agreed to in the contract. To the extent agreed upon in the contract, these requirements or restrictions are incorporated into the business processes used to deliver the services.

If the transfer of personal customer data from the EU, EEA, and Switzerland to Hitachi Vantara non-EU operations is required in connection with any service, HV will sign controller to processor EU Model contracts with the customer.

For more information, contact Hitachi Vantara.

Data and data access

Do Hitachi Vantara employees have superuser access to GreenLake customer workspaces?

No. Only users that are added to an GreenLake workspace have access.

The user who creates an GreenLake account is the default administrator, and this user can invite other users and configure user account permissions.

Hitachi Vantara cannot access the customer data on managed servers.

What access do Hitachi Vantara support personnel need for troubleshooting an issue?

A support agent needs access to the activity logs, which the customer can provide.

A customer also has the option of granting workspace access to a support agent.

In some cases, a support agent needs the GreenLake workspace ID so that they can review the Compute Ops Management application logs.

Selected support personnel and engineers have access to managed server hardware inventory data and software-as-a-service (SaaS) application data. Hitachi Vantara has a review process to control access to this data.

Hitachi Vantara cannot access the customer data on managed servers.

What GreenLake and Compute Ops Management roles are available?

You can assign built-in or custom roles. Users have access to only the features supported by their assigned roles.

For more information, see:

What information does Compute Ops Management store, and where is it stored?

- Compute Ops Management stores the full server inventory that is available through Redfish APIs from a managed server. The stored data includes server IP address, serial number, and part number. Compute Ops Management stores this data within the region selected by the customer during the initial setup process.
- GreenLake stores users, roles, user email addresses, and permissions. Compute Ops Management retrieves this information when it is needed.

What data is transmitted from Compute Ops Management to the customer?

- Email notifications are sent if configured by the customer. These notifications might include summary and health information and automatic case creation details.
- Reports are generated within Compute Ops Management and can be saved externally.
- Server inventory and other details are stored within Compute Ops Management and are not transmitted externally.

Are audit, authentication, and configuration logs ISO 27001 compliant, and can they be forwarded or downloaded for integration into solutions like SAN CLaaS?

Audit logs can be downloaded from GreenLake.

ISO 27001 requires logging for Security, System, Application, and User Events. The GreenLake audit log includes these events, but GreenLake had not completed the ISO 27001 certification process.

Are server iLO configurations saved and stored to enable restoration?

Compute Ops Management does not back up and store the iLO configuration.

What happens to the data when a server is removed from Compute Ops Management?

All managed server inventory data is deleted when a server is removed from Compute Ops Management. This process relies on AWS controls for data sanitization.

For more information, see *Media destruction* in the following document: <https://aws.amazon.com/compliance/data-center/controls/>.

Regulations compliance governance

What are the details of the Hitachi Vantara compliance framework and programs?

- Hitachi Vantara is a global company and many of our business processes utilize a global operational model. The Regulatory Compliance & Governance Office is responsible for establishing and maintaining compliance with applicable laws.
- Information about the Standards of Business Conduct, contact Hitachi Vantara.

How does Hitachi Vantara anticipate changes in laws and regulations?

Hitachi Vantara is a global company. The Operations, Legal & Administrative Affairs team employs attorneys who monitor for emerging laws and regulations in their jurisdictions. Emerging requirements are assessed to determine whether they will affect Hitachi Vantara. If so, a readiness and implementation project team, which includes stakeholders from global functions and business units, is assembled. Its mission is to prepare the company for compliance.

Does Hitachi Vantara comply with all regulations or is Hitachi Vantara confronted with conflicting regulations resulting in noncompliance?

Hitachi Vantara complies with applicable laws and contractual requirements.

What does Hitachi Vantara have in place to ensure that customers are informed about service or brand-damaging events?

Hitachi Vantara has a security incident response process that includes:

- Industry-wide best practices
- Knowledge of and adherence to applicable legal requirements in the event of data loss
- Communication plans geared toward limiting risk exposure

The Privacy Office maintains an incident response plan to address privacy issues, including required notifications to regulators, individuals, or customers as a result of an incident involving personal data.

- Security incidents involving personal data controlled by a customer are handled in conjunction with the data breach response requirements in the services contract.
- The incident response process requires notification to a customer “without undue delay” when their EU personal data has been involved in a “personal data breach” as defined by the General Data Protection Regulation (GDPR).

Business continuity

Does Hitachi Vantara have a Business Continuity Plan?

Compute Ops Management has a documented, evaluated, approved, communicated, tested, and maintained business continuity management and operational resiliency policy and procedure. This document is published internally.

For more information, see the **Consensus Assessment Initiative Questionnaire (CAIQ)** document.

