Hewlett Packard Enterprise

HPE ProLiant XL450 Gen10 Server User Guide

Abstract

This document is for the person who installs, administers, and troubleshoots servers and storage systems. Hewlett Packard Enterprise assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Contents

Troubleshooting..53

Removing and replacing the system battery.....................54

Electrostatic discharge..55

Specifications..56

Websites...57

Support and other resources.......................................58

Component identification

Front panel components
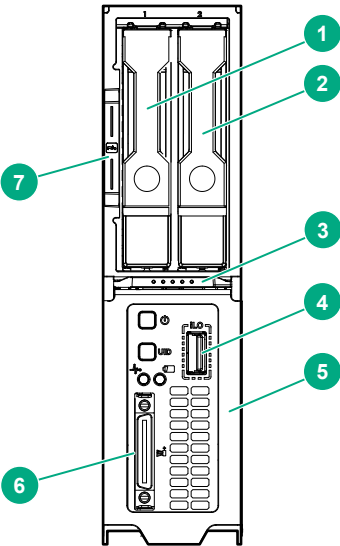
Item	Description
1	Drive bay 1
2	Drive bay 2
3	Server ejector button
4	iLO Service port
5	Server release lever
6	SUV cable connector
7	Serial label pull tab

Front panel LEDs and buttons

Item	Description	Status
1	Power On/Standby button and system power LED	Solid green = System on
		Flashing green (1 Hz/cycle per sec) = Performing power on sequence
		Solid amber = System in standby
		Off = No power present
2	UID LED/button	Solid blue = Activated
		Flashing blue:
		• 1 Hz/cycle per sec = Remote management or firmware upgrade in progress
		• 4 Hz/cycle per sec = iLO manual reboot sequence initiated
		• 8 Hz/cycle per sec = iLO manual reboot sequence in progress
		• 1 fast flash and then off for 3 seconds = iLO Service Port status is Complete
		• 4 medium flashes and then off for 1 second = iLO Service Port status is Busy
		• 8 fast flashes and then off for 1 second = iLO Service Port status is Error
		Off = Deactivated

Table Continued

Item	Description	Status
3	Server health LED	Solid green = Normal
		Flashing green (1 Hz/cycle per sec) = iLO is rebooting
		Flashing amber = System degraded
		Flashing red (1 Hz/cycle per sec) = System critical
4	Server backup LED	Off = Normal operations. No backup in progress.
		Flashing white = Backup in progress. Do not remove drives, nodes, or associated system components, and do not power down the server.

Hot-plug drive LED definitions

Item	LED	Status	Definition
1	Locate	Solid blue	The drive is being identified by a host application.
		Flashing blue	The drive carrier firmware is being updated or requires an update.
2	Activity ring	Rotating green	Drive activity
		Off	No drive activity
3	Do not remove	Solid white	Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.
		Off	Removing the drive does not cause a logical drive to fail.
4	Drive status	Solid green	The drive is a member of one or more logical drives.

Table Continued

Item	LED	Status	Definition
		Flashing green	The drive is doing one of the following: • Rebuilding • Performing a RAID migration • Performing a strip size migration • Performing a capacity expansion • Performing a logical drive extension • Erasing • Spare part activation
		Flashing amber/green	The drive is a member of one or more logical drives and predicts the drive will fail.
		Flashing amber	The drive is not configured and predicts the drive will fail.
		Solid amber	The drive has failed.
		Off	The drive is not configured by a RAID controller or a spare drive.

NVMe SSD LED definitions

The NVMe SSD is a PCIe bus device. A device attached to a PCIe bus cannot be removed without allowing the device and bus to complete and cease the signal/traffic flow.

> △ **CAUTION:** Do not remove an NVMe SSD from the drive bay while the Do not remove LED is flashing. The Do not remove LED flashes to indicate that the device is still in use. Removing the NVMe SSD before the device has completed and ceased signal/traffic flow can cause loss of data.
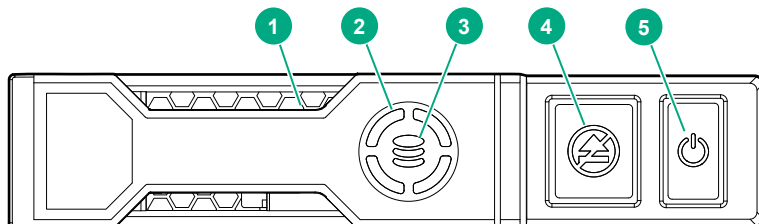
Item	LED	Status	Definition
1	Locate	Solid blue	The drive is being identified by a host application.
		Flashing blue	The drive carrier firmware is being updated or requires an update.
2	Activity ring	Rotating green	Drive activity
		Off	No drive activity
3	Drive status	Solid green	The drive is a member of one or more logical drives.

Table Continued

Item	LED	Status	Definition
		Flashing green	The drive is doing one of the following: • Rebuilding • Performing a RAID migration • Performing a stripe size migration • Performing a capacity expansion • Performing a logical drive extension • Erasing
		Flashing amber/green	The drive is a member of one or more logical drives and predicts the drive will fail.
		Flashing amber	The drive is not configured and predicts the drive will fail.
		Solid amber	The drive has failed.
		Off	The drive is not configured by a RAID controller.
4	Do not remove	Solid white	Do not remove the drive. The drive must be ejected from the PCIe bus prior to removal.
		Flashing white	The drive ejection request is pending.
		Off	The drive has been ejected.
5	Power	Solid green	Do not remove the drive. The drive must be ejected from the PCIe bus prior to removal.
		Flashing green	The drive ejection request is pending.
		Off	The drive has been ejected.

