Hewlett Packard
Enterprise

HPE Edgeline Integrated System Manager User Guide

Abstract

This guide provides information about configuring, updating, and operating an HPE Edgeline EL300 Converged Edge System by using the iSM web interface. This document is intended for system administrators, Hewlett Packard Enterprise representatives, and Hewlett Packard Enterprise Authorized Channel Partners who are involved in configuring and using HPE Edgeline EL300 Converged Edge Systems.

Part Number: P12833-002
Published: August 2020
Edition: 1

Notices

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

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

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

Acknowledgments

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks 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.

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

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

UNIX® is a registered trademark of The Open Group.

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

Contents

Part 1: The Integrated System Manager web interface

About the HPE Integrated System Manager and this guide

The HPE Edgeline EL300 Converged Edge System is a compact modular device that provides an effective way to connect and manage various operational systems such as control systems, data acquisitions system, and industrial networks. It supports remote management over both wireless and wired networks.

HPE Edgeline Integrated System Manager (iSM) is a remote management tool embedded in the HPE Edgeline EL300 Converged Edge System. iSM allows system administrators to remotely configure, update, and monitor system health and activity. The embedded iSM management module has its own network connection and IP address to which administrators connect on their dedicated management network, even when the system is powered down. Depending on hardware configuration, Edgeline systems with iSM can be connected to a management network using Ethernet or a wireless Wi-Fi, 3G, 4G, or LTE connection. iSM offers a Web-based console (iSM GUI), a command line interface (iSM CLI), and is accessible using the REST API.

This guide is separated into two parts. Part 1 explains the web interface for iSM. Part 2 explains the available commands for the iSM command line (CLI). Throughout Part 1, you can find links to the related commands in Part 2 for equivalent operations.

HPE Edgeline EL300 Converged Edge System security features

Hewlett Packard Enterprise (HPE) is committed to constantly improving its security stance to meet challenges such as attacks on firmware by continually improving the hardware and firmware security of its server platforms and related hardware environments-ensuring that every link in the chain of security provides the most effective cyber security protections possible.

HPE Edgeline EL300 Converged Edge System offers the following security features:

- Hardware root of trust
- Secure firmware updating
- Secure erase
- Chassis and external connector disable
- Chassis Intrusion Detection
- Audit logs

Hardware root of trust

A root of trust, sometimes referred to as a hardware (or silicon) root of trust, provides a series of trusted handshakes from low level firmware up to BIOS and software, to ensure a known good state. The iSM root of trust consists of individual keys for the HPE EL300 to keep malicious software from executing. The HPE EL300 host board has standard factory secure keys that can be enabled, or the user can add even more security by customizing the keys.

The HPE EL300 chipset provides an unprecedented level of hardware security with its root of trust. The root of trust is based in the silicon chip hardware itself, and is virtually impossible to alter. By using this approach, firmware can be authenticated as far back as the supply chain. Additionally, the hardware root of trust makes an ideal environment for secure boot.

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

Secure erase

The HPE EL300 GUI and BIOS interfaces both support secure erase, which provides a method to secure data on a server you want to decommission or redeploy. The secure erase method follows NIST Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization*.

For more information about the specification, see **https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf**. Section 2.5 of the specification describes the level of sanitization. The appendix recommends minimum sanitization levels for media.

Secure erase purges user data and returns the server and supported components to the default state, and automates many of the tasks described in the *Statement of Volatility* document for a server.

To use this feature, the SATA M.2 media storage drives attached to the HPE EL300 must support a native sanitize method. This also enables the data on the host board to be erased by using the iSM GUI or even from the BIOS.

Examples of the low level commands executed using secure erase include the SANITIZE command for SATA and SAS drives and FORMAT for NVM Express drives (NVM Express drives are not currently supported by the HPE EL300). The NIST publication recommends these commands for purging data on these device types. Using these commands is more secure than using software to overwrite data on storage drives.

Secure erase capabilities

When using secure erase, be aware of the following:

- You must have admin access to perform a secure erase.
- Secure erase cannot purge USB devices or internal SD cards.
- Unsupported HDD or SSD storage media cannot be purged using secure erase. Unsupported devices are skipped during the process.
- Secure erase cannot remove serial numbers or product ID.
- All battery backed memory is overwritten.
- Securely erased SATA M.2 drives have their user data internal encryption keys changed, making user data irretrievable. All physical memory blocks including those that are not user accessible, become irretrievable - including any previous data in caches.

More information

Using Secure Erase

System disablement

If a chassis is to be decommissioned, a user can disable the system. Disabling the system halts all functionality of the HPE EL300. The host reboots into BIOS to perform a secure erase, disables the power button, shuts down the host, and will not let the host power on. All access to the iSM is suspended until the recovery password is entered to revive the system. A password is generated as part of the disable process.

⚠ **WARNING:** Using the iSM **Disable System** function renders the host system unusable. A disabled system host will not power on and will not respond on any programming interfaces. It is not possible to load a recovery image onto a disabled system. All internal hard disks are securely erased when the system is disabled. While the iSM will retain power, only an authorized repair person can recover a disabled system.

- Hewlett Packard Enterprise recommends that all critical data is backed up prior to disabling.
- Reactivating a disabled system requires a unique recovery password that is generated as part of the disable process.
    - Keep the password in a safe place.
    - HPE does not store the recovery password and a lost password may require a system replacement.
    - HPE does not cover this event under standard warranty and support server.

The iSM **Disable System** function is useful for administrators that discover system tampering and want to make the system unusable immediately.

Hardware disablement

The HPE EL300 supports specific hardware disablement through the GUI or CLI for additional physical security. The following external connectors, buttons, and ports can be disabled:

- SD card port
- Host reset button
- Power button

- iSM reset button
- USB ports 1-4

More information

Configuring hardware buttons and ports

Hardware port and button disablement

Secure firmware updates and protection from malicious firmware

Only firmware signed by HPE is accepted for installation. No unsigned or corrupted firmware can be installed in the Edgeline EL300. All firmware must be signed and approved through the root of trust.

Because only authorized users can log in to the system, and only users with iSM Admin privilege can update the firmware, only valid signed images from HPE can be installed in the system.

More information

Updating firmware

Chassis intrusion detection

The Edgeline EL300 is equipped with chassis intrusion detection switches that detect the following:

- Top cover removal
- Bottom cover removal
- Top cover replacement
- Bottom cover replacement

An event is recorded in the Event Log for each of the above, even if the power is off. These events are also added to the Audit Log, and can be read by HPE Support even if the Event Log is cleared.

More information

Event Logs

Audit Log

Integrated System Manager maintains an Audit Log that is inaccessible to normal users, even user with Admin privilege. All configuration changes to the system are logged by time and username to both the Event Log and the Audit Log. In case the Event Log is cleared, the Audit Log is always available to HPE support for auditing.

More information

Event Logs

Setting up iSM

Connecting to HPE iSM the first time

Once the system is unboxed, connected to your management network, and powered up, there are a few options for accessing iSM the first time. You can initially configure iSM by:

- Connecting to the iSM web interface using the WiFI access point (WiFi AP).
- Connecting to the iSM web interface through the management network.
- Connecting to the iSM CLI using a DB9 null modem serial cable and retrieving the DHCP assigned IP address.

Connecting to the web interface using the WiFi Access Point

HPE recommends this method for initial configuration.

Prerequisites

- System hardware unboxed and powered up, and WiFi antenna connected
- System hardware unboxed, installed, and powered up
- Username and password noted from the chassis tag
- WiFi-enabled laptop or mobile device

Procedure

1. Search for available WiFi connections on your device.

   The WiFi SSID starts with **iSM**, followed by a dash, and up to 12 letters and numbers. The letters and numbers are the Chassis Serial Number that is on the chassis tag. For example, **iSM-813d2g5144fd**.

2. Select the iSM WiFi connection.
3. Open a browser window to `192.168.37.1` to access the iSM login page. Log in with the credentials printed on the chassis tag.

   NOTE: If this is the first time logging into the system, you are required to change the password.

Connecting to the web interface using Ethernet

When your setup devices are not WiFi-enabled, acquire the IP address or hostname through your management network.

Prerequisites

- System hardware unboxed and powered up
- Username and password noted from the chassis tag
- Ethernet cable
- DHCP enabled network

Procedure

1. Connect an Ethernet cable between the MGMT port on the system chassis and your management network.
2. Wait for the hostname of your new system to propagate onto your network through DDNS and have an IP address assigned through DHCP.
3. On a separate computer connected to your network, enter the address **`https://<iSM hostname or IP address>`** in a browser window. HTTPS (HTTP exchanged over an SSL encrypted session) is required for accessing the iSM web interface.

   To use the hostname, enter the fully qualified domain name (if your computer is outside the domain) or just the hostname (if your computer is inside the domain).
4. Log in with the default credentials listed on the system chassis tag.

Connecting to the CLI in a serial session

If ICMP ping or other tools are disabled on your management network, retrieve the IP address in a serial session.

Prerequisites

- System hardware unboxed and powered up
- Username and password noted from the chassis tag
- Null modem serial cable with connectors or adapters suitable for your environment
- DHCP enabled management network

Procedure

1. Connect a null modem serial cable to the serial port on the system. Connect the other end to the system you are using to configure.

   NOTE: If your system was shipped with an HPE Edgeline Dual Serial Port daughter card, do not use serial daughter ports for initial configuration of the system.
2. Use a standard tool like PuTTY to start a serial terminal session on the system you are using to configure. Use the following settings:

Specification	Value
Serial Line	Appropriate for the system you are using to connect
Baud rate	115200
Data bits	8
Parity	None
Stop bit	1
Flow control	XON/XOFF

3. Log in by entering the default credentials shown on the chassis tag at the prompt.
4. To see the network details, enter the `show network` command.

Prepare for configuration

Prepare to configure your new system by completing the tasks below.

1. **Verify operating system support**

   For information about supported operating systems, see the *Supported Operating Systems for Edgeline, Moonshot, and IoT Gateway Systems* at **http://www.hpe.com/support/edgeline-moonshot-IoT-OS**.

2. **Gather operating system installation media and product key** (Windows, Linux)

   Operating system installation can be performed using a network share (PXE boot), USB, SD card, or virtual media. Be sure to have installation keys for operating systems that require them, and read any implementation notices that accompany the OS. For portable media, the drive must have enough space to store a complete OS image, with enough space left over for OS reporting files. HPE recommends that portable media have a minimum of 32GB of space before storing installation images.

   NOTE: An iSM Advanced license is required to use virtual media.

3. **Verify network connectivity**

   Ensure that the network connection is active, if needed.

4. **Verify Internet connectivity**

   Verify Internet access from your business network. Make a note of the gateway IP address, you may need it later.

5. **Plan for the network address**

   If you do not have DHCP enabled on the network, you must have networking details ready: An IP address to assign, subnet mask, gateway address, and DNS name. For initial setup, it is faster to allow automatic assignment of these details by connecting your system to a DHCP enabled network.

Complete the network configuration using Integrated System Manager and install an operating system

Complete the configuration by performing the following tasks.

NOTE: iSM communicates with Remote Console over a private 16.x.x.x subnet. Do not connect the MGMT port, and by extension iSM, to a subnet that has the same address space or network errors will occur.

1. Configure all iSM network connection settings that you intend to use on the **Wired and Wireless Network** pages:

   - Enable and configure the WiFI access point on the **WiFi AP** page. This method of access can only be used for initial setup.
   - Configure a WiFi network connection on the **WiFi** page.
   - Enable and configure cellular access on the **LTE** page.
   - Configure the **Host Name Settings** on the **General** page.
   - Choose and configure LAN addressing on the **IPv4** or **IPv6** pages.

   Click here for detailed instructions about configuring network settings.

2. Update firmware or add files to the repository on the **Firmware** pages. Download firmware updates from the HPE Support Center at **http://www.hpe.com/support/hpesc**.

Click here for detailed instructions about updating the firmware.

3. Store an operating system image on your chosen installation media. You can install an operating system from a USB drive, virtual USB (virtual media), SD card, or PXE.

   NOTE: If you plan to use virtual media, mount the media before starting a remote console session or changing the host boot order. An iSM Advanced license is required to use virtual media and the remote console. For detailed information about the iSM Advanced license, see the *HPE Edgeline IoT and Converged Edge Systems Licensing Guide* at **https://www.hpe.com/support/EL-IoT-Converged-Edge-System-Licensing-en**.

   ⓘ **IMPORTANT:** When using virtual media to install a Windows operating system, Windows may interrupt the installation by asking for a driver. To avoid this, use a boot-ready consolidated image of a bootable USB Windows installation.

4. Update the host boot order in BIOS, iSM GUI, or by using the iSM CLI so that the next reboot of the host system checks your chosen installation media first.

   NOTE: HPE recommends setting the boot order on the iSM GUI **Boot Order** page. Use remote console (iSM Advanced license required) to update the boot order in BIOS, or connect a keyboard, monitor, and mouse directly to the system. To update the boot order using the iSM CLI, open an SSH command-line session to the IP address of iSM.

   Click here for detailed instructions about modifying the boot order.

5. Restart the host system and following the onscreen instructions to install the operating system.

   Click here for detailed instructions about managing the system power.

6. Immediately after installing the OS, unmount the virtual media and then move **SATA** or **NVMe** to the top of boot order (depending on where you installed the OS).

   Click here for detailed instructions about modifying the boot order.

7. Register the product.

More information

Creating a USB bootable image for Windows virtual media installation

Mounting virtual media

Unmounting virtual media

`set` CLI command

`enable` CLI command

`disable` CLI command

`show` CLI command

`update` CLI command

Prepare the system for daily use after installing an operating system

Prepare your new system for service by completing the following tasks after installing an operating system.

- Access iSM from practically anywhere, or access the host operating system using Remote Console (after acquiring a license).

NOTE: To enable Remote Console, Virtual Media, Configuration Lock, and the Disable function, you must have an iSM Advanced license.

- Add authorized user accounts in iSM on the **User Administration** page. Remove the default user ID and password.
- Add SSH keys for each user on the **Security** page.
- Replace the default self-signed certificate and create a trusted SSL certificate for iSM on the **SSL Certificate** page.
- Configure option cards as needed on the **Option Card** page.
- Control the system and chassis power, and view temperatures, from the **Power and Thermal** pages.
- Back up the iSM configuration on the **Backup & Restore** page.
- To decommission the system, use the **Secure Erase** function.
- If you become concerned about system tampering, disable the system on the **Disable** page. An iSM Advanced license is required to disable a system.
- Troubleshoot system issues by viewing the Health and Event logs on the **Logs** page.
- Disable external ports and buttons as needed.
- Set an asset tag.
- Enable the BIOS Configuration Lock.
- Enable HPE Remote Device Access.
- Configure ignition timeouts (if the system is installed in a vehicle.)
- Configure session timeouts.