How often is the Business Continuity Plan tested, and how is it tested?

The Compute Ops Management team reviews and tests the business continuity and operational resiliency documentation and plans annually, and any necessary updates are made.

The business response team (BRT) participates in an annual game day with other stakeholders.

Compute Ops Management has a documented, evaluated, approved, communicated, and maintained business continuity management and operational resiliency policy and procedure. This document is published internally.

For more information, see the **Consensus Assessment Initiative Questionnaire (CAIQ)** document.

Does the Business Continuity Plan include a minimum tolerable service disruption period? How does Hitachi Vantara ensure that they can recover service within that period?

Hitachi Vantara has processes in place to ensure that service will be recovered within a prescribed time frame.

How are data backups conducted?

GreenLake and Compute Ops Management are a hosted solution that is built with redundancy in mind so that the solution could tolerate the failure of a data center.

Database backups are taken periodically so that they can be used in a disaster recovery scenario.

Could GreenLake access to iLO be temporarily disabled if a security breach occurred in an GreenLake workspace?

Internet connectivity for iLO can be disabled. In this scenario, direct access to the iLO from the local network is available for direct device management.

Can customers choose where data is hosted?

Compute Ops Management is a software-as-a-service (SaaS) application shared by multiple customers. The solution is architected across multiple availability zones for disaster recovery and business continuity.

Compute Ops Management uses AWS for hosting in the following locations:

- US West
- AP NorthEast
- EU Central

Data is stored at the hosted region. Backup, disaster recovery, and business continuity policies are configured appropriately by the application team and are not configurable by customers.

Authentication

How does authentication work with GreenLake and Compute Ops Management?

GreenLake requires an email address for login, SSO, and communication. Customers can also store user contact information related to a managed device location.

What iLO features are accessible through Compute Ops Management for remote administrators?

iLO access depends on the assigned iLO user privileges. Compute Ops Management supports remote console access and requires the user to log in with their iLO credentials. When you click a link in Compute Ops Management to start the iLO remote console, you have access to only the features allowed by your iLO privileges.

When a server is connected to Compute Ops Management, Compute Ops Management has administrator access to the server iLO. All iLO features are not available through the Compute Ops Management connection. Only the features exposed by Compute Ops Management are available. Access to specific Compute Ops Management features is protected by the roles, scope, and permissions granted to users in GreenLake.

Connectivity

What encryption technology is used with Compute Ops Management?

Each managed device uses a unique key pair for sending data securely over mTLS with a zero trust policy.

- Encryption in transit uses the following ciphers:

TLS 1.2

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TSL_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

TLS 1.3

- TLS_AES_128_GCM_SHA256
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
- Encryption at rest uses AES-256.

Does the iLO on a managed server require access to local network resources?

iLO connectivity to other network segments is not required, only iLO access to Compute Ops Management (through the Internet) is required. If there is no connectivity to the local network resources, some services such as Active Directory and NTP servers are not available. These resources are not required for using Compute Ops Management.

Local network access is recommended for performing operating system installations through Compute Ops Management.

Are configuration changes and software updates pushed from GreenLake to the server iLO, or are they prepared for the server profile, after which the server iLO connects, downloads, and installs and configures them?

Changes are driven from Compute Ops Management to the server. When the change request is a firmware update, the iLO downloads the firmware directly.

Is the Compute Ops Management connection unidirectional or bidirectional?

The connection is a WebSocket connection that includes requests and responses. iLO initiates the WebSocket connection, Compute Ops Management does not open a connection to iLO on its own. The connection is always initiated by the managed server to Compute Ops Management. Communication is bidirectional after the encrypted WebSocket connection is established.

iLO server management features

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

You can use the iLO RESTful API to perform many of the tasks that are available through the iLO web interface. For more information, contact Hitachi Vantara.

NOTE:

For iLO 5 and iLO 6, RIBCL and the scripting tools HPQLOCFG, LOCFG.PL, and HPONCFG have entered the sustenance stage. Hitachi Vantara will now provide only critical bug and security fixes for RIBCL. These tools are not supported with iLO 7.

Hitachi Vantara recommends using the iLOREST Tool or iLO RESTful API.

More information


[Recommended security settings](#)

iLO security guidelines

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

The following guidelines apply to iLO 5, iLO 6, and iLO 7.

- Set up iLO on a dedicated management network.
Hitachi Vantara 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.
- Do not connect iLO 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.

- Replace the default self-signed certificate by installing an SSL certificate that is signed by a Certificate Authority (CA).
- Install trusted CA certificates to enable certificate validation for external services such as LDAP.
- Change the password for your user accounts, including the default user account.
Change the iLO management passwords according to the same guidelines as the server administrative passwords.

 **IMPORTANT:** Follow the iLO user account [password guidelines](#) when you create and update user accounts.

- Instead of creating user accounts with all privileges, create multiple accounts with fewer privileges.
- Keep your iLO and server firmware up to date.
- 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.

This feature provides 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.

- Disable ports and protocols that you do not use (for example, **SNMP** or **IPMI/DCMI over LAN**).
- Disable features that you do not use (for example, remote console).
- Configure the remote console to automatically lock the server OS console.
- Disable the iLO Configuration Utility in the UEFI System Utilities or configure iLO to require login credentials when users access it.
- Disable the ROM-based configuration utility in the UEFI System Utilities or configure iLO to require login credentials when users access it.
- Configure iLO to log authentication failures.
- Enable firmware verification scans.
- Depending on your iLO version, use the **Security** or **Security Dashboard** page to monitor security risks and recommendations.
- Use the **Security Log** to monitor security-related events.
- Set the **Downgrade Policy** to **Downgrade requires Recovery Set privilege**.
- Keep the Recovery Set up to date.
- 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.

The following guidelines apply only to iLO 5 and iLO 6.

- Configure a higher security state on the **Encryption Settings** page.
- Enable the **Require Host Authentication** feature.
- 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.

Ports used by the 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.

Network settings and ports

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 ²	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 ²	17988	TCP
Virtual Media Enables you to specify whether virtual media is enabled or disabled.	Enabled	
Web Server Non-SSL Port (HTTP) ²	80	TCP
Web Server SSL Port (HTTPS) ²	443	TCP
Web Server ^{3, 2} Allows you to enable or disable access through the iLO web server.	Enabled	

¹ Applies to iLO 6 and iLO 7

² Applies to iLO 5 and iLO 6

³ 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 might be used for outgoing third-party services in your environment.

Other ports used by iLO

Description	Default port	Protocol type
DNS Resolution	53	UDP
iLO Federation/SSDP Multicast ¹	1900	UDP
SSDP Multicast ²		
DHCPv4	67, 68	UDP
DHCPv6	547	UDP
NTP	123	UDP
NetBIOS Name Service/WINS ³	137	UDP
Kerberos KDC Server Port	88	TCP, UDP
Directory Server LDAP SSL Port	636	TCP
AlertMail SMTP Port	25	TCP
Remote Syslog Port	514	UDP
Key Manager Port	9000	TCP
Remote Support Port	7906	TCP

¹ Applies to iLO 5.

² Applies to iLO 6 and iLO 7.

³ Applies to iLO 5 and iLO 6.

Ports not supported by iLO

iLO does not support the commonly used ports listed in the next table.

Unsupported ports

Description	Port	Protocol type	Notes
LDAP-unsecured <ul style="list-style-type: none">• Connection (TCP)• Connectionless (UDP)	389	TCP/UDP	iLO uses secure port 636 for outgoing LDAP connections.
Global Catalog LDAP-unsecured <ul style="list-style-type: none">• Connection (TCP)• Connectionless (UDP)	3268	TCP/UDP	iLO uses secure LDAP connections.

Access control for features, ports, and protocols

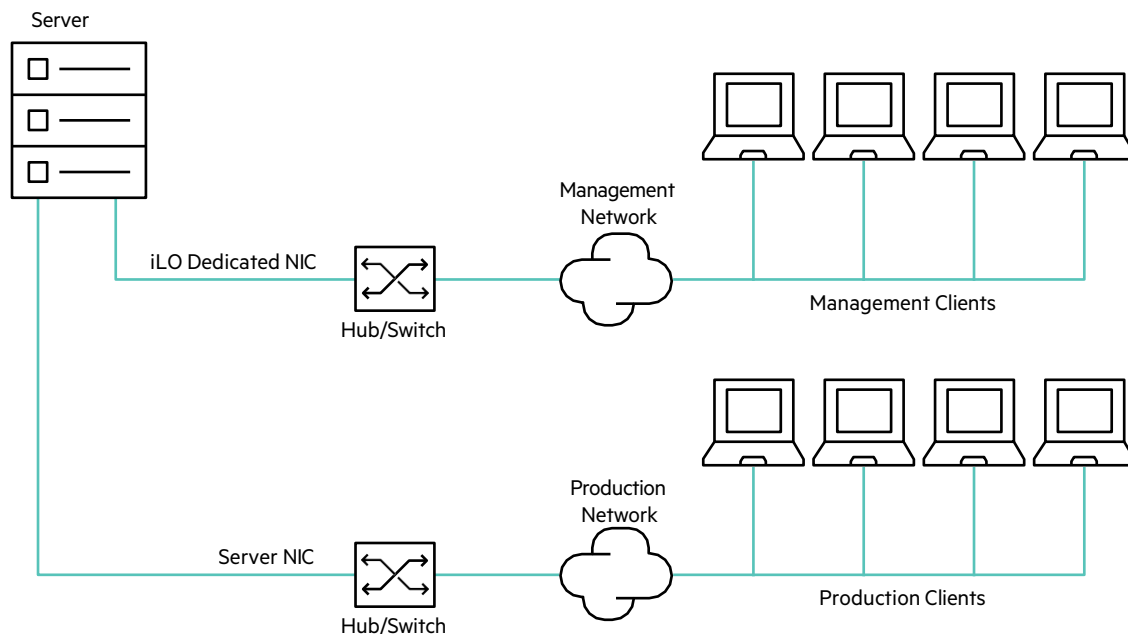
iLO allows you to disable unused features, ports, and protocols. For more information, see the iLO user guide.