Registering the product

To experience quicker service and more efficient support, register the product at the **Hewlett Packard Enterprise Product Registration website**.

Registering and redeeming a license key

iSM licensing

iSM standard features are included with every HPE Edgeline EL300 Converged Edge System to simplify system setup and to help monitor health, power, and thermal control.

The iSM Advanced license activates four advanced features of the interface:

- System Lock
- Remote Console
- Virtual Media
- System Disable

For detailed information about licensing, see the *HPE Edgeline IoT and Converged Edge Systems Licensing Guide* at **https://www.hpe.com/support/EL-IoT-Converged-Edge-System-Licensing-en**.

More information

Installing an iSM license

Installing a license using REST API

Why register your iSM Advanced license?

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

Creating a USB bootable image for Windows virtual media installation

Create a consolidated image file clone of a bootable USB Windows installation using Windows or Linux.

Prerequisites

- An USB drive with at least 8GB of available space.
- An image on the USB of Windows 2016 or Windows 10 created using manufacturer instructions.
- At least 8GB of available space on a local HDD.
- If using Windows to clone the bootable USB drive, you must have Cygwin, a Linux runtime environment, installed.

Procedure

1. Create a bootable USB drive by following the instructions for the operating system to be installed:
   - Windows 2016: Create a bootable USB drive using the instructions here: **https://docs.microsoft.com/en-us/windows-server-essentials/install/create-a-bootable-usb-flash-drive**
   - Windows 10: Create a bootable USB drive using the tool here: **https://www.microsoft.com/en-us/software-download/windows10**
   - Obtain an image for either OS from MSDN and use Rufus to create the USB drive: **https://rufus.ie**
2. (Windows method) Clone the bootable USB drive using Windows:
   a. Insert the USB drive with the image created in step 1.
   b. Run Cygwin Terminal as Administrator.
   c. In Cygwin Terminal, enter: **`cat /proc/partitions`**
   Example output (sd**b** is the disk letter for our 8GB USB Drive, notice the E:\ and F:\ windows mounts under it):

```
major minor  #blocks  name   win-mounts

    8     0 488386584 sda
    8     1    562176 sda1
    8     2 487822336 sda2   C:\
8    16   7554758 sdb
8    17   7552660 sdb1   E:\
8    18       512 sdb2   F:\
```

d. Enter the following command, where *disk_letter* is the letter from the previous step. The `of` argument is to name the output image, such as `windows.img`.

```
dd if=/dev/sddisk_letter of=name.img bs=1M
```

For example:

```
dd if=/dev/sdb of=windows.img bs=1M
```

3. (Linux method) Clone the bootable USB drive using Linux:

a. Insert the USB drive with the image created in step 1.

b. Enter: **`cat /proc/partitions`**
Example output (sd**b** is the disk letter for our 8GB USB Drive):

```
$ cat /proc/partitions
major minor  #blocks  name

 259        0  500107608 nvme0n1
 259        1     460800 nvme0n1p1
 259        2     102400 nvme0n1p2
 259        3      16384 nvme0n1p3
 259        4  499526656 nvme0n1p4
   8        0  494927872 sda
   8        1     524288 sda1
   8        2  477721600 sda2
   8        3   16679936 sda3
   8       16    7554758 sdb
   8       17    7552660 sdb1
   8       18        512 sdb2
```

c. Enter the following command, where *disk_letter* is the letter from the previous step. The `of` argument is to name the output image, such as `windows.img`.

```
sudo dd if=/dev/sddisk_letter of=name.img bs=1M
```

For example:

```
sudo dd if=/dev/sdb of=windows.img bs=1M
```

4. Place the image file on an HTTP server and then mount it as virtual media (vusb) in iSM.

Using the iSM web interface

The iSM web interface

Use the iSM web interface to manage your Edgeline EL300. You can also use the iSM CLI.

Browser requirements

The iSM web interface requires a browser that meets the following requirements:

- **JavaScript**—The iSM web interface uses client-side JavaScript extensively.

  This setting is not enabled by default in all versions of Internet Explorer. To check or change this setting, see **Enabling JavaScript for Internet Explorer**.
- **Cookies**—Cookies must be enabled for certain features to function correctly.
- **Pop-up windows**—Pop-up windows must be enabled for certain features to function correctly. Verify that pop-up blockers are disabled.
- **TLS**—To access the iSM web interface, you must enable TLS 1.0 or later in your browser.

Supported browsers

iSM supports the following browsers:

- Microsoft Edge version 80 or later
- Mozilla Firefox (latest version)

  NOTE: Due to a limitation in link local IPv6 handling in Firefox, you cannot use Firefox when accessing iSM using IPv6 on SUSE Linux Enterprise Server 15 SP0.
- Google Chrome desktop version 79.0.3945.79 (Official Build) (64-bit) or later
- Apple Safari desktop (latest version)
- Microsoft Internet Explorer 11

  NOTE: If you encounter errors when using Internet Explorer 11, be sure to download and install this update from Microsoft:

  https://support.microsoft.com/en-us/help/4537767/cumulative-security-update-for-internet-explorer

Enabling JavaScript for Internet Explorer

Some versions of Internet Explorer have JavaScript disabled by default. Use the following procedure to enable JavaScript.

Procedure

1. Start Internet Explorer.
2. Select **Tools** > **Internet options**.
3. Click **Security**.

4. Click **Custom level**.

5. In the **Scripting** section, set **Active scripting** to **Enable**.

6. Click **OK**.

7. Refresh your browser window.

Logging in to the iSM web interface

Procedure

1. Enter `https://<iSM host name or IP address>.`

   When you access the iSM web interface, use HTTPS (HTTP exchanged over an SSL encrypted session).

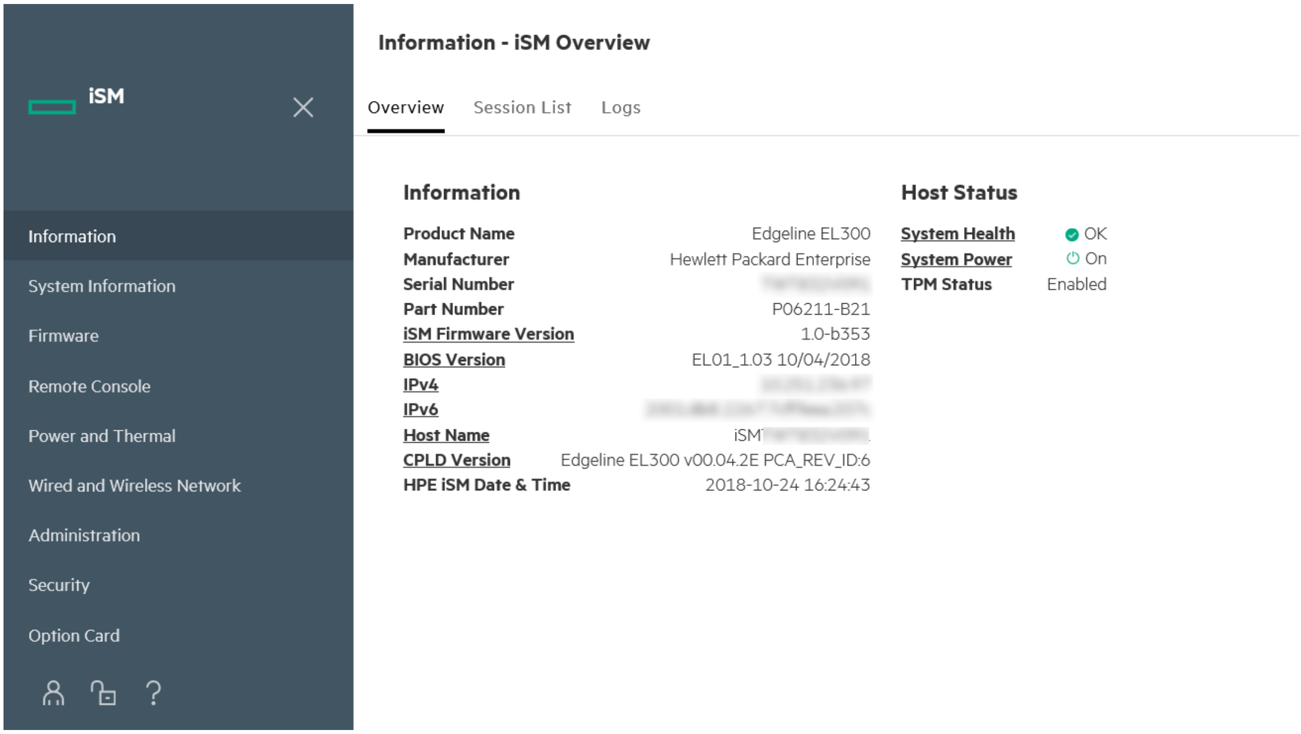
   The iSM login page displays. If a login security banner is configured, the banner text is displayed above the username and password fields.

2. Enter a local account **Username** and **Password**.

   Enter the default username and password shown on the chassis tag when logging in for the first time.

iSM web interface overview

The iSM web interface groups similar tasks for easy navigation and workflow. The interface is organized with a navigation tree in the left page. To use the web interface, click an item in the navigation tree, and then click the name of the tab you want to view.



Information - iSM Overview

Information

Product Name	Edgeline EL300
Manufacturer	Hewlett Packard Enterprise
Serial Number	[redacted]
Part Number	P06211-B21
iSM Firmware Version	1.0-b353
BIOS Version	EL01_1.03 10/04/2018
IPv4	[redacted]
IPv6	[redacted]
Host Name	iSM[redacted]
CPLD Version	Edgeline EL300 v00.04.2E PCA_REV_ID:6
HPE iSM Date & Time	2018-10-24 16:24:43

Host Status

System Health	✓ OK
System Power	On
TPM Status	Enabled

About the iSM web interface controls

The left pane of the iSM web interface can be hidden from view at any time. Hiding the left pane gives more space for the main pages to be displayed, but hides the navigation tree.

- To hide the left pane, click **X** or click ▬.
- To show the left pane, click ▬.

Logout, lock, and help

There are three icons shown at the bottom of the left pane when the pane is open:

- 👤—This icon shows the currently logged-in username and a **Logout** option. Clicking **Logout** closes your web interface session and returns to the login screen.
- 🔓—This icon locks iSM and prevents configuration changes in the web interface and CLI. Clicking the icon opens a confirmation dialog. Click **Lock System** or **No, Go Back**. You are asked to verify your choice a second time.

  ⓘ **IMPORTANT:** A license that supports this feature must be installed.

- ?—This icon displays the online help for the iSM web interface.

Confirmation, status, and error messages

Some pages of the iSM web interface require you to scroll down to see all the options available, or to reach an **Apply** button. Confirmation, status and error messages display at the top of the page, so remember to scroll back up to the top of the page after clicking **Apply**.

Viewing iSM information and logs

Viewing iSM overview information

The iSM Overview page displays high-level details about the system and the iSM subsystem as well as links to commonly used features.

Procedure

Click **Information** in the navigation tree.

System information details

- **Product Name**—The system model name on which iSM is running.
- **Manufacturer**—The name of the company that made the system.
- **Serial Number**—The system serial number, which is assigned when the system was manufactured.
- **Part Number**—The part number assigned when the system was manufactured.
- **iSM Firmware Version**—The version of installed firmware. To navigate to the **Installed Firmware** page, click the link.
- **BIOS Version**—The version and date of the installed BIOS. To navigate to the **Installed Firmware** page, click the link.
- **IPv4**—The network IP address of the iSM subsystem. To navigate to the **Network Summary** page, click the link.
- **IPv6**—The link-local address of the iSM subsystem (if IPv6 addressing is enabled). To navigate to the **Host Name Settings** page, click the link.
- **Host name**—The name assigned to the iSM subsystem. This value is used for the network name and must be unique. To navigate to the **Installed Firmware** page, click the link.
- **CPLD Version**—The firmware version installed on the Edgeline EL300 complex programmable logic device. To navigate to the **Installed Firmware** page, click the link.
- **HPE iSM Date & Time**—The current date and time according to the system. Set the current date and time using the iSM CLI.

Host Status details

- **System Health**—The system health indicator. This value summarizes the condition of the monitored subsystems. The possible values are **OK**, **Degraded**, and **Critical**. To navigate to the **Health Summary** page, click the **System Health** link.
- **System Power**—The system power state (**ON** or **OFF**).
- **TPM Status**—The status of the TPM or TM socket or module. The possible values are **Enabled**, or **Disabled**.
- **UID Indicator**—Displays whether the external LED on the Edgeline EL300 is lit. Click the icon to change the state of the UID.

Managing iSM sessions

Prerequisites

iSM Admin privilege (when disconnecting sessions other than your own)

Procedure

1. Navigate to the **Information** page, and then click the **Session List** tab.

   The **Session List** page displays information about the active iSM sessions.

2. (Optional) To disconnect one or more sessions, click the check box next to each session you want to disconnect. Then click **Disconnect Session**.

Session list details

iSM displays the following details in the **Current Session** and **Session List** tables:

- **User**—The iSM user account name.
- **IP**—The IP address of the computer used to log in to iSM.
- **Login Time**—The date and time that the iSM session started.
- **Access Time**—The date and time that the current user was last active in the session. This entry is updated whenever the user is active in the session.
- **Expires**—The date and time that the session will end automatically. The expiration is updated whenever the user is active in the session. All sessions expire after 30 minutes of inactivity.
- **Source**—The method of access used by each session to connect to iSM.

Event Logs

The event log provides a record of significant events recorded by the iSM firmware.

Logged events include major system events such as a system power outage or a system reset. Other logged events can include:

- Successful or unsuccessful browser and Integrated Remote Console logins
- Virtual power and power-cycle events
- Log clearance
- Configuration changes such as creating or deleting a user

More information

`show` CLI command

Health Logs

iSM monitors and records changes in the system hardware and system configuration. The Health Log provides:

- Continuous health monitoring of system parameters
- Consolidated health and service alerts with precise time stamps

More information

`show` CLI command

Viewing logs

Procedure

1. Click **Information** in the navigation tree, and then click the **Logs** tab.
2. Select the type of logs from the menu (Health Logs or Event Logs).