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.



Dedicated management network

Production network

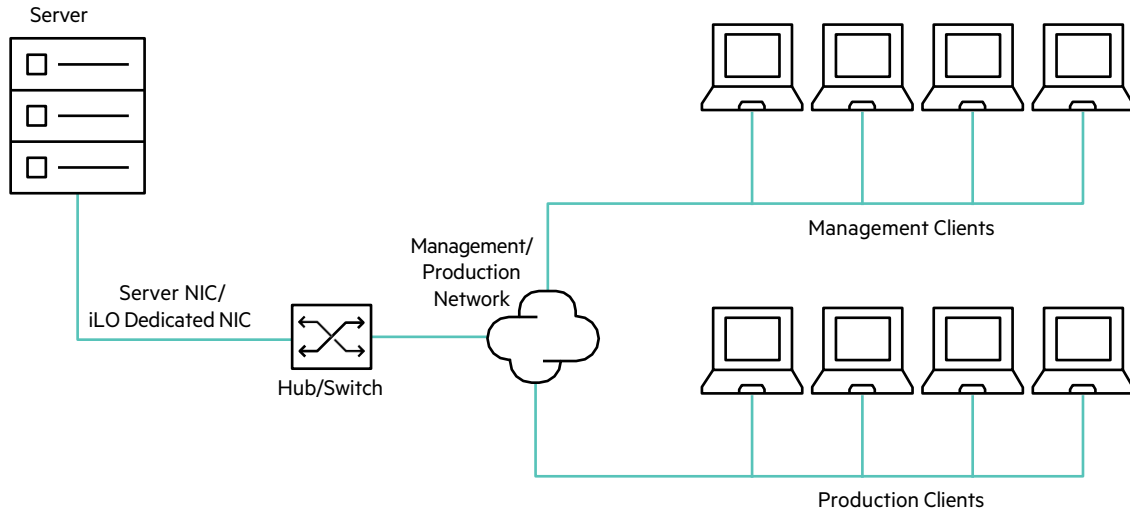
In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hitachi Vantara embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere 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.



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.
- 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 a user is removed after an SSH key is authorized for that user, the SSH key is removed.
- For iLO 5 and iLO 6 only:


- Only the iLO legacy format is supported with RIBCL scripts.
- 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.

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. Hitachi Vantara 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

[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 Hitachi Vantara.

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>.

These vulnerabilities were addressed 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. Hitachi Vantara 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, Hitachi Vantara 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.

More information

[Server Configuration Lock](#)

[iLO security states](#)

Causes of security risk status

The following security features are monitored on the iLO **Security Dashboard**. 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.

NOTE: On G3 servers with iLO 7 only: iLO detects a chassis intrusion even if the system does not have any power source. An IML entry is logged with the time stamp of the first intrusion.

Hitachi Vantara 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.

Hitachi Vantara recommends enabling this feature.

Default SSL Certificate In Use

The iLO default self-signed certificate is in use.

Hitachi Vantara recommends configuring a trusted certificate.

IPMI/DCMI Over LAN

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

Hitachi Vantara recommends disabling this feature. **Last**

Firmware Scan Result

The last firmware verification test failed. A firmware component is corrupted or its integrity is compromised. Hitachi Vantara recommends updating the affected firmware component to a verified image.

To use this feature, you must install a license.

Minimum Password Length

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

Hitachi Vantara recommends setting this value to 8 (default) or greater.

Password Complexity

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

Require Host Authentication (iLO 5 and iLO 6 only)

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.

Hitachi Vantara recommends enabling this feature. **Require**

Login for iLO RBSU (iLO 5 and iLO 6 only)

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.

Hitachi Vantara recommends enabling this feature. **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.

Hitachi Vantara recommends enabling this feature.

For more information, see the UEFI System Utilities documentation.

Security Override Switch (iLO 5 and iLO 6 only)

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.