   The selected logs appear.
3. (Optional) To filter and customize the log view, enter text in the search box.

   As you enter terms in the search field, the matching logs are displayed.
4. (Optional) To sort by the contents of a column, click a column heading.

   An arrow in the column heading indicates whether the column is sorted in ascending or descending order.

More information

`show` CLI command

iSM log details

- **ID**—The event ID number. Events are numbered in the order in which they are generated.

  By default, the event log is sorted by the ID, with the most recent event at the top.
- **Severity**—The importance of the detected event.
- **Description**—The description identifies the component and detailed characteristics of the recorded event.
- **Last Update**—The date and time when the event occurred. This value is based on the date and time stored by the iSM firmware.

Event log icons

- ❖ **Critical**—The event indicates a service loss or imminent service loss. Immediate attention is needed.
- ⚠ **Caution**—The event is significant but does not indicate performance degradation.
- ⓘ **Informational**—The event provides background information.

Downloading iSM logs

iSM logs can be downloaded in CSV format for external reference.

Procedure

1. Click **Information** in the navigation tree, and then click the **Logs** tab.
2. Select the type of logs the menu (Health Logs or Event Logs).

   The selected logs appear.
3. (Optional) To filter and customize the log view, enter text in the search field.

   As you enter terms in the search field, the matching logs are displayed.
4. Click the CSV icon: CSV

   The browser downloads the file according to your browser settings and the options you choose. If you filter the records before downloading, only the filtered events are included.

Deleting iSM logs

Prerequisites

Admin privileges

Procedure

1. Click **Information** in the navigation tree, and then click the **Logs** tab.
2. Select the type of logs from the menu (Health Logs or Event Logs).

   The selected logs appear.
3. (Optional) To filter and customize the log view, enter text in the search field.

   As you enter terms in the search field, the matching logs are displayed.
4. Click the delete icon: 🗑

   The system displays a confirmation message.
5. Click **OK**.

   iSM deletes all entries from the current log type.

   NOTE: The delete function deletes all entries in the current log type, regardless of the optional search box filtering.

More information

`clear` CLI command

Viewing general system information

Viewing health summary information

The **Summary** tab displays the status of monitored subsystems and devices. Depending on the system configuration, the information on this page varies.

If the system is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the system is powered on and POST is complete.

Procedure

1. Click **System Information** in the navigation tree.
2. Optional: To sort by a table column, click the column heading.

   To change the sort order to ascending or descending, click the column heading again or click the arrow icon to the right of the column heading.

Subsystem and device status

Summarized status information is displayed for the following:

- **BIOS and Hardware Health**
- **Host Communications**
- **Power Supply**
- **Temperatures**

Subsystem and device status values

The **Health Summary** page uses the following status values:

- ✓ **OK**—The device or subsystem is working correctly.
- ⓘ **Not Available**—The component is not available or not installed.
- ⚠ **Degraded**—The device or subsystem is operating at a reduced capacity.
- ✖ **Failed**—One or more components of the device or subsystem are nonoperational.
- ⓘ **Other**—For more information, navigate to the appropriate page of the component that is reporting this status.
- ? **Unknown**—The iSM firmware has not received data about the device status. If iSM was reset when the system was powered off, some subsystems display the status **Unknown** because the status cannot be updated when the system is powered off.
- − **Not Installed**—The subsystem or device is not installed.

Viewing processor information

The **Processor** information page displays the type of processor installed and a summary of the processor subsystem.

If the system is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the system is powered on and POST is complete.

Procedure

Click **System Information** in the navigation tree, and then click the **Processor** tab.

Processor details

The following information is displayed for each processor:

- **Processor Name**—The name of the processor.
- **Processor Speed**—The current speed of the processor.
- **Execution Technology**—The number of cores and threads in use.
- **Internal L1 cache**—The L1 cache size.
- **Internal L2 cache**—The L2 cache size.
- **Internal L3 cache**—The L3 cache size.

Viewing memory information

If the system is powered off, the information on this page is current as of the last power off. Memory information is updated only when the system is powered on and POST is complete.

Procedure

1. Click **System Information** in the navigation tree, and then click the **Memory** tab.
2. Optional: To sort by a table column, click the column heading.

   To change the sort order to ascending or descending, click the column heading again or click the arrow icon to the right of the column heading.

Memory information details

The **Memory Details** section shows the installed physical memory modules on the host.

Memory Location

The slot or processor on which the memory module is installed. See the hardware setup guide for memory slot locations.

Size

The size of the memory module, in GB.

Current Frequency

The currently measured memory module speed, in MHz.

Part number

The manufacturer memory module part number.

Viewing network information

If the system is powered off, the information on this page is current as of the last power off. Network adapter information is updated only when the system is powered on and POST is complete.

The information on this page is updated when you log in to iSM. To refresh the data, log out of iSM, and then log back in.

Procedure

Click **System Information** in the navigation tree, and then click the **Network** tab.

Physical Network Adapters

This section shows the details of the physical network adapters in the system. All available NIC and associated MAC addresses are shown.

Physical Network Adapter details

The MAC addresses relate to the ports as follows:

- **MAC 0**—MAC address for the management port.
- **MAC 1**—MAC address for NIC1.
- **MAC 2**—MAC address for NIC2.

Viewing the device inventory

The **Device Inventory** page displays information about devices installed in the system. Some examples of the devices listed on this page include installed PCI devices, and attached USB devices.

If the system is powered off, the information on this page is current as of the last power on. Inventory information is updated only when the system is powered on and POST is complete.

Procedure

Click **System Information** in the navigation tree, and then click the **Device Inventory** tab.

Device Inventory details

The page displays the following details in each device section:

- **Device Name**—The product device name.
- **Device ID**—The hex value identifier for the device.
- **Vendor ID**—The device vendor's primary part number in hex.

Viewing and managing firmware

Viewing installed firmware information

Procedure

Click **Firmware** in the navigation tree.

The **Firmware** page displays firmware information for various components.

If the system is powered off, the information on this page is current as of the last power off. Firmware information is updated only when the system is powered on and POST is complete.

Firmware types

The firmware types listed on the **Firmware** page vary based on the system configuration.

For most configurations, the system BIOS, CPLD, and iSM firmware and base image are listed. Other possible options include TPM, HPE remote device access, and option card.

Firmware details

The Firmware page displays the following information for each listed firmware type:

- **Firmware name**—The category name of the firmware.
- **Firmware version**—The currently installed version number of the firmware.

Updating firmware

While firmware can be updated using components uploaded to the iSM Repository, you can also update firmware directly.

NOTE: Updates to firmware can be performed in this manner for the CPLD, iSM, and BIOS. However, base image updates, which replace the iSM web and CLI interfaces entirely with newer versions, must be performed out of band using the host operating system. Additionally, updates can be required to be installed in a specific order. See the *HPE Edgeline EL300 Converged Edge System Release Notes* before updating firmware to check whether there is a specific order requirement.

Prerequisites

iSM Admin privilege

Procedure

1. Click **Firmware** in the navigation tree, and then click **Update Firmware** in the right pane.
2. Select the **Local file** or **Remote file** option.
3. Depending on the option you selected, do one of the following:

a. In the **File** box, click **Browse** (Internet Explorer or Firefox) or **Choose File** (Edge or Chrome), and then specify the location of the firmware component.

b. In the **URL** box, enter the URL for a firmware component on an accessible web server.

4. Click **Flash**.

   The firmware update status will be visible in the event log.

Updating the base image with Windows using a bootable USB drive

⚠ **WARNING:** Base image updates replace both the iSM web interface and the CLI interface with updated versions. No previously entered data is retained. After a base image update is complete all previously configured settings, including usernames and passwords, must be re-entered. Accessing the system after a base image update will require the original factory set username and password.

Prerequisites

- A USB drive with at least 2GB of available space
- At least 2GB of available space on a local HDD
- Downloaded the base image update file: `EL300-base-image-3.0.2-1.4b22.iso` from the HPE Support Center
- (Optional) Downloaded the sig file: `EL300-base-image-3.0.2-1.4b22.iso.sig` to verify the ISO
- Downloaded a freeware bootable USB creation application - these instructions use the latest version of Rufus, found at **https://rufus.ie**
- An available keyboard, monitor, and mouse ready to attach to the EL300
- BIOS Configuration lock disabled
- External USB ports enabled
- Secure Boot disabled

Procedure

Create a bootable USB drive from the ISO

1. Attach the USB drive to a Windows computer.
2. Run the Rufus utility.
3. Click the **Select** button, navigate to the ISO base image file, and then click **Open**.

   The ISO filename appears in the **Boot selection** box.
4. Leave the **Persistent partition size** at 0 (No persistence).
5. Under **Partition scheme**, select **GPT** (since the EL300 host BIOS is UEFI). The **Target system** selection will automatically change to **UEFI (non CSM)**.

   Leave the **Format Options** selections as default. Rufus is now ready to create the bootable USB from the ISO.
6. Click **Start**.
7. A message may appear that Rufus detected the ISO as a hybrid image. Select **Write in ISO image mode (Recommended)** and then click **OK**.

8. The **Status** bar shows the progress of the USB creation. Wait until it is finished.

Adjust the EL300 BIOS to boot from USB and then reboot to finish the installation

9. Connect a monitor, mouse and keyboard to the EL300 to see the host operating system.

   Base image upgrades require no involvement from the iSM web interface.

10. Insert the USB drive into the EL300, and then power on (or reboot) the host operating system.

11. Press **F9** at the appropriate time during boot to start the BIOS setup.

   NOTE: Make sure that secure boot is disabled. Secure boot is on the Security tab of the BIOS setup.

12. Use the arrow keys to navigate to the **Boot** tab.

13. Use the arrow keys to select **Boot Option #1** and then press **Enter**.

   A list of available boot devices displays.

14. Use the arrow keys to select the USB drive.

15. Press F4 to save and exit the BIOS setup.

   The system reboots from the USB drive and installs the base image update. The process is automated and can take up to 10 minutes to complete. You may notice that the process pauses while showing the `Sending 'rootfs' (1110016 KB)`. This is normal. When the base image update is complete, the system will show a completion message.

16. **Remove the USB drive** and then reboot the system.

Accessing the system after a base image update

17. Log into the CLI.

   - Username: **`iot`**
   - Password: **`password`**

18. Change the username and password as required.

19. Enter three commands:

   a. Enter the command **`set factorydefaults`**

      This restores the hostname to the default, and sets the credentials to those shown on the chassis tag.

   b. Enter the command **`set ssl default_cert`**.

      This sets the default hostname in the self signed certificate.

   c. Enter the command **`kvm init`**.

20. Upon the first subsequent login, which will require the credentials from the chassis tag, change the password as required.

   NOTE: If you were using Secure Boot before starting this procedure, be sure to re-enable it. Additionally, remember to reset the boot order to the original settings.

The base image has now been updated and is ready for reconfiguration.

Updating the base image using Linux

⚠ **WARNING:** Base image updates replace both the iSM web interface and the CLI interface with updated versions. No previously entered data is retained. After a base image update is complete all previously configured settings, including usernames and passwords, must be re-entered. Accessing the system after a base image update will require the original factory set username and password.

Prerequisites

- Downloaded the Linux base image upgrade smart component file `CP044951.scexe` from the HPE Support Center, stored on a USB drive or available at an accessible network location
- A keyboard, monitor, and mouse attached to the EL300 (Base image upgraded require no involvement from the iSM web interface.
- An available keyboard, monitor, and mouse ready to attach to the EL300
- BIOS Configuration lock disabled
- External USB ports enabled
- Secure Boot disabled

Procedure

1. Copy the `CP044951.scexe` to the host OS.
2. Open a command window, and navigate to the directory in which the update file is stored.
3. Enter `CP044951.scexe` and then press **Enter**. **This command must be run with root privileges.**

   The update process starts. Follow any prompts.

Accessing the system after a base image update

4. Log into the iSM CLI.
   - Username: **`iot`**
   - Password: **`password`**
5. Change the username and password as required.
6. Enter three commands:
   a. Enter the command **`set factorydefaults`**

      This restores the hostname to the default, and sets the credentials to those shown on the chassis tag.

   b. Enter the command **`set ssl default_cert`**.

      This sets the default hostname in the self signed certificate.

   c. Enter the command **`kvm init`**.
7. Upon the first subsequent login, which will require the credentials from the chassis tag, change the password as required.

NOTE: If you were using Secure Boot before starting this procedure, be sure to re-enable it. Additionally, remember to reset the boot order to the original settings.

iSM Repository

The iSM Repository is a secure storage area in the nonvolatile flash memory embedded on the system board. Store firmware updates here to be applied to the system.

Viewing iSM Repository summary and component details

Procedure

Click **Firmware** in the navigation tree, and then click the **Repository** tab.

iSM Repository details

The summary section of the **iSM Repository** page displays the following details about the repository storage use:

- **Capacity**—Total repository storage capacity
- **In use**—Total repository storage in use
- **Free space**—Total unused repository storage capacity
- **Components**—Number of saved components in the repository

iSM Repository contents

The **Contents** section of the **iSM Repository** page displays the following details about each firmware or software component:

- **Name**—The name of the saved component.
- **Version**—The version of the saved component, if applicable.
- 📦 (Install component icon)—Click to install component firmware from the repository.
- 🗑(Delete icon)—Click to remove the file from the repository.

Adding components to the iSM Repository

Prerequisites

Admin privilege

Procedure

1. Click **Firmware** in the navigation tree, and then click **Upload to Repository** in the right pane.
2. Select the **Local file** or **Remote file** option.
3. Depending on the option you selected, do one of the following:
    a. In the **File** box, click **Browse** (Internet Explorer or Firefox) or **Choose File** (Edge or Chrome), and then specify the location of the firmware component.
    b. In the **URL** box, enter the URL for a firmware component on an accessible web server.
4. Click **Upload**.

The file is uploaded to the repository and displayed in the repository contents list.

More information

`add` CLI command

Installing a component from the iSM Repository

You can install new firmware from the iSM Repository page.

Prerequisites

Admin privilege

Procedure

1. Click **Firmware** in the navigation tree, and then click **Repository**.
2. Click the install component icon 📦 next to the component you want to install.
3. Click **Yes, install now**.

   The update begins immediately.

More information

`update` CLI command

Removing a component from the iSM Repository

Prerequisites

iSM Admin privilege

Procedure

1. Click **Firmware** in the navigation tree, and then click the **iSM Repository** tab.
2. Click the remove component icon 🗑.

   iSM prompts you to confirm the request.
3. Click **yes, remove**.