Hitachi Vantara recommends disabling this feature.

For more information, see the iLO user guide.

SNMPv1 Request

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

Hitachi Vantara recommends disabling this feature.

Global Component Integrity (iLO 6 and iLO 7 only)

SPDM authentication is enabled. This configuration allows iLO to authenticate all applicable components in the server using SPDM. Disabling the **Global Component Integrity** option 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 (iLO 5 and iLO 6)

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.

Hitachi Vantara 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

iLO Standard gives customers the ability to configure a server security state. The highest-level encryption capabilities of CNSA are supported with an iLO Advanced license.

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.

iLO 7 security states

- Secure Standard
- FIPS
- CNSA
- Synergy Security Mode

iLO 5 and iLO 6 security states

- Production
- High Security
- FIPS
- CNSA
- Synergy Security Mode

iLO security states

Production (iLO 5 and iLO 6 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 (iLO 5, iLO 6) and Secure Standard (iLO 7 default)

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

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
- Remote console data uses AES-128 bidirectional encryption.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- On G4 servers only: 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.

When iLO is set to this security state:

- iLO 5 2.73 and later, iLO 6 and iLO 7 operate in a mode intended to comply with the requirements of FIPS 140-3 level 1.

Earlier versions of iLO 5 operate 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. For more information, see **FIPS validation and Common Criteria certification**.

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

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
- Remote console data uses AES-128 bidirectional encryption.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- On G4 servers only: 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 (previously called SuiteB mode) is available only when the FIPS security state is enabled.

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.
- On G4 servers, 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
- Hitachi Vantara and third-party scripting and command-line tools
- Hitachi Vantara and third-party management tools

- AlertMail, syslog, LDAP, or key manager servers
- Remote support software
- The iLO 7 firmware uses CNSA 2.0 signing algorithms - *Leighton-Micali Signature* (LMS).
- Firmware that is not LMS-signed cannot be flashed or uploaded to iLO 7 repository when the CNSA security state is configured.
- On servers with iLO 5 and iLO 6, use the HTML5 remote console instead of the .NET IRC. The HTML5 remote console enforces the use of AES-256 bit CNSA-compliant ciphers and the .NET IRC is not CNSA-compliant.

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

[iLO 5 SSH cipher, key exchange, and MAC support](#)

[iLO 6 SSH cipher, key exchange, and MAC support](#)

[System maintenance switch](#)

Connecting to iLO when using CNSA mode

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

Web browser

Configure the browser to support TLS 1.2, 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.

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

SSH connection

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

iLO RESTful API

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

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

iLO 7 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:

FIPS or Secure Standard

- aes256-ctr, aes256-gcm@openssh.com
- diffie-hellman-group-exchange-sha256, ecdh-sha2-nistp384
- hmac-sha2-256
- ssh-ed25519, rsa-sha2-512, rsa-sha2-256

CNSA

- aes256-gcm@openssh.com
- ecdh-sha2-nistp384
- hmac-sha2-256
- ecdsa-sha2-nistp384,rsa-sha2-512

Synergy Security Mode

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

iLO 5 and iLO 6 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
- iLO RESTful API

- CLI commands
- 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)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-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)
- 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)
- 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)

iLO 7 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, and CLI commands.

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
- iLO RESTful API
- CLI commands

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

Secure Standard

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)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-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)
- 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)
- 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

iLO 7

The iLO 7 secure enclave is designed to meet the FIPS 140-3 Level 3 standards.

Compute G6 servers support the NIST and CNSA 2.0 quantum resistance requirement.



TIP: Watch future revisions to this document for information about iLO 7 FIPS validation and Common Criteria certification.

iLO 6

- The cryptographic module for iLO 6 is in the evaluation process for FIPS 140-3 validation. For more information, see the **[NIST Cryptographic Module Validation Program web page](#)**.
- iLO 6 v1.11 is in the evaluation process for Common Criteria certification (EAL4+ (ALC_FLR.2)). For more information, see the following website: **[Products in evaluation](#)**.

iLO 5

iLO 5 v1.11 has attained the following:

- The cryptographic module for iLO 5 v1.11 is FIPS 140.2 Level 1 validated. See the NIST Cryptographic Module Validation certificate on the [NIST website](#).
- 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 on the [Common Criteria](#) website.

Check the following link for Common Criteria evaluation updates: [Products in evaluation](#).

- iLO 5 v2.73 is in the evaluation process for Common Criteria certification (EAL4+ (ALC_FLR.2)). For more information, see the following website: [Products in evaluation](#).