More information

`remove` CLI command

Remove all components from the Repository

Prerequisites

iSM Admin privilege

Procedure

1. Click **Firmware** in the navigation tree, and then click the **Repository** tab.
2. Click **Remove All**.

The system prompts you to confirm the request.

3. Click **yes, remove all**.

   The components are removed.

More information

`remove` CLI command

Viewing and configuring installed iSM daughter cards

This page displays the installed option cards in the system, and enables the configuration for each card.

Procedure

1. Click **Option Cards** in the navigation tree.
   The **Daughter Cards** page displays.
2. Modify the settings of the installed cards as needed.
3. When finished, click **Apply**.

Using the Integrated Remote Console

Launching an Integrated Remote Console session

The iSM **Integrated Remote Console** can be used to remotely access the graphical display, keyboard, and mouse of the host system. The Integrated Remote Console provides access to the remote file system and network drives.

With Integrated Remote Console access, you can observe POST messages as the system starts, and initiate ROM-based setup activities to configure the system hardware. When you install an operating system remotely, the Integrated Remote Console enables you to view and control the host system and monitor the installation process.

Prerequisites

A license that supports this feature is installed.

Procedure

1. Click **Remote Console** in the navigation tree.

   The **Launch** tab displays the Integrated Remote Console **Launch** button.

2. Click **Launch**.

   The Integrated Remote Console session starts in a new browser window or tab.

3. Click **Connect** at the top left of the Integrated Remote Console window.
4. (Optional) Click **Mount** to open the Virtual Media tab.

Integrated Remote Console usage information and tips

- The Integrated Remote Console is suitable for high-latency (modem) connections.
- Do not run the Integrated Remote Console from the host operating system on the system that contains the iSM processor.
- Hewlett Packard Enterprise recommends that users who log in to a system through the Integrated Remote Console logout before closing the console.
- Only one Remote Console session can be in progress at a time. If another user is currently connected to remote console, click **Disconnect Session** to close the connection.
- When you finish using the Integrated Remote Console, close the window or click the browser **Close** button (X) to exit.
- When the mouse is positioned over the Integrated Remote Console window, the console captures all keystrokes, regardless of whether the console window has focus.
- Avoid using reserved keys, such as the Windows key, in Integrated Remote Console sessions. The response to the Windows key in IRC sessions can be unpredictable.

Integrated remote console and low-power OS modes

Many operating systems offer low-power modes (also known as sleep modes). For example, Microsoft Windows offers both sleep and hibernate modes, depending on hardware capability and configuration.

The integrated remote console may not always resume correctly when attempting to resume operations from the following modes:

- State S3—Sleep, or suspend to RAM
- State S4—Hibernate, or suspend to disk
- State S5—Soft off (some devices remain powered by standby voltage)

When resuming from one of these low-power states, the integrated remote console may not be able to resume a session that was open before setting the OS to the low-power state. If this happens, close the IRC session. Wait for the host operating system to fully resume, and then open a new IRC session to the host OS.

Mounting virtual media

The **Virtual Media** page allows you to mount virtual images and drives.

Prerequisites

A license that supports this feature is installed.

Procedure

1. Click **Remote Console** in the navigation tree, and then click the **Virtual Media** tab.
2. Do one of the following:
    a. Select **Remote file**, and then in the **URL** box, enter the URL for a virtual USB file on an accessible server.
    b. Select **Repository file** and then select a virtual USB image from the **File from Repo** list.

       The image must have been previously loaded to the iSM Repository.
3. Click **Mount**.

   The virtual media is now available to the Integrated Remote Console session.

More information

`set` CLI command

Unmounting virtual media

Procedure

1. Click **Remote Console** in the navigation tree, and then click the **Virtual Media** tab.
2. Click **Unmount**.

   The virtual media is no longer available to the Integrated Remote Console session.

More information

`set` CLI command

Using power and thermal features

Managing the system power

The **Virtual Power Button** section on the **System Power** page displays the current system power state, as well as options for remotely controlling system power. **System Power** indicates the state of the system power when the page is first opened. Use the browser refresh feature to view the current system power state. The system is rarely in the **Reset** state.

Procedure

1. Click **Power and Thermal** in the navigation tree.

   The page opens with the **System Power** tab selected.

2. Click a button to change the power state. The available buttons change according to the current power state.
3. When prompted to confirm the request, click **OK**.

More information

`set` CLI command

`show` CLI command

Supported system power status types

The **System Power** status displayed on this tab can include multiple power modes, depending on the support offered by the installed operating system. The buttons and actions displayed on this tab change depending on the power mode.

System Power: (S-status)	Buttons displayed and affect when clicked
System Power: Off (S5)	**Power On**—Equivalent to pressing the physical power button to turn the system on.
System Power: On (S0)	**Push Power Button**—Equivalent to pressing the physical power button. The result of this action depends on the configuration of the host's operating system.
	Force Power Off—Equivalent to holding down the host power button to turn the host off.
	Force System Reset—Forces the server to warm-boot: CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system.
System Power: Sleep/Suspend (S3)	**Wake**—Equivalent to pressing the physical power button to wake the host.
	Force Power Off—Equivalent to holding down the host power button to turn the host off.
System Power: Hibernate (S4)	**Power On**—Equivalent to pressing the physical power button to turn the system on.
	Full Shutdown—Equivalent to holding down the power button to completely shut down the host. Clicking this moves the host to state S5.

Virtual Power Button labels

Each button available during the different supported power modes (determined by operating system support) is labeled. These labels refer to an equivalent physical button activity typically included on a computer system.

- **Momentary Press**—Clicking this button type is equivalent to momentarily pressing the physical power button.

  Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event, or to wake from a low-power mode.

- **Press and Hold**—Clicking this button type is equivalent to pressing the physical power button for 5 seconds and then releasing it.

  This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently depending on a short press or long press.

- **Reset**—Clicking this button type is equivalent to clicking a physical reset button. This can force the server to warm-boot, and CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system. If possible, be sure to manually shut down the operating system using OS controls before clicking this button type.

Temperature information

The **Temperature** page includes a table that displays the sensor name/location, status, reading, and threshold settings of temperature sensors in the system chassis.

If the system is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the system is powered on and POST is complete.

Viewing temperature sensor data

Procedure

1. Click **Power & Thermal** in the navigation tree, and then click the **Temperatures** tab.
2. (Optional) When temperatures are displayed in Celsius, click **°F** to change the display to Fahrenheit. When temperatures are displayed in Fahrenheit, click the **°C** switch to change the display to Celsius.

Temperature sensor details

- **Sensor**—The ID of the temperature sensor, which also gives an indication of the sensor location.
- **Status**—The temperature status.
- **Temperature**—The temperature recorded by the temperature sensor.

  NOTE: Sensor readings for the host CPU do not report temperatures lower than 0 (zero) degrees C, or 32 degrees F.

- **Threshold**—The temperature thresholds for the warning for overheating conditions. The two threshold values are **Caution** and **Critical**.

Managing chassis power and resetting iSM

Prerequisites

Admin privilege

Procedure

1. Click **Power and Thermal** in the navigation tree, and then click the **Management Power** tab.
2. To reset the chassis power, click **Reset Chassis** and then click **Yes, Reset Now**.

   Resetting the chassis power resets the power on all chassis components, including all power supplies, daughter cards, NICs, storage disks, and the motherboard.
3. To restart the iSM session, click **Reset iSM**, and then click **Yes, Reset Now**.

   Using the Reset option does not make any configuration changes, but ends all active connections to the firmware. If a firmware file upload is in progress, it is terminated. If a firmware flash is in progress, you cannot reset until the process is finished. Wait a few minutes before attempting to log in to a new session.

More information

`reset` CLI command

Configuring network settings

Network Summary

iSM provides multiple options for network connection.

To access the network settings, view or edit the network settings on the following pages:

- **Summary**
- **General**
- **IPv4**
- **IPv6**
- **WiFi**
- **WiFi AP**
- **LTE**
- **Proxy**

Viewing the network configuration summary

Procedure

Click **Wired and Wireless Network** in the navigation tree.

The **Summary** tab is displayed.

Network configuration summary details

- **Name**—The name of the active iSM network interface.
- **Host Name**—The name assigned to the iSM subsystem. By default, the host name is iSM, followed by the system serial number. This value is used for the network name and must be unique.

  NOTE: You can configure the iSM host name on the **General** page.
- **MAC Address**—The MAC address of the iSM network interface.
- **Permanent MAC Address**—The unchangeable MAC address of the iSM network interface.
- **FQDN**—The fully qualified domain name of the system.
- **IPv6 Default Gateway**—When IPv6 is enabled, the gateway is the default IP address iSM uses to access the network. When not enabled, this entry is blank.
- **Speed (Mbps)**—The speed of the wired network, measured in megabits per second.

- **WiFi Network**—The SSID of the WiFi network (if connected).
- **Cellular Network**—The broadband wireless provider.

IPv4 Summary details

- **Address**—The IPv4 address currently in use. If the value is `0.0.0.0`, the IPv4 address is not configured.
- **Address Origin**—Indicates whether the address was supplied automatically by DHCP or is static.
- **Gateway**—The gateway address in use for the IPv4 protocol. If the value is `0.0.0.0`, the gateway is not configured.
- **Subnet Mask**—The subnet mask of the IPv4 address currently in use. If the value is `0.0.0.0`, no address is configured.

IPv6 Summary details

- **Address**—The IPv6 address currently in use. If the value is blank, the IPv6 address is not configured.
- **Address State**—Indicates whether the address was supplied automatically or is static.
- **Gateway**—The gateway address in use for the IPv6 protocol. If the value is blank, the gateway is not configured.
- **Prefix Length**—The subnet mask of the IPv6 address currently in use.
- **Link Local Address**—The IPv6 address for the network segment.
- **Link Local Gateway**—The IPv6 address of the local network segment gateway. If the value is blank, the gateway is not configured.
- **Prefix Length**—The subnet mask of the IPv6 link-local address.

IPv6 Address Policy table

A table is displayed that shows whether IPv6 or IPv4 addresses are preferred.

WiFi Summary details

- **SSID**—The service set identifier which provides the name of the wireless network.
- **Strength**—A measure of how powerful the signal strength of the connection is to the WiFi network.
- **Status**—The status of the WiFi connection, connected or not connected.
- **Security**—The type of security in use on the WiFi connection.

LTE Summary details

- **Owner**—Indicates whether LTE is used by the host or by iSM.
- **APN**—The access point name, which may or may not include an operator identifier.
- **Status**—Indicates the state of the connection.

Configuring Host Name Settings

Use the **General** page to configure the **Host Name** and **Domain Name**. The host name and the domain name together constitute the fully qualified domain name.

Prerequisites

iSM Admin privilege

Procedure

1. Click **Wired and Wireless Network** in the navigation tree, and then click the **General** tab.
2. Enter the **Subsystem Name (Host name)**.

   The host name is the DNS name of the iSM subsystem. This name can be used only if DHCP and DNS are configured to connect to the iSM subsystem name instead of the IP address.
3. Enter the **Domain Name** if DHCP is not configured.
4. Click **Apply**.

More information

`set` CLI command

`show` CLI command

Host name and domain name limitations

The **Subsystem Name (Host name)** is initially set at the factory, and is listed on the chassis tag. This default host name is a combination of **iSM** followed by the system serial number.

When reconfiguring the **Host Name Settings**, note the following:

- **Name service limitations**—The subsystem name is used as part of the DNS name.
  - DNS allows alphanumeric characters and hyphens.
  - Always start the hostname with a letter, and not with a number or a hyphen. Any combination of letters, numbers, and the hyphen can be used after the first letter.
  - Name service limitations also apply to the **Domain Name**.
- **Namespace issues**—To avoid these issues:
  - Do not use the underscore character.
  - Limit subsystem names to 15 characters.
  - Verify that you can ping the iSM processor by IP address and by DNS name.
  - Verify that NSLOOKUP resolves the iSM network address correctly and that no namespace conflicts exist.
  - Flush the DNS name if you make any namespace changes.

Configuring IPv4 settings

Prerequisites

iSM

Admin privilege

Procedure

1. Click **Wired and Wireless Network** in the navigation tree, and then click the **IPV4** tab.
2. **Enable** the **IPv4 Configuration** setting.
3. Configure the **DHCPv4 Configuration** setting.
4. Configure the **IPv4 Address Configuration** settings.
5. Configure the **DNS Configuration** settings.
6. To save the changes you made on the **IPv4 Settings** page, click **Apply**.
7. When you are finished configuring the iSM network settings on the **Wired and Wireless Network** tabs, restart the iSM system.

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

More information

`set` CLI command

DHCPv4 Configuration setting

The DHCPv4 setting is enabled by default.

Enable DHCPv4

Enables iSM to obtain an IP address (and other network specific address settings) from a DHCP server.

NOTE: When DHCPv4 is enabled, the **IPv4 Address Configuration** section and **DNS Configuration** section are automatically assigned. When the system is rebooted, these automatic assignments might change.

Static IPv4 Address Configuration settings

IPv4 Address

The iSM IP address. The IP address is supplied automatically when DHCP is enabled. When DHCP is not enabled, enter a static IP address.

IPv4 Subnet Mask

The subnet mask of the IP network. The subnet mask is supplied automatically when DHCP is enabled. When DHCP is not enabled, enter a subnet mask for the network.

IPv4 Gateway

The iSM gateway IP address. The iSM gateway IP address is supplied automatically when DHCP is enabled. When DHCP is not enabled, enter an IP address for the gateway.

IPv4 DNS Configuration settings

Primary DNS Server

This value is supplied automatically when DHCP is enabled. If you are using a static IP address, no name servers are used.

Secondary DNS Server

This value is supplied automatically when DHCP is enabled. If you are using a static IP address, no name servers are used.

Tertiary DNS Server

This value is supplied automatically when DHCP is enabled. If you are using a static IP address, no name servers are used.

Configuring IPv6 settings

Prerequisites

iSM Admin privilege

Procedure

1. Click **Wired and Wireless Network** in the navigation tree.
2. Click the **IPv6** tab.
3. Configure the **Global IPv6 Configuration** setting, and enable IPv6.
4. Configure the **IPv6 Configuration** settings.
5. Configure the **DNS Configuration** settings.
6. To save the changes you made on the **IPv6 Settings** page, click **Apply**.
7. If you are finished configuring the iSM network settings, restart iSM.

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

More information

`set` CLI command

IPv6 Configuration settings

Global IPv6 Configuration

Client Applications use IPv6 first

This option specifies which protocol iSM is tried first when accessing a client application. It is useful when both IPv4 and IPv6 service addresses are configured for iSM client applications. This setting also applies to lists of addresses received from the name resolver when using FQDNs to configure NTP.

- Enable this option if you want iSM to use IPv6 first.
- Disable this option if you want iSM to use IPv4 first.

If communication fails when attempting to use the first protocol, iSM automatically tries the second protocol.

This option is enabled by default.

IPv6 Configuration

Enable IPv6 in Auto Mode

Enable this option to configure iSM to use an IPv6 DHCP server (if found). If no IPv6 DHCP server is available, IPv6 automatically falls back to using SLAAC. This option is enabled by default.

iSM creates its own link-local address even when this option is not enabled.

NOTE: Entering the command `set network6 off` at the Integrated System Manager CLI disables IPv6, and no IPv6 addresses can be used. The link-local address is disabled when IPv6 is disabled.

IPv6 Static Address

When assigning static IPv6 addresses, enter the main IP address here.

IPv6 Static Address Prefix Length

When assigning static IPv6 addresses, enter the prefix length here.

IPv6 Default Gateway

When assigning static IPv6 addresses, enter the default IPv6 gateway here.

DNS Configuration

When assigning static IPv6 addresses, enter the **Primary**, **Secondary**, and **Tertiary DNS Server** addresses.

Configuring WiFi settings

A WiFi connection presents an alternative when a wired connection is not feasible.

Prerequisites

iSM Admin privilege

Procedure

1. Click **Wired and Wireless Network** in the configuration tree, and then click the **WiFi** tab.

   The iSM scans for WiFi signals and displays any SSIDs that are in range. The system will continue to scan until an SSID is found.

2. Click an **SSID**.

   The credentials page displays.

   NOTE: Hewlett Packard Enterprise strongly recommends only connecting to secure networks.

3. Enter the password, and modify other settings as needed.

4. To activate the WiFi connection, select **Enable**.

5. Click **Apply**.

   The iSM connects to the WiFi.

6. Optional: To force a new check for available WiFi networks, click **Scan**.

7. Optional: To manually add a non-broadcasting SSID, click **Add WiFi**.

⚠ **WARNING:**

- **FCC warning:** This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- **Canada warning:** This device complies with Industry Canada licence-exempt RSS standards. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- **French warning:** il est conforme aux normes d'exemption de licence RSS d'Industrie Canada. Son fonctionnement est assujetti aux deux conditions suivantes : 1) Ce dispositif ne doit causer aucune interférence dangereuse, et 2) ce dispositif doit accepter toute interférence reçue, y compris les interférences pouvant provoquer un fonctionnement indésirable.

More information

`set` CLI command

Configuring WiFi Access Point settings

Prerequisites
iSM Admin privilege

Procedure

1. Click **Wired and Wireless Network** in the navigation tree, and then click the **WiFi AP** tab.

   The WiFi Access Point page appears.
2. Use **Enable/Disable** to control the state of the WiFi access point.
3. Enter a **SSID**.
4. Click **Apply**.

NOTE:

- When connecting to the access point, you will be required to enter your iSM credentials. Credentials are case sensitive.
- The use of the WiFi AP is used only for initial configuration of iSM.
- Enabling or disabling the access point may cause iSM network connections to become unresponsive for 10 seconds.

More information

`set` CLI command

Configuring LTE settings

iSM can connect to an LTE network to provide cellular data access to the user interface.

NOTE: When disabling and then re-enabling the APN, there is a delay before the settings are restored and appear on the page. Wait until the settings reappear before continuing.

Procedure

1. Click **Wired and Wireless Network** in the navigation tree, and then click the **LTE** tab.

   The LTE Configuration page appears.

2. To configure iSM, click **iSM**.
3. Enter the **APN** (Access Point Name) to present to the carrier.
4. Click Apply.

   The following information will be automatically be provided after a few seconds:

   - **IMEI** (International Mobile Equipment Identity)
   - **IMSI** (International Mobile Subscriber Identity)
   - **IP**

5. To configure the host, click **Host**.
6. Enter the **APN** (Access Point Name) to present to the carrier.
7. Click Apply.

   The following information will be automatically be provided after a few seconds:

   - **IMEI** (International Mobile Equipment Identity)
   - **IMSI** (International Mobile Subscriber Identity)
   - **IP**

More information

`set` CLI command

Configuring Proxy settings

If you have a proxy on your network, you can configure iSM to use it.

Procedure

1. Click **Wired and Wireless Network** in the navigation tree, and then click the **Proxy** tab.

   The Proxy page appears.

2. Enter the FQDN or IP address of the proxy server in the **Proxy** field.
3. Click **Apply**.

Remote support

Registering your server with HPE Remote Support

Registering your server with HPE provides the ability to quickly identify and resolve issues in an automated, seamless and secure way.

Procedure

1. Click **Remote Support** in the navigation tree, and then click **Registration**.
2. Click **Enable Support**.
3. Enter your HPE Passport user name and password.
4. Select **I accept the terms and conditions**. Click the terms and conditions link to view.
5. To view HPE's privacy policy, click **Privacy Policy**.
6. Click **Register**.

   After clicking **Register**, iSM begins reporting temperature events and hardware failures to HPE support automatically.

Unregistering the server with HPE

Unregistering your server removes the ability to solve issues in an automated manner.

Prerequisites

The server is already registered with HPE Remote Support.

Procedure

1. Click **Remote Support** in the navigation tree, and then click **Registration**.
2. Click **Unregister**.

Sending a test service event

Prerequisites

The server must be registered with HPE Remote Support.

Procedure

1. Click **Remote Support** in the navigation tree, and then click **Service Events**.
2. To verify the remote support configuration, click **Send Test Event**.

   This sends a test event to HPE Remote Support test servers to verify connectivity. You may be advised by HPE support to do this as a troubleshooting step.

   NOTE: All Send Test Event actions are recorded in the event log.

Sending data collection information

Prerequisites

The server must be registered with HPE Remote Support.

Procedure

1. Click **Remote Support** in the navigation tree, and then click **Data Collections**.
2. To send test data collection information to HPE Remote Support, click **Send test data collection**.

   The configuration data for the system is compiled into a single file and sent to HPE Remote Support. You may be advised by HPE Support to send this test data as a troubleshooting step.

Using administration features

iSM user accounts

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

User privileges are set to either User or Administrator level. Any activity that requires modifying or setting a configuration item requires Administrator level privileges.

Adding local user accounts

Prerequisites

iSM Admin privilege

Procedure

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

   The **User Administration** tab is displayed.

2. Click **New**.
3. Enter or select the following details:

   - **User Name**
   - **Role**
   - **Password**
   - **Confirm Password**

4. To save the new user, click **Add User**.

More information

`add` CLI command

Editing local user accounts

Prerequisites

iSM Admin privilege

Procedure

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

   The **User Administration** tab is displayed.

2. Select a user, and then click the edit icon ✎.
3. Update the following details:

- **User Name**
- **Role**

4. To change the password, click **Change Password**, and then complete the Password and Confirm Password fields.
5. To save the changes to the user account, click **Edit User**.

More information

`set` CLI command

Deleting local user accounts

Prerequisites

iSM Admin privilege

Procedure

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

   The **User Administration** tab is displayed.
2. Select the checkbox next to one or more user accounts that you want to delete.

   ⚠ **WARNING:** Always leave at least one administrator-level account.
3. Click **Delete Account(s)**.
4. When prompted, click **Yes, Delete**.
   The system displays a note that the account was deleted.

More information

`remove` CLI command

iSM user account options

- **User Name** appears in the user list on the **User Administration** page. The maximum length for a user name is 39 characters. The **User Name** must use printable characters. Assigning descriptive user names can help you to identify the owner of each login name.
- **Role** identifies the privilege level of the user name, **user** or **admin**.
- **Password** and **Password Confirm** set and confirm the password that is used for logging in to iSM.

Password guidelines

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

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

    - Do not use passwords that are made up of words found in a dictionary.
    - Do not use passwords that contain obvious words, such as the company name, product name, user name, or login name.
    - Change passwords regularly.
    - Keep the iSM default credentials in a safe place.
- Use strong passwords with at least three of the following characteristics:
    - One numeric character
    - One special character
    - One lowercase character
    - One uppercase character
- Specifically, all passwords and user names must conform to the following requirements:
    - All user names can be 1 to 32 characters long. User names:
        - Are not case sensitive
        - Must start with a letter
        - Can include any combination of letters, numbers, underscores (_), and dashes (-)
        - Must be unique (not already entered into the system)
    - All passwords must be a minimum of 8 characters, and a maximum of 64 characters, long. Passwords:
        - Can include any characters of the alphabet
        - Must not include NUL (0), a control sequence such as **Ctrl-c**, or **Enter**.

Boot order

The **System Boot Order** feature enables you to set the system boot device priority.

Changes made to the boot order might require a system reset.

An error occurs if you try to change the system boot order when the system is in POST. You cannot modify the boot order during POST. If this error occurs, wait for POST to finish, and then try again.

Configuring the system boot order

Procedure

1. Click **Administration** in the navigation tree, and then click the **Boot Order** tab.
2. (Optional) Use the controls to add or remove **Devices Supported** to or from the **Boot Order** list.
    a. To add a boot device to the **Boot Order** list, select a boot device in the **Devices Supported** list and then click **Select**.
    b. To remove an item from the **Boot Order** list, select a boot device and then click **Remove**.
3. To move a device up or down in the boot order, select the device in the **Boot Order** list, and then click **Up** or **Down**.
4. Click **Apply**.

    The system confirms that the boot order was updated successfully.

NOTE: Any applied changes to the boot order require two system reboots to become active.

More information

`set` CLI command

iSM Backup and Restore

The **Backup and Restore** feature allows you to restore the iSM configuration on a system with the same hardware configuration as the system that was backed up. This feature is not meant to duplicate a configuration and apply it to a different iSM system.

In general, it is not expected that you will need to perform an iSM restore operation. However, there are cases in which having a backup of the configuration eases and expedites the return to a normal operating environment.

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

You might want to restore the iSM configuration in the following situations:

Battery failure or removal

Various configuration parameters are stored in the battery-powered SRAM. Although rare, the battery can fail. In some situations, battery removal and replacement might be required. To avoid the loss of configuration information, restore the iSM configuration from a backup file after the battery is replaced.

Reset to factory defaults

In some cases, you might need to reset iSM to the factory default settings to erase settings external to iSM. Resetting iSM to the factory default settings erases the iSM configuration. To recover the iSM configuration quickly, restore the configuration from the backup file after the reset to the factory default settings is complete.

Accidental or incorrect configuration change

In some cases, the iSM configuration might be changed incorrectly, causing important settings to be lost. This situation might occur if iSM is set to the factory default settings or user accounts are deleted. To recover the original configuration, restore the configuration from the backup file.

System board replacement

If a system board replacement is required to address a hardware issue, you can use this feature to transfer the iSM configuration from the original system board to the new system board.

Lost license key

If a license key is accidentally replaced, or you reset iSM to the factory default settings, and you are not sure which key to install, you can restore the license key and other configuration settings from a backup file.

Backing up the HPE iSM configuration

Backup files contain only the Chassis Manager configuration settings. No blade configuration settings are saved.

Prerequisites

Admin privilege

Procedure

1. Click **Administration** in the navigation tree, and then click **Backup & Restore**.
2. Click **Backup**.

The system warns that this will save the iSM configuration.

3. Click **Yes, Backup now**.

   The system saves the configuration and displays a message that the backup was successful. Find the saved file in the default output directory for your browser.

Restoring the HPE Edgeline iSM configuration

Prerequisites

Admin privilege

Procedure

1. Click **Administration** in the navigation tree, and then click **Backup & Restore**.
2. Click **Restore**.

   A warning displays that this action restores the backup iSM configuration, overwriting any changes to the settings made since the last backup.

3. Click **Yes, Restore now**.

   The system displays a message that the backup was restored.

Resetting HPE Edgeline iSM to the factory default settings

The Factory defaults feature resets all settings to default, but does not remove the following:

- User accounts and certificates
- Licenses

Prerequisites

Admin privilege

Procedure

1. Click **Administration** in the navigation tree, and then click **Backup and Restore**.
2. Click **Factory defaults**.

   iSM displays a warning message.

3. Click **Yes, Proceed**.

   iSM reboots and closes all sessions, returning you to the login page. It might take several minutes before you can re-establish a connection.

More information

`reset` CLI command

Using Secure Erase

iSM provides secure erase functionality for the system hard drives.

⚠ **WARNING:** Use Secure Erase with extreme caution. This function completely deletes system data. No recovery of data is possible once Secure Erase completes. HPE recommends that all critical data is backed up prior to initiating a Secure Erase.

NOTE: The Secure Erase feature requires support in SSD firmware. If you attempt to perform a Secure Erase, and none of the drives in the system support Secure Erase, iSM returns an error message.

Prerequisites

iSM Admin privilege

Procedure

1. Click **Administration** in the navigation tree, and then click **Secure Erase**.
2. Click **Secure Erase**.

   The **Authenticate before Secure Erase** page displays.
3. Enter an administrator-level **User Name** and **Password**.
4. Click **Authenticate**.

   The system displays a message asking whether you are sure you want to Secure Erase the system.
5. Click **Yes, Secure Erase**.

   The system verifies by asking whether you want to stop the Secure Erase process and go back.
6. Click **No, Secure Erase now**.

   The system displays a message that the operation successfully started.

More information

`set` CLI command

Using the iSM Disable function

⚠ **WARNING:** Using the iSM **Disable System** function renders the host system unusable. A disabled system host will not power on and will not respond on any programming interfaces. It is not possible to load a recovery image onto a disabled system. All internal hard disks are securely erased when the system is disabled. While the iSM will retain power, only an authorized repair person can recover a disabled system.

- HPE recommends that all critical data is backed up prior to disabling.
- Reactivating a disabled system requires a unique recovery password that is generated as part of the disable process.
  - Keep the password in a safe place.
  - HPE does not store the recovery password and a lost password may require a system replacement.
  - HPE does not cover this event under standard warranty and support server.

The iSM **Disable System** function is useful for administrators that discover system tampering and want to make the system unusable immediately.