Kerberos authentication with iLO

Kerberos support enables a user to log in to iLO by clicking the **Zero Sign In** button on the login page instead of entering a user name and password. To log in successfully, the client workstation must be logged in to the domain, and the user must be a member of a directory group for which iLO is configured. If the workstation is not logged in to the domain, the user can log in to iLO by using the Kerberos UPN and domain password.

Because a system administrator establishes a trust relationship between iLO and the domain before user sign-on, any form of authentication (including two-factor authentication) is supported. For information about configuring a user account to support two-factor authentication, see the server OS documentation.

For more details on Configuring Kerberos authentication and directory configurations, see Setting up Kerberos authentication and directory services section in the iLO User Guide.

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. Hitachi Vantara 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.

Extended Schema directory authentication

Using the 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 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.

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 Hitachi Vantara Extended Schema configuration.

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.

Depending on the iLO version, scans support several firmware types. 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

NOTE: Check the iLO user guide to verify the firmware types that your iLO version supports.

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.

Default System Recovery Set contents

Firmware	Intel servers	AMD servers	NVIDIA and Ampere servers
System ROM (BIOS)	X	X	X
iLO firmware	X	X	X
System Programmable Logic Device (CPLD)	X	X	X ¹
Innovation Engine (IE) ²	X		

Table Continued

Firmware	Intel servers	AMD servers	NVIDIA and Ampere servers
Server Platform Services (SPS) Firmware ³	X		
Server Platform Services-IE Full Recovery Image ²	X		
Server Platform Services Full Recovery Image ⁴	X		

¹ Primary System Programmable Logic Device (CPLD) and Secondary System Programmable Logic Device (CPLD)

² G4 only

³ G4, G5 only

⁴ G5 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. If data corruption is detected, iLO tries to restore the configuration information from the backup file. Automatic restore operations are recorded in the IML.

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.

When iLO security is disabled with the system maintenance switch (iLO 5 and iLO 6 only), the SRAM data is not restored automatically.

Manual backup and restore

iLO supports manually restoring the configuration information.

Hitachi Vantara 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. Hitachi Vantara recommends performing a backup each time that you update the iLO firmware.

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 a higher mode.

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. For information about how to implement a solution, see the iLO user guide for your platform.

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.

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, Hitachi Vantara recommends leaving the IPMI over LAN interface disabled.

A Security Bulletin for this issue is available at the [Hitachi Vantara website](#).

Hitachi Vantara recommends the iLO RESTful API as a replacement for the IPMI over LAN capabilities.

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

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.

IPMI 1.5 GetChannelAuth Response Information Disclosure

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

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. Hitachi Vantara recommends changing the default username.

If you are not actively using IPMI, Hitachi Vantara recommends disabling the interface.

Weak cryptographic key

On servers with iLO 5 and iLO 6, 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.

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.

Hitachi Vantara 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`.

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.

More information

[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.

For information about the options you can configure, see the user guide for your platform.

⚠ 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 G4 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 (iLO 5 and iLO 6 only)

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 (iLO 5 and iLO 6 only)

Enable or disable data section non-execution protection.

Microsoft Secured-core Support (iLO 7)

Configure the server for Microsoft Secured-core Support. When enabled, various virtualization and security settings are automatically enabled.

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***](#).

SR storage controllers

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

CBE

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

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.

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 Smart Array SR Secure Encryption LTU, and a supported key management application.

MR storage controllers

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 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 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.

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)
- 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 Hitachi Vantara and Thales.

Advanced key management with iLO 7

Advanced Key Management in iLO 7 protects local keys by providing a secure repository for keys, certificates, and other server security assets. This feature is an improvement over using the TPM to encrypt local keys, because the keys are not stored in an exposed location.

Server lifecycle decommission or repurpose

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

⚠ CAUTION: Use the OBSE feature only when a system is being decommissioned. More importantly, proceed with extreme caution as using the OBSE feature will result in all accessible storage drives and volumes being securely erased.

Similarly, use the System Erase and Reset feature only when a system is being decommissioned. Also proceed with extreme caution as using the System Erase and Reset feature will result in all internal and external storage drives and volumes accessible to the system being erased.

One-button secure erase

If you want to decommission a server, you can use the One-button secure erase (OBSE) feature.

OBSE 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**.

OBSE 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.

You can initiate the OBSE process from the following products:

- iLO—For details about the effects of using this feature, see the **iLO user guide** for your platform.
- Intelligent Provisioning—For more information, see the **Intelligent Provisioning user guide**.

⚠ CAUTION: Use the OBSE feature with extreme caution as such use will result in all accessible storage drives and volumes being securely erased.

If you perform OBSE through Intelligent Provisioning v3.89 or earlier (G4 or v4.32 or earlier (G5), there is no pop-up or any other type of warning displayed in the application.