Prerequisites

- An installed license that supports this functionality
- iSM Admin privilege

Procedure

1. Click **Administration** in the navigation tree, and then click the **Disable** tab.
2. Click **Disable System**.

   The **Authenticate before Disable** page displays.
3. Enter an administrator-level **User Name** and **Password**, and then click **Authenticate**.

   The system displays a verification, asking whether you are sure you want to disable the system.
4. Click **Yes, Disable now**.

   The system displays a final verification, asking whether you want to stop the Disable process and go back.
5. Click **No, Disable now**.

   A final warning appears explaining the nature of the disable function, and displays the recovery username and recovery password.

   NOTE: Record the recovery username and recovery password and store it in a safe place.
6. Click **OK**.

   Your iSM session ends immediately and the host system becomes unresponsive.

More information

`disable` CLI command

Viewing iSM installed licenses

iSM 1.4 accepts two types of licenses. The Advanced license enables the Remote Console, Virtual Media, Lock, and Disable features. The WiFi Radio License enables the WiFi radio and is available free to users in countries where WiFi certification is required.

NOTE: Earlier versions of iSM firmware do not display the WiFi Radio License. If the WiFi Radio License Status section is not present, then WiFi is enabled by default.

Procedure

1. Click **Administration** in the navigation tree, and then click **License**.
2. Installed licenses are displayed in the **Advanced License Status** and **WiFi Radio License Status** sections of the page.

   The license details include the start date, the expiration date, and the status of the installed license.

Installing an iSM license

Procedure

1. Click **Administration** in the navigation tree, and then click **License**.
2. Regardless of the type of license to be installed, click **Install License**.
3. Select the **Local file** or **Remote file** option.
4. Depending on the option you selected, do one of the following:
    a. In the **File** box, click **Browse** (Internet Explorer or Firefox) or **Choose File** (Edge or Chrome), and then specify the location of the license file.
    b. In the **URL** box, enter the URL for a license file on an accessible web server.
5. Click **Install**.

   The license is uploaded and installed to the system and displayed in the applicable license status section of the page.

More information

add CLI command

Installing a license using REST API

Prerequisites

- Privileges to configure iSM settings.
- A valid iSM license file stored on the local system or uploaded to a web server.
- The iSM date and time are set correctly.
- Network connectivity to iSM.

Procedure

1. Locate your license activation key.
2. Download a Redfish interface tool such as Postman (**https://www.getpostman.com/**).
3. Enter the license using the JSON Constrained Notation script.

   Sample license JSON script:

```
Add license via remote file:
URI: (POST) https://{{iSM-ip}}/redfish/v1/Managers/1/LicenseService/Actions/LicenseService.InstallLicense
Input data(JSOn format): {"ImageURI": “URL” } [URL= Link to the license file]

Output:
{
    "error": {
        "@Message.ExtendedInfo": [],
        "code": "Base.1.0.0.Success",
        "message": "The operation completed successfully."
    }
}

Add license via local file (Customer will need to install some tool like Postman for using this below step)
URI: (POST) https://{{iSM-ip}}/redfish/v1/Managers/1/LicenseService/InstallLicenseFromPost
Input Data: (form-data) file, value: Browse license file in client computer
```

```
Output:
{
    "error": {
        "@Message.ExtendedInfo": [],
        "code": "Base.1.0.0.Success",
        "message": "The operation completed successfully."
    }
}
```

Hardware port and button disablement

The Device Switches tab enables you to disable or enable certain hardware on the Edgeline EL300. Certain switches, such as the host reset button, iSM rest button, and power button, along with the four USB ports can be enabled or disabled as physical access conditions warrant.

Configuring hardware buttons and ports

Prerequisites

iSM Admin privilege

Procedure

1. Click **Administration** in the navigation tree, and then click **Device Switches**.
2. In the **Switch Configuration** section, select the following:
    a. For the **Serial Port** configuration, click to select whether the serial port is connected to **iSM** or to the **Host**. The default selection is **iSM**.
    b. Select whether to disable the following (default is enabled):
        - **SD Card** (port)
        - **Host Reset Button**
        - **Power Button**
        - **iSM Reset Button**
3. For the **USB Configuration** section, select whether to disable each USB port, **USB1** through **USB4** (default is enabled).
4. Click **Apply**.

Asset Tag

The Asset Tag assists your organization with tracking material. You can set the Asset Tag for the system on this page.

Setting the Asset Tag

Prerequisites

Admin privilege

Procedure

1. Click **Administration** in the navigation tree.
2. Click the **Asset Tag** tab.
3. Click in the **Asset Tag** field and enter an asset tag.
4. Click **Apply**.

   The interface reports that the asset tag was successfully set.

Configuring the BIOS Configuration Lock

Use the BIOS Configuration Lock to control access to the BIOS. You must have BIOS 1.31 or later installed to support this feature.

Procedure

1. Click **Administration** in the navigation tree, and then click **BIOS Configuration Lock**.
2. Enable or disable the **BIOS Configuration Lock** setting.

   - When this setting is **disabled**, access the BIOS by pressing **F9** at the appropriate time during boot.
   - When this setting is **enabled**, access to the BIOS is blocked.

   NOTE: The online help incorrectly states the behavior of this feature.

3. Click **Apply**.

Configuring the Ignition timer

The settings on this tab allow you to configure the time (in minutes) to delay the powering off of the host and system when the vehicle ignition is turned off. When enabled, the host and the system are kept running for the specified amount of time to allow further operation before shut down. These settings are only available if the ignition power board is installed.

Procedure

1. Click **Administration** in the navigation tree, and then click **Ignition**.
2. Set the **Host Power Off Delay** in minutes by entering a number or using the **+** and **-** buttons.
3. Set the **Switch Power Off Delay** in minutes by entering a number or using the **+** and **-** buttons.
4. Select a setting for the **Enable/Disable the timer** control.
5. Click **Apply**.

Ignition and timer delay sequence

When the vehicle is powered off, the following sequence begins:

1. The Switch Power Off Delay timer begins counting down. During this period you can interact with the system as normal.
2. When the Switch Power Off Delay timer ends, the Host Power Off Delay begins counting down and iSM attempts to gracefully power down the host operating system.
3. If the host operating system does not finish shutting down before the Host Power Off Delay timer reaches zero, iSM forces the OS off.
4. iSM powers off the system.

⚠ **WARNING:** If the **Enable/Disable the timer** setting is disabled, the Edgeline EL300 will continue to run, powered by the vehicle's battery, while the vehicle ignition is turned off. This may deplete the vehicle's battery. HPE recommends enabling this setting whenever the Edgeline EL300 is installed in a vehicle and powered through an ignition power board.

HPE Remote Device Access

HPE Remote Device Access (HPE RDA) allows HPE Support access to the system. When HPE RDA is enabled, HPE Support can login into the web interface or the CLI even if the system is behind a firewall. When contacting support, you will need to supply them with the system serial number (displayed on the **Information** > **Overview** page.)

The HPE Remote Device Access feature does not require that the system is registered with HPE Remote Support.

Configuring HPE Remote Device Access

Procedure

1. Click **Administration** in the navigation tree, and then click **HPE Remote Device Access**.
2. Enable or disable the HPE Remote Device Access setting.
3. Click **Apply**.

   A confirmation dialog displays.
4. Click the confirmation button to confirm your setting.

   To cancel, click the **X** at the top right of the message box.

Configuring security

iSM SSH key specifications

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

Supported SSH key formats

- RFC 4716
- OpenSSH key format

The iSM firmware supports the OpenSSH key format.

SSH key considerations

- The supported SSH key formats are supported with the iSM 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 iSM firmware can import SSH keys that have a length of 1,366 bytes or fewer. 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 iSM web interface to enter the public key, you select the user associated with the public key.
- 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 iSM.

Authorizing a new SSH key by using the web interface

Prerequisites

iSM Admin privilege

Procedure

1. Generate a 2,048-bit RSA key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.
2. Create the `key.pub` file.
3. Click **Security** in the navigation tree, and then click the **Secure Shell Key** tab.

   The **Secure Shell Key** page displays the hash of the SSH public key associated with each user account.
4. Select the check box to the left of the user account to which you want to add an SSH key.
5. Click **Authorize New Key**.
6. Copy and paste the public key into the **Public Key Import Data** box.

   Each user account can have only one key assigned.
7. Click **Import Public Key**.

More information

`add` CLI command

Deleting SSH keys

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

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

Prerequisites

iSM admin privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **Secure Shell Key** tab.
2. In the **Authorized SSH Keys** list, select the check box to the left of one or more user accounts.
3. Click **Delete Selected Key**.

More information

`remove` CLI command

iSM SSL certificate administration

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 system public key) with the system name. Only the system itself has the corresponding private key, allowing for authenticated two-way communication between a user and the system.

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, iSM creates a self-signed certificate for use in SSL connections. This certificate enables iSM to work without additional configuration steps. Certificates are included when you use the iSM backup and restore feature.

IMPORTANT: Using a self-signed certificate is less secure than importing a trusted certificate. Hewlett Packard Enterprise recommends importing a trusted certificate to protect the iSM user credentials by creating a Certificate Signing Request (CSR).

The CSR contains a public and private key pair that validates communications between the client browser and iSM. iSM generates a 2048-bit RSA key or a CNSA-compliant key signed using SHA-256. The generated CSR is held in memory until a new CSR is generated, iSM is reset to the factory default settings, or a certificate is imported.

More information

`add` CLI command

Viewing SSL certificate information and customizing a certificate

Procedure

1. Click **Security** in the navigation tree, and then click the **SSL Certificate** tab.
2. (Optional) Click **Customize Certificate** to begin the process of **obtaining and importing a trusted certificate**.

More information

show CLI command

SSL certificate details

- **Issued To**—The entity to which the certificate was issued.

  When you view the iSM self-signed certificate, this value displays information related to the Hewlett Packard Enterprise Houston office.

- **Issued By**—The CA that issued the certificate.

  When you view the iSM self-signed certificate, this value displays information related to the Hewlett Packard Enterprise Houston office.

- **Valid From**—The first date that the certificate is valid.
- **Valid Until**—The date that the certificate expires.
- **Serial Number**—The serial number assigned to the certificate. This value is generated by iSM for the self-signed certificate, and by the CA for a trusted certificate.

Obtaining and importing an SSL certificate

iSM allows you to create a Certificate Signing Request (CSR) that you can send to a Certificate Authority (CA) to obtain a trusted SSL certificate to import into iSM.

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

Prerequisites

iSM Admin privilege

Procedure

1. **Obtain a trusted certificate from a CA**.
2. **Import the trusted certificate to iSM**.

Obtaining a trusted certificate from a CA

Prerequisites

iSM Admin privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **SSL Certificate** tab.
2. Click **Customize Certificate**.
3. On the **SSL Certificate Customization** page, enter the following:
   - **Country (C)**
   - **State (ST)**

- **City or Locality (L)**
- **Organization Name (O)**
- **Organizational Unit (OU)**
- **Common Name (CN)**

4. (Optional) To include iSM IP addresses in the CSR, select the **include Moonshot Chassis Manager 2.0 IP Address(es)** check box.

   NOTE: Many CAs cannot accept this input. Do not select this option if you are not sure that the CA you are using can accept this input.

   When this option is enabled, the iSM IP addresses will be included in the CSR Subject Alternative Name (SAN) extension.

5. Click **Generate CSR**.

   A message notifies you that a CSR is being generated and that the process might take up to 10 minutes.

6. After a few minutes (up to 10), click **Generate CSR** again.

   The CSR is displayed.

7. Select and copy the CSR text.
8. Open a browser window and navigate to a third-party CA.
9. Follow the onscreen instructions and submit the CSR to the CA.

   NOTE: When you submit the CSR to the CA, your environment might require the specification of Subject Alternative Names. If necessary, enter the iSM DNS name.

   The CA generates a certificate. The certificate signing hash is determined by the CA.

10. After you obtain the certificate, make sure that:

    - The CN matches the iSM FQDN. This value is listed as the **iSM Hostname** on the **Overview** page.
    - The certificate is a Base64-encoded X.509 certificate.
    - The first and last lines are included in the certificate.

More information

`set` CLI command

CSR input details

When you create a CSR, enter following:

- **Country (C)**—The two-character country code that identifies the country where the company or organization that owns this iSM subsystem is located. Enter the two-letter abbreviation in capital letters.
- **State (ST)**—The state where the company or organization that owns this iSM subsystem is located.
- **City or Locality (L)**—The city or locality where the company or organization that owns this iSM subsystem is located.
- **Organization Name (O)**—The name of the company or organization that owns this iSM subsystem.
- **Organizational Unit (OU)**—(Optional) The unit within the company or organization that owns this iSM subsystem.

- **Common Name (CN)**—The FQDN of this iSM subsystem.

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

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

- **include Moonshot Chassis Manager 2.0 IP Address(es)**—Select this check box to include the iSM IP addresses in the CSR.

  Changing CSR details requires admin privileges.

  NOTE: Many CAs cannot accept this input. Do not select this option if you are not sure that the CA you are using can accept this input.

Importing a trusted certificate

iSM supports 2,048-bit SSL certificates that are up to 3 KB (including the 1,187 bytes used by the private key).

Prerequisites

iSM Admin privilege

Procedure

1. Click **Security** in the navigation tree, and then click the **SSL Certificate** tab.
2. Click **Customize Certificate**.
3. Click **Import Certificate**.
4. In the **Import Certificate** window, paste the certificate into the text box, and then click **Import**.

   iSM prompts you to confirm the request. An iSM reset is required to complete the process.
5. Click **Yes, apply and reset**.

   iSM imports the certificate and initiates an iSM reset.

More information

`set` CLI command

Configuring the Login Security Banner

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

Prerequisites

iSM Admin privilege

Procedure

1. Click **Security** in the navigation tree, and then click **Login Security Banner**.
2. Enable the **Enable Login Security Banner** setting.

   iSM uses the following default text for the Login Security Banner:

   ```
   This is a private system. It is to be used solely by authorized users
   and may be monitored for all lawful purposes. By accessing this system,
   you are consenting to such monitoring.
   ```

3. (Optional) To customize the security message, enter a custom message in the **Security Message** text box.

   The byte counter above the text box indicates the remaining number of bytes allowed for the message. The maximum is 1,500 bytes.

   Do not add blank spaces or blank lines to the security message. Blank spaces and blank lines contribute to the byte count, and they are not displayed in the security banner on the login page.

   TIP: To restore the default text, click **Use Default Message**.

4. Click **Apply**.

   The security message is displayed at the next login.

Configuring session timeouts

The Set Timeout page enables you to adjust the amount of time (in minutes) that passes without any activity by the user before a session is automatically closed. **Session Timeout** controls HTTP (web) sessions, and **SSH Timeout** controls CLI sessions.

Prerequisites

iSM Admin privilege

Procedure

1. Click **Security** in the navigation tree, and then click **Set Timeout**.
2. Enter the **Session Timeout**.

   The default is 30 minutes.

3. Enter the **SSH Timeout**.

   The default is 120 minutes.

4. Click **Apply**.

   The message `Successfully changed the timeout` displays.

Viewing and configuring installed iSM daughter cards

This page displays the installed option cards in the system, and enables the configuration for each card.

Procedure

1. Click **Option Cards** in the navigation tree.
   The **Daughter Cards** page displays.
2. Modify the settings of the installed cards as needed.
3. When finished, click **Apply**.

HPE Edgeline Dual CAN Port daughter card

This daughter card includes two Controller Area Network bus serial ports, typically used for automotive applications.

Information about the card includes:

- **Model**—The model name of the installed daughter card.
- **Serial Number**—The manufacturer-set identification number of the product.
- **Script Version**—The version of the script that iSM uses to communicate with the daughter card. Scripts are automatically updated when iSM firmware is updated.
- **Termination** setting for **Port1** and **Port2**.

HPE Edgeline Dual CAN Port daughter card details

The following setting is available for each of the two ports:

Termination—Specifies whether the port is **Enabled** or **Disabled**.

HPE Edgeline Dual Serial Port daughter card

This daughter card includes two serial ports that accept selectable serial communication protocols.

Information about the card includes:

- **Model**—The model name of the installed daughter card.
- **Serial Number**—The manufacturer-set identification number of the product.
- **Script Version**—The version of the script that iSM uses to communicate with the daughter card. Scripts are automatically updated when iSM firmware is updated.
- **Mode** and **Termination** settings for **Port1** and **Port 2**.

HPE Edgeline Dual Serial Port daughter card details

The following settings are available for each of the two ports:

- **Mode**—Specifies the port communication protocol or electrical interface:

  - Loopback
  - RS-232
  - RS-485Half
  - RS-485FULL
- **Termination**—Specifies whether the port is **Enabled** or **Disabled**.

HPE Edgeline TSN Card

This Time-Sensitive Networking daughter card accepts network time-keeping protocols to keep synchronized with all other devices on the network that support TSN. The TSN card also supports real-time communication, scheduling, and traffic shaping.

Information about the card includes:

- **Model**—The model name of the installed daughter card.
- **Serial Number**—The manufacturer-set identification number of the product.
- **Script Version**—The version of the script that iSM uses to communicate with the daughter card. Scripts are automatically updated when iSM firmware is updated.

HPE Edgeline TSN Card details

There are no configuration settings for this daughter card.

HPE Edgeline 1x8 DIO Daughter Card

This daughter card includes eight physical single wire port connections. Each port has selectable voltage input thresholds from 1V to 9V.

Information about the card includes:

- **Model**—The model name of the installed daughter card.
- **Serial Number**—The manufacturer-set identification number of the product.
- **Script Version**—The version of the script that iSM uses to communicate with the daughter card. Scripts are automatically updated when iSM firmware is updated.
- **Mode** and **Threshold** settings for **Port1** to **Port8** .

HPE Edgeline 1x8 DIO Daughter Card details

The following settings are available for each of the eight ports:

- **Mode**—Specifies whether the port is for **Input** or **Output**.
- **Threshold**—
  - When **Mode** is set to Input, **Threshold** sets the voltage above which the incoming signal is interpreted as 1. Input under the specified voltage is interpreted as 0.
  - When **Mode** is set to Output, **Threshold** is not applicable.

Part 2: Integrated System Manager CLI reference

Scripting and command line overview

HPE iSM provides multiple ways to configure, update, and operate HPE Edgeline servers remotely. The command line tools provide quick and easy methods to send commands to the firmware and host system.

Connect to the system using a terminal SSH session with a standard tool, like PuTTY.

More information

Connecting to HPE iSM the first time

add CLI command

Syntax

```
add [file | user | sshkey | license]
```

Parameters

The following describes the valid arguments and argument parameters for this command:

file <url>

Adds a file from a web address to the internal repository.

Use the URL format `http://`*`serverlocation`*`/`*`path`*`/`*`filename`*.

Supported files:

- Host BIOS
- Integrated System Manager firmware
- Boot image file

NOTE: Integrated System Manager detects if the file is signed firmware. If the added file is not firmware, it is still added to the repository but cannot be used by the update command.

user <username>

Add a new login username. After entering this command, enter the password, and then re-enter the password to confirm it. The screen does not display any text when you enter the password. To change the password, see the `set` command. Usernames and passwords are case-sensitive.

sshkey <ssh public key>

Add the public key of the client machine for the currently logged in user. You can use `sshkey` instead of the user password.

After typing `add sshkey`, paste the public key to the command prompt and then press **Enter**.

license <filename>

Import a license from a file. You can provide a URL or filename in the repository.

Example input

Adding a remote file:

```
add file http://server/path/filelocation
```

Adding a user:

```
add user <username>
```

Adding an ssh key:

```
add sshkey <ssh public key>
```

Adding a license from a local file:

```
add license <filename>.xml
```

Adding a remote license:

```
add license http://server/folder/<filename>.xml
```

clear CLI command

Syntax

```
clear [log {health | event} | session]
```

Description

Clears the selected item. Administrator privileges required.

Parameters

log {health | event}

- health: Clears the health log file.
- event: Clears the event log file.

session *<index #>*

Clears (closes) the selected session. This can help when the maximum number of 6 Web UI sessions is reached and one needs to be closed manually. Find the index number by entering the *show session active* command.

Example input

Showing the current sessions and then closing the Web UI session:

```
show session active
        Index Username                   IP             Connection
        ----- -------------------------- -------------- ----------
        1     <user>                     <IP address>   Web UI
        2     <user>                     <IP address>   Web UI
        3     <user>                     <IP address>   Web UI
        4     <user>                     <IP address>   Web UI
        5     <user>                     <IP address>   Web UI
        6     <user>                     <IP address>   Web UI
        7     *Administrator             <IP address>   SSH

        * denotes current session
```

```
clear session 4
```

```
clear log health
```

```
clear log event
```

connect CLI command

Syntax

```
connect vsp
```

Description

Starts a Virtual Serial Port (VSP) session with the host. Allows network users to access the serial port on the host remotely.

To exit the VSP session, type **CTRL** + **]** and **CTRL** + **x**.

Parameters

vsp

Launches the VSP session.

Example input

```
connect vsp
```

`disable` CLI command

Syntax

```
disable [bios lock | ignition timer | remotedeviceaccess
    | remotesupport | tether | lock | usb <1-4> | power button | host reset
    | ism reset | sdcard | system | tpm]
```

Description

Disables the selected target.

Parameters

`bios lock`

Disabling the BIOS lock enables the F9 key to enter BIOS setup during boot.

`ignition timer`

Disables the ability to monitor ignition switch setting and power off when the ignition is off.

NOTE: This command is only available on compatible systems.

`host reset`

Turns off the Host Reset button functionality.

`ism reset`

Turns off the iSM Reset button functionality.

`lock`

Turns off the lock that restricts access to configuration changes. This command requires a license key.

`power button`

Turns off power button functionality.

`remotedeviceaccess`

Disables remote device access.

`remotesupport`

Disables the HPE Remote Support.

`sdcard`

Turns off SD card functionality.

`system`

Disables the system permanently. This command requires a license key.

`tether`

Turns off the iSM network connection to the host.

`tpm`

Disables the TPM.

`usb`*`<1-4>`*

Turns off the specified USB port.

Example input

Disabling network connections to the host:

```
disable tether
```

Disabling USB1:

```
disable usb1
```

Disabling the power button:

```
disable power button
```

Disabling the host reset button:

```
disable host reset
```

Disabling the iSM reset button:

```
disable ism reset
```

Disabling the SD Card port:

```
disable sdcard
```

Disabling the system and deleting system data:

```
disable system
```

Disabling the trusted platform module:

```
disable tpm
```

`enable` CLI command

Syntax

```
enable [bios lock | remotesupport |  ignition timer | tether | lock
       | usb <1-4> | power button | host reset | ism reset
       | remotedeviceaccess | sdcard | tpm]
```

Description

Enables the target that you enter.

Parameters

`bios lock`

Enables the BIOS lock. When BIOS lock is enabled, you will not be allowed to enter the configuration screen using F9 at boot. You must be using the latest BIOS to support this feature.

`remotesupport`

Enables the eRS Remote Support.

`ignition timer`

Enables the ability to monitor ignition switch setting and power off when the ignition is off

NOTE: This command is only available on compatible systems.

`tether`

Turns on the iSM network connection to the host. When enabled, a wired connection alias appears available to the host OS, which shares the network access connection that iSM is using.

`lock`

To prevent configuration changes, enable the lock. To change configurations, use the command `disable lock`. This command requires a license key.

`usb`

Turns on the specified USB port.

When you use this command, include the USB port you want to identify, for example `enable usb` *`<1-4>`*.

`power button`

Turns on power button functionality.

`host reset`

Turns on the Host Reset button functionality.

`ism reset`

Turns on the iSM Reset button functionality.

`remotedeviceaccess`

Turns on HPE Remote Device Access, which is disabled by default. Enabling this feature allows HPE service personnel to diagnose issues remotely.

`sdcard`

Turns on SD card functionality.

`tpm`

Enables the TPM.

Example input

Enabling tether:

```
enable tether
```

Enabling the configuration lock:

```
enable lock
```

Enabling the USB1 port:

```
enable usb1
```

Enabling the power button:

```
enable power button
```

Enabling the host reset button:

```
enable host reset
```

Enabling the iSM reset button:

```
enable ism reset
```

Enabling the SD card port:

```
enable sdcard
```

Enabling the TPM:

```
enable tpm
```

exit CLI command

Syntax

```
exit
```

Description

Ends the current login session. If you are using PuTTy, the window closes. If you are using a Linux SSH, the prompt returns to the machine hosting the SSH client.

Example input

```
exit
```

`help` CLI command

Syntax

```
help
```

Description

Open the CLI command help. If you include a command name, it opens the help description for the command.

NOTE: Some commands require parameters to run. If you do not provide parameters, help is displayed for that command. If no parameters are required, the command is executed.

You can also enter a command with a **?** (question mark) to get help for that command. For example:

```
exit ?
```

Options

You can receive help for the following commands:

- `add`
- `backup`
- `clear`
- `connect`
- `disable`
- `enable`
- `exit`
- `kvm`
- `ping`
- `quit`
- `remove`
- `reset`
- `restore`
- `set`
- `show`
- `test`
- `update`

Example input

```
help
help add
help show
```

`kvm` CLI command

Syntax

```
kvm init
```

Description

Initializes the AMT Remote Console with settings that support iSM.

Example input

```
kvm init
```

`ping` CLI command

Syntax

```
ping <ip>
```

Description

Test the network connection with the target.

Parameters

`<ip>`

Provide a network address to test.

Restrictions

- Target must be on the same subnet.
- Target must respond to network pings.

Example input

```
ping 192.168.1.1
```

`ping6` CLI command

Syntax

```
ping6 <ipv6>
```

Description

Test the network connection with an IPv6 target.

Parameters

`<ipv6>`

Provide an IPv6 network address to test.

NOTE: If you are pinging a link local IPv6 address, the system automatically provides the scope value.

Restrictions

- Target must be on the same subnet.
- Target must respond to IPv6 network pings.

Example input

Sending a ping to an IPv6 address:

```
ping6 fe80::af1:eaff:fefb:41
```

`quit` CLI command

Syntax

```
quit
```

Description

Ends the current login session. If you are using PuTTy, the window closes. If you are using a Linux SSH, the prompt returns to the machine hosting the SSH client.

Example input

```
quit
```

`recover` CLI command

Syntax

```
recover [bios | mac]
```

Description

Forces a flash of the BIOS firmware.

Parameters

`bios`

The `recover bios` command is provided for situations where the `update` command does not work. For example, you can use the `recover bios` command if you accidentally replace the BIOS firmware with the wrong version. Note that you should use the `update` command to update the BIOS firmware when possible.

`mac`

Enter this command to read the MAC address from the host board and modify the hardware MAC, so that the values match, particularly in cases of hardware replacement. The values must match to enable the integrated remote console feature of the iSM web interface.

Example input

To force the bios recovery:

```
recover bios
```

To change the MAC:

```
recover mac
```

remove CLI command

Syntax

```
remove [file | user | sshkey | wifi certs]
```

Description

Deletes the selected target.

Parameters

`file <filename>`

Deletes the selected file from the repository.

`user <username>`

Deletes a user account from the system. Usernames are case-sensitive.

`sshkey <ssh public key index>`

Removes the selected SSH key for the current user.

NOTE: If you are removing multiple SSH keys, refresh the list after removing each SSH key. To refresh the list, use the command `show sshkey`.

`wifi certs <certificate_filename>`

Removes the selected WiFi certificate from the certificate repository.

Example input

```
remove file <filename>

remove user <username>

remove sshkey <ssh public key>

remove wifi certs <certificate_filename>
```

`reset` CLI command

Syntax

```
reset [ism | auxpower]
```

Description

Resets the selected device.

Parameters

`ism`

Resets the iSM. The reset disconnects all open SSH or serial login sessions. After the iSM reboots, you can log in to start a new session. Reboot takes approximately 30 seconds.

`auxpower`

Resets both the iSM and the host by cycling the auxiliary power. The reset disconnects all SSH or serial login sessions. You can log in to a new session after the iSM finishes the reboot. Reboot takes approximately 30 seconds.

Example input

```
reset ism
```

```
reset auxpower
```

set CLI command

Syntax

```
set [ap | asset | autopoweron | boot devices | boot details | boot once
    | date | dc | domain | factorydefaults | hostname | ignition | lte
    | nameservers | network | network6 | password | permissions | power
    | proxy | secureerase | serial | ssl | timeout | tpm | uid | username
    | vusb | wifi]
```

Description

Sets the attribute for the target you provide.

Parameters

`ap [on | off]`

Creates an open WiFi access point so you can configure the system. The network SSID is `SSID_<macaddress>`.

NOTE: Turn off the access point when not in use.

`asset <item_name>`

Sets the identifier for the system. For example, "Office machine".

`autopoweron [on | off]`

- `on`: Powers up the host when the system is powered on.
- `off`: The host stays powered down when the system powers on.