Prior to implementing the OBSE, it is critical to follow the instructions in **Preserving data on drives or storage volumes that you do not want to erase**. Failure to follow these instructions will result in all accessible storage-attached devices exposed to the server being securely erased. Hitachi Vantara will not be responsible for any loss arising from storage-attached devices being erased by using the OBSE feature.

OBSE will securely erase any accessible storage-attached devices exposed to the server, including without limitation, storage disks, or volumes.

Examples of such accessible storage volumes are the ones presented from an external SAN storage array or device.

Preserving data on drives or storage volumes that you do not want to erase

To preserve the data on drives or storage volumes that you do not want to erase:

- For rack systems, remove the physical cables, remove the server from the SAN zoning, or remove the server from the storage presentation prior to such use.

One-button secure erase for DevIDs and System IAK

iLO IDevID, LDevID, System IDevID, and System IAK certificates are removed during the OBSE process.

When you use the OBSE process, Hitachi Vantara 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.

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 Storage controllers?

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?

One-button secure erase does not erase these items.

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

NOTE: 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. Use other methods to delete the data or securely dispose of the devices according to your organization security policies.

Device	Operation requested	Result
NVRAM ¹	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 ²	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.
TPM	TPM Clear + Clear NV indices + Delete Platform Symmetric key	All data in TPM is cleared including any nonvolatile information.
Smart Array SR controllers ^{3, 4}	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive	<ul style="list-style-type: none"> The security reset function removes the drive keys that are stored on the key manager for
Compute SR Controllers ⁵	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.	<ul style="list-style-type: none"> 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 the following sections for operations requested on the drives.

Table Continued

Device	Operation requested	Result
Compute MR Controllers ^{6, 7}	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	<ul style="list-style-type: none"> 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 the following sections for operations requested on the drives.
NS204i Boot Controllers ⁸	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	<ul style="list-style-type: none"> 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 the following sections for operations requested on the drives.
Smart Array S100i and SR100i Software RAID ²	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 described in the following sections.
SATA HDD ⁹	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.
SATA SSD ⁹	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 ^{6, 10}	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.

Table Continued

Device	Operation requested	Result
	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 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 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 process 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)	All data and metadata associated with all namespaces is destroyed. All user content present in the NVM subsystem is erased.
	A single pass of NVM Express FORMAT with SES = 1. This option is used if the drive does not support the SANITIZE.	

¹ Applies to iLO 5 and iLO 6

² Applies to iLO 5

³ G4

⁴ For the Smart Array E208e-p SR G4 controller installed in a G5 or later server, OBSE is not supported for sanitizing drives

(D3000 enclosure only) and factory resetting the controller. As an alternate to using one-button secure erase, you can use the Redfish

⁵ `#Storage.ResetToDefaults` and `#Drive.SecureErase` actions.
G5 and later

⁶ MR controllers do not support one-button secure erase on G4 servers.

⁷ MR controllers support one-button secure erase only for drives that support Crypto Erase (CRYPTO SCRAMBLE EXT for SATA, CRYPTOGRAPHIC ERASE for SAS, and Crypto Erase for NVMe). One-button secure erase for self-encrypting drives (SED) is not supported.

⁸ One-button secure erase for self-encrypting drives (SED) is not supported on NS204i controllers.

⁹ These drives might be connected to SR controllers and MR controllers or the Chipset SATA controller. ¹⁰

MR controllers support only CRYPTOGRAPHIC ERASE.

System Erase and Reset

The System Erase and Reset action is initiated from Intelligent Provisioning or the ROM-based setup utility (RBSU). It clears hard drives and Intelligent Provisioning preferences.

This feature securely erases all data on all accessible storage disks or volumes 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.



CAUTION: Use the System Erase and Reset feature with extreme caution as such use will result in all internal and external storage drives and volumes accessible to the system being erased.

If you use the System Erase and Reset feature through Intelligent Provisioning v3.89 or earlier (G4) or v4.32 or earlier (G5), there is no pop-up or any other type of warning displayed in the application.

Prior to implementing the System Erase and Reset, it is critical to follow the instructions in **Preserving data on drives or storage volumes that you do not want to erase**. Failure to follow these instructions will result in all accessible storage-attached devices exposed to the server being erased. Hitachi Vantara will not be responsible for any loss arising from storage-attached devices being erased by using the System Erase and Reset feature.

System Erase and Reset will securely erase any accessible storage disk or volume, including without limitation, FCOE, iSCSI, SAN, NVMe, SAN-attached, and direct-attached storage.

Examples of such accessible storage volumes are the ones presented from a SAN storage frame. O

For more information, see the Hitachi Advanced Server HA800 G6 Series Intelligent Provisioning User Guide.