`boot devices [nvme| pxe | sata | sdcard | uefi | usb | vusb]`

Sets the boot order of device types.

`boot details [device_type] <primary_device>`

Sets the primary boot device for a given device type. This is only useful for device types that have multiple options, such as PXE, SATA, and USB.

`boot once [nvme| pxe | sata | sdcard | uefi | usb | vusb | bios]`

Sets the boot device for the next boot only. You cannot specify which device port to use, so for devices with multiple entries (like pxe1, pxe2, etc.) make sure to have only the desired boot device active. Use the BIOS argument to go to the BIOS on the next boot. Enter **`show boot once`** to see the boot once status.

`date <date> <time>`

Sets the management date and time in UTC format.

- `date` format: YYYY-MM-DD.
- `time` format: HH:MM:SS, where hours use 24-hour format.

`dc <params>`

Sets the parameters for the daughter card. Parameters differ based on the daughter card. To view valid parameters, use the `show` command. For example, `show dc config`.

`domain <domain_name>`

Sets the domain name.

`factorydefaults`

Resets the system to factory defaults.

NOTE: All settings are returned to defaults except user accounts and certificates. However, you must change your initial password to log in. After entering this command, iSM reboots and your session will lose connection. It may take several minutes before you can re-establish a connection.

`hostname <name>`

Assigns the DNS hostname of the iSM.

`ignition [hostpoweroff <minutes> | switchpoweroff <minutes>]`

- `hostpoweroff <minutes>`: Sets the timeout for host to power off until iSM forces a power off.
- `switchpoweroff <minutes>`: Sets the delay from when the ignition switch is turned off until the Edgeline EL300 turns off. This allows the customer time to use the system before it goes to an off state.

  NOTE: This command is only available on compatible systems.

`lte [apn <apn_setting> | host | ism ]`

- `apn <apn_setting>`: Configures the LTE connection for the access point name. Contact your cellular carrier for the LTE APN details.
- `host`: Sets the Edgeline EL300 LTE card to be used by the host.
- `ism`: Sets the LTE card to be used by iSM.

NOTE: Edgeline EL300 You can set either the `host` or `ism`, not both.

`nameservers`

Provide a list of IPv4 or IPv6 addresses to act as the name servers to translate URLs into an IP address. If you are using a static IP address, no name servers are used.

`network [off | dhcp | <ip_address> <netmask> <gateway>]`

Sets information for the IPv4 network.

- `off`: Turns off the network.
- `dhcp`: Creates a network with a DHCP connection.
- `<ip_address> <netmask> <gateway>`: Sets a static IP address. Include the address, netmask, and gateway.

`network6 [off | auto | ip_<address> <netmask> <gateway>]`

Sets information for the IPv6 network.

- `off`: Turns off the network.
- `auto`: Creates a network with a DHCP connection.
- `<ip_address> <netmask> <gateway>`: Sets a static IP address. Include the address, netmask, and gateway.

`password`

Changes the password for the logged in user. You are prompted for the new password, and for password confirmation. Passwords must include a minimum of eight characters.

NOTE: Admins can set the password for other users. Provide the *<username>* for the account you want to set. Usernames are case-sensitive.

`permissions [admin | user] <username>`

Sets the permissions for the user.

NOTE: Only admins can change this setting.

`power [on | forceoff | pushbutton | reset]`

Controls power to the host.

- `on`: Powers on the system.
- `forceoff`: Turns off power immediately.

  NOTE: The `forceoff` command might cause a loss of information.
- `pushbutton`: Simulates a short button press. Depending on how the host operating system is configured, this can result in a power down, sleep, hibernate, or it can be ignored.
- `reset`: Forces an immediate reset of the host.

  NOTE: The `reset` command might cause a loss of information.

`proxy [<web proxy> | none]`

Sets the proxy for all network access.

`secureerase`

Sets the secure erase flag in the host BIOS. The next time the host boots, it erases all drives.

`serial [host | ism]`

- `host`: Accesses the host.
- `ism`: Accesses the iSM.

`ssl [csr | default_cert | import_cert | key]`

- `csr`: Generates a Certificate Signing Request (CSR) that you can copy and paste into a file that you send to a signing authority.
- `default_cert`: Resets the default SSL certificate.

  For example:

  ```
  set ssl csr ->enter -> provide info
  Country (2-character code): US
  State/Province: New York
  City: New York City
  Organization: Vandelay Industries
  ```

```
Organizational Unit: Latex Products
Hostname [steven-artik.americas.hpqcorp.net]:
Use IP Address (yes/no)? [no]:
```

- `import_cert`: Imports an SSL certificate from a Certificate Signing Authority (CSA).
- `key`: Allows you to regenerate an SSL key. This command creates an SSL key and generates a matching self-signed certificate.

timeout [ssh | http] <timeout>

Sets the timeout values for SSH (CLI) and HTTP (Web and Redfish) sessions.

tpm [ism | host]

Switches the location of the tpm between two points in the chassis.

- `ism`: Uses the tpm delivered in the system.
- `host`: Uses the socket installed on the carrier board, which can accept a tcm module.

uid [on | off | blink]

Sets the status of the UID LED on the chassis.

username <old username> <new username>

Changes an existing username.

vusb [repofile | http_url | none]

Enables virtual USB with image file. Allows host to boot off the image from the repository, or from an HTTP File Server. This command requires a license key.

- `repofile`: Provide a boot image (.iso) file.
- `http_url`: Provide a URL that contains a boot image (.iso) file.
- `none`: Unmounts an image file or URL.

wifi

Creates a WiFi network and allows you to then change the WiFi network variables. You can create multiple WiFi networks. You can create a WiFi network ID, or the system can create an ID automatically.

Before modifying network variables, add the wifi network:

```
set wifi add
```

For example:

```
set wifi add
   New Network ID: 5
  set wifi 5 ssid MyWifiSSID
  set wifi 5 sec psk
  set wifi 5 pass "this is my passphrase!"
  set wifi 5 enable
```

The system generates and displays a network ID.

After you add a network, you use the following variables when you provide the network ID. Use the format, `set wifi <networkid> <variable> <variable_value>`

NOTE: Disable the WiFi Access Point when you connect to a WiFi network. After connecting to a WiFi network, you can enable the WiFi Access Point.

- `ssid`: Provide the network SSID. If the SSID includes empty spaces, use quotation marks around the SSID. For example, `set wifi 1 ssid "Publicly Broadcast"`.
- `hidden [yes | no]`: Sets whether the system broadcasts the WiFi SSID.
- `sec [psk | eap | none]`: Sets the security mode for the Wi-Fi network.
- `pass <password>`: Sets the password for the WiFi network. If the password includes empty spaces, use quotation marks around the password. For example, `set wifi 1 password "Local password"`.
- `eap [tls | ttls | PEAPsake]`: Sets the Extensible Authentication Protocol.
- `identity <network identity>`: Sets the network identity if the WiFi AP requires user credentials to connect to a network. Contact your network administrator for identity details.
- `anonymous_identity <anonymous_id>`: Sets the anonymous network identity.
- `ca_cert <filename>`: Provide the filename of a certificate in the certificate repository.
- `private_key <filename>`: Selects the private key in the certificate repository.
- `private_key_passwd <passphrase>`: Provide the passphrase that applies to the private key.
- `phase2 [md5 | tls | ttls | mschapv2 | peap | gtc | otp | leap | aka | fast | pax | sake |gpsk | wsc | ikev2 | tnc]`: Some networks require a phase 2 parameter. Contact your network administrator for details.
- `enable`: Enables the WiFi network, making the system connect automatically to WiFi networks. By default, new networks are disabled. Issue this command after setting up the network and providing the configuration variables. If there are multiple WiFi networks, the system connects to the strongest network. For example, `set wifi <networkid> enable`.
- `disable`: Disables the WiFi network without removing network configuration. For example, `set wifi <networkid> disable`.

To remove a WiFi network, use the `remove` variable. For example, `set wifi remove <networkID>`

Example input

Setting the access to LTE to the iSM:

```
set lte ism
```

Setting the boot order of devices to SATA first, then USB, NVME, and finally the first PXE device:

```
set boot devices sata usb nvme pxe
```

Setting the second PXE entry as the primary boot device of the PXE device type:

```
set boot details pxe pxe2
```

Setting the number of minutes to wait for the host to shut down gracefully after the vehicle ignition is turned off, and after the switch power off timer ends, before forcing the host power off:

```
set ignition hostpoweroff 10
```

Setting the number of minutes to keep iSM and the chassis running after the vehicle ignition is turned off:

```
set ignition switchpoweroff 5
```

Setting an IPv4 connection to DHCP:

```
set network dhcp
```

Setting an IPv6 connection to automatic addressing:

```
set network6 auto
```

Setting the serial port to be used by the host rather than iSM.

```
set serial host
```

Changing a username:

```
set username userold usernew
```

Setting the wifi details:

```
set wifi add
set wifi 5 ssid MyWifiSSID
set wifi 5 sec psk
set wifi 5 pass "this is my passphrase!"
set wifi 5 enable
```

show CLI command

Syntax

```
show [ap | asset | autopoweron | bios lock | boot devices | boot details
     | boot once | date | dc | files | firmware | hostname | ignition
     | inventory | license | lock | log | lte | network | power
     | powersupply | proxy | remotedeviceaccess | remotesupport | sensor
     | sshkey | ssl | status | switches | timeout | tpm | uid | vusb
     | users | wifi]
```

Description

Shows details for the defined variable.

Parameters

ap

Shows the status of the WiFi access point.

asset

Shows the asset tag for the system.

autopoweron

Shows the status of the automatic power on parameter.

bios lock

Shows the status of the BIOS lock.

boot devices

Shows the available types of boot devices. Some might contain devices in the same category.

boot details

Shows the available types of boot devices, plus the individual devices within the type that can be set.

boot once

Shows the boot device for the next boot only.

date

Shows the current system time and date.

dc [config | stats]

- `config`: Shows the daughter card configuration details.
- `stats`: Shows live information about the installed daughter cards.

files

Shows the files in the software repository.

firmware

Shows the firmware versions for the iSM, CPLD, BIOS, and iSM Base Image.

hostname

Shows the hostname for the iSM.

`ignition`

Shows the ignition switch configuration settings.

NOTE: This command is only available on compatible systems.

`inventory`

Shows the information for a replaceable unit. Details include, part number, serial number, processor, and memory for carrier board, host board, and power board.

`license all`

Shows information about the currently installed license.

`lock`

Shows if the lock is enabled or disabled.

`log [health | event]`

Shows health or event log information. You can use the following variables to filter the results.

- `{numentries}`: Displays the events based on the event number.
- `{info | caution | critical}`: Displays entries based on the event status.
- `{start_date | start_time | end_date | end_time}`: Lists the events based on the time or date of the event. For the dates, the format is YYYY-MM-DD. For the time, the format is HH:MM:SS.

  NOTE: Use `start_date` and `start_time` parameters together. The report will display information after the date. For example:

  ```
  show log event 2018-08-15 22:13:57
  ```

  If you use start and end date and time, then the system displays all health or event log between those time parameters.

`lte`

Shows the wireless LTE settings, including owner, APN, and status.

`network`

Shows iSM network settings.

`power`

Shows the power status of the host.

`powersupply`

Shows the status of the voltage monitoring of the power supplies.

`proxy`

Shows the current proxy, if there is a proxy set.

`remotedeviceaccess`

Shows the status of HPE Remote Device Access, including whether it is enabled, running, and the version. When enabled, HPE service personnel can diagnose issues remotely. This feature is disabled by default.

`remotesupport`

Shows the status of eRS Remote Support

`sensor`

Shows the status for all sensors.

`sshkey`

Shows the users SSH keys.

`ssl`

Shows information about the installed SSL private key and SSL certificate.

`status`

Shows the status of the voltage monitoring of the power supplies, and the temperatures for various components and zones in the chassis.

`switches`

Shows the status for physical input devices. Use the `enable` or `disable` command to change the status.

`users`

Shows the list of users, along with their access permissions (admin or user).

`timeout`

Shows the timeout values for SSH and HTTP sessions.

`tpm`

Shows the status of the TPM.

`uid`

Shows the status of the chassis UID.

`vusb`

Shows the status, connection, and image name of the virtual USB.

`wifi [status | scan | certs | config | config <networkID>]`

Shows WiFi client information, if a WiFi license is installed. The following arguments are supported:

- `status`: Shows the status of the WiFi client.
- `scan`: Performs a WiFi scan, and shows nearby WiFi networks.
- `certs`: Shows the WiFi certifications in the certificate repository.
- `config`: Shows which networks are configured, and whether they are enabled or disabled.
- `config <networkID>`: Shows the configuration setting for the specified WiFi network.

If the `show wifi` command is entered without an installed WiFi license, the command returns an error message.

Example input

```
show wifi
```

```
show power
```

test CLI command

Syntax

```
test [event | collection]
```

Description

Send the specified test data to Remote Support. Remote Support must be enabled to support this command.

Parameters

event

Sends a single test event to HPE Remote Support.

collection

Sends a test Data Collection to HPE Remote Support. The Data Collection is a copy of the system configuration information.

Example input

Sending a single test event:

```
test event
```

Sending a test data collection:

```
test collection
```

update CLI command

Syntax

```
update [url | filename]
```

Description

Updates or downgrades the firmware from the local repository or a valid URL. After performing an update, log out of the system and then log in again. After logging in, you can view the updated firmware details.

Parameters

url

Enter a valid URL where the firmware updates are saved. Use the URL format `http://`*serverlocation*/*path*/*filename*.

filename

Enter a filename that has been added to the local repository.

Example input

Updating the firmware from a URL:

```
update http://<IPv4 address or host name>/<path>/<filename>
```

Updating the firmware using a file already in the repository:

```
update <repository filename>
```

Websites and Support

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Hewlett Packard Enterprise Edgeline Documentation

www.hpe.com/info/edgeline-docs

Hewlett Packard Enterprise Edgeline Information

www.hpe.com/info/edgeline

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

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

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

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

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

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

  Hewlett Packard Enterprise Support Center: Software downloads

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

  My HPE Software Center

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

- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

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

ⓘ **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

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

HPE Proactive Care services

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

HPE Datacenter Care services

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

HPE Proactive Care service: Supported products list

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

HPE Proactive Care advanced service: Supported products list

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

Proactive Care customer information

Proactive Care central

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

Proactive Care service activation

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

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

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

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

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

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

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

Documentation feedback

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