Preserving data on drives or storage volumes that you do not want to erase To preserve the data on drives or storage volumes that you do not want to erase:

- For rack systems that support Intelligent Provisioning with external storage, remove the physical cables, remove the server from the SAN zoning, or remove the server from the storage presentation prior to such use.

Third-party security solutions

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.

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 G4 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.

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.

Pensando Distributed Services Platform

The Pensando Distributed Services Platform (DSP) for supported Hitachi Vantara 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.

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.

Password guidelines

Hitachi Vantara 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).
- The minimum length for a user account password can be configured in iLO. Depending on the configured **Minimum Password Length**, the password can have a minimum of zero characters (no password) and a maximum of 39 characters. Hitachi Vantara recommends configuring a **Minimum Password Length** of eight or more characters, which is the default value.



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.

Recommended security settings for iLO

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

Recommended security settings

Feature or function	Setting	Recommended value
TPM or TM status	Trusted Platform Module	Read only
	Module Type	Read only (displayed only when a TPM or TM is present)
Local user account controls	Add, edit, and delete local users	Up to 12 local accounts, with a range of individual user privilege settings to support the security principle of least access.
Directory group account controls	Add, edit, and delete directory groups	Up to 6 directory groups, to be used with Kerberos authentication or schema-free directory integration.
iLO server 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.
iLO account service settings	Authentication Failures Before Delay	1 failure causes no delay
	Authentication Failure Delay Time	10 seconds
	Authentication Failure Logging	Enabled-Every Failure
	Minimum Password Length	8
	Password Complexity	Enabled
iLO network settings	Anonymous Data	Enabled
	IPMI/DCMI over LAN	Disabled (includes port setting)
	Remote Console	Enabled (includes port setting)
	Secure Shell (SSH)	Enabled (includes port setting)
	SNMP	Disabled
	Virtual Media	Enabled (includes port setting)
	Virtual Serial Port Log	Enabled

Table Continued

Feature or function	Setting	Recommended value
	Web Server ¹	Enabled (must set non-SSL and SSL ports) ²
iLO settings	Idle Connection Timeout (minutes)	30 minutes
	iLO Functionality	Enabled
	iLO RIBCL Interface ¹	Enabled (Hitachi Vantara recommends using the iLO RESTful API.)
	iLO ROM-Based Setup Utility	Enabled
	iLO Web Interface	Enabled
	Remote Console Thumbnail	Disabled
	Require Host Authentication ¹	Enabled
	Require Login for iLO RBSU	Enabled
	Serial command line interface status	Enabled-Authentication Required (must set interface speed)
	Show iLO IP during POST	Enabled
	Show Server Health on External Monitor	Enabled
	VGA Port Detect Override	Enabled
	Virtual NIC	Enabled
iLO Service Port	iLO Service Port	Enabled
	USB flash drives	Disabled
	Require authentication	Enabled
	USB Ethernet adapters	Disabled
Secure shell key settings	Keys must be 2048-bit DSA or RSA (or ECDSA 384-bit keys in CNSA security state) ¹	Using SSH keys provides better security than simple password authorization.
	Keys must be 2048-bit RSA (or ECDSA 384-bit keys in CNSA security state) ³	

Table Continued

Feature or function	Setting	Recommended value
Certificate mappings ¹	Each local user account must have an associated certificate.	Using a smart card with certificates provides better security than simple password authentication.
Smartcards	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 certificate administration	Customize Certificate	Install a trusted SSL certificate for each iLO. Default self-signed certificates are not secure.
Directory-based authentication	LDAP Directory Authentication	Select Extended Schema (requires Active Directory) or use the Directory Default Schema. This feature requires some configuration steps outside of iLO.
	Local User Accounts	Depending on environment, enabled or disabled.
	Kerberos Authentication	Enabled (Also must set Realm, Server Address, Server Port, and Keytab file). This feature requires some configuration steps outside of iLO.
Encryption	Security State	High Security (minimum) ¹
		Secure Standard Mode ³
SSO	SSO Trust Mode	Trust by Certificate (Can select SSO privileges per user role)
Login security banner	Enable Login Security Banner	Enabled (must set a security message)
Firmware verification	Scan Settings	Enable Background Scan (must set the Integrity Failure Action)

¹ iLO 5 and iLO 6

² If disabled, access is removed for RIBCL, iLO RESTful API, remote console, iLO Federation, and the iLO web interface.

³ iLO 7

UEFI System Utilities security setting recommendations

Hitachi Vantara 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. 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

iLO 7 Configuration Utility

- **iLO 7 Functionality**—Enabled
- **iLO 7 Configuration Utility**—Enabled
- **Require Login for iLO 7 Configuration**—Enabled
- **Show iLO 7 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

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com

Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com