SFF flash adapter components and LED definitions
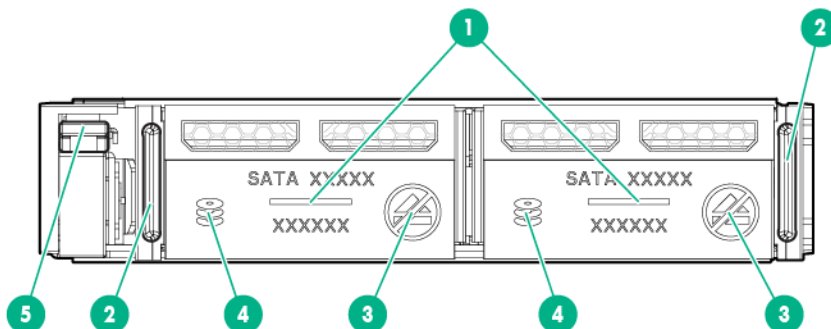
Item	Component	Description
1	Locate	• Off—Normal
		• Solid blue—The drive is being identified by a host application.
		• Flashing blue—The drive firmware is being updated or requires an update.
2	uFF drive ejection latch	Removes the uFF drive when released.
3	Do not remove LED	• Off—OK to remove the drive. Removing the drive does not cause a logical drive to fail.
		• Solid white—Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.
4	Drive status LED	• Off—The drive is not configured by a RAID controller or a spare drive.
		• Solid green—The drive is a member of one or more logical drives.
		• Flashing green (4 Hz)—The drive is operating normally and has activity.
		• Flashing green (1 Hz)—The drive is rebuilding, erasing, or performing a RAID migration, stripe size migration, capacity expansion, logical drive extension, or spare activation.
		• Flashing amber/green (1 Hz)—The drive is a member of one or more logical drives that predicts the drive will fail.
		• Solid amber—The drive has failed.
		• Flashing amber (1 Hz)—The drive is not configured and predicts the drive will fail.
5	Adapter ejection release latch and handle	Removes the SFF flash adapter when released.

Server components

Item	Description
1	Drive cage
2	Drive backplane
3	TPM 2.0 connector
4	Controller connector
5	System maintenance switch
6	Processor 1
7	Processor 1 DIMMs (8)
8	Processor 2
9	Processor 2 DIMMs (8)
10	System battery
11	SFF drive cage data cable connector
12	M.2 riser board
13	Front panel I/O board cable connector
14	microSD card slot
15	Front panel I/O board
16	iLO Service Port board

DIMM slot locations

The arrow points to the front of the server.

DIMM slots closest to the processors support NVDIMMs.
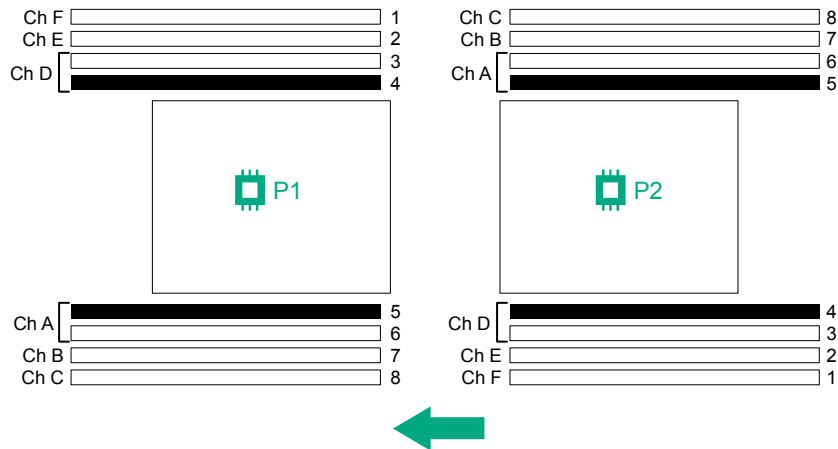
System maintenance switch

Position	Default	Function
S1	Off	Off = iLO security is enabled.
		On = iLO security is disabled.
S2	Off	Reserved
S3	Off	Reserved
S4	Off	Reserved
S5	Off	Off = Power-on password is enabled.
		On = Power-on password is disabled.
S6	Off	Off = No function
		On = ROM reads system configuration as invalid.
S7	Off	Reserved
S8	—	Reserved
S9	—	Reserved
S10	—	Reserved
S11	—	Reserved
S12	—	Reserved

To access the redundant ROM, set S1, S5, and S6 to On.

When system maintenance switch S6 is set to the On position, the system is prepared to erase all system configuration settings from both CMOS and NVRAM.

Operations

Powering down the server

Before powering down the server for any upgrade or maintenance procedures, perform a backup of critical server data and programs.

> (!) **IMPORTANT:** When the server is in standby mode, auxiliary power is still being provided to the system.

To power down the server, use one of the following methods:

- Press and release the Power On/Standby button.

  This method initiates a controlled shutdown of applications and the OS before the server enters standby mode.

- Press and hold the Power On/Standby button for more than 4 seconds to force the server to enter standby mode.

  This method forces the server to enter standby mode without properly exiting applications and the OS. If an application stops responding, you can use this method to force a shutdown.

- Use a virtual power button selection through iLO.

  This method initiates a controlled remote shutdown of applications and the OS before the server enters standby mode.

Before proceeding, verify that the server is in standby mode by observing that the system power LED is amber.

Powering up the server

To power up the server, press the Power On/Standby button.

Remove the server from the chassis

> △ **CAUTION:** Before removing the server, verify that the server backup LED is not flashing.

Procedure

1. **Powering down the server** on page 14.

   > △ **CAUTION:** To avoid damage to the server, always support the bottom of the server when removing it from the chassis.

2. Remove the server from the chassis.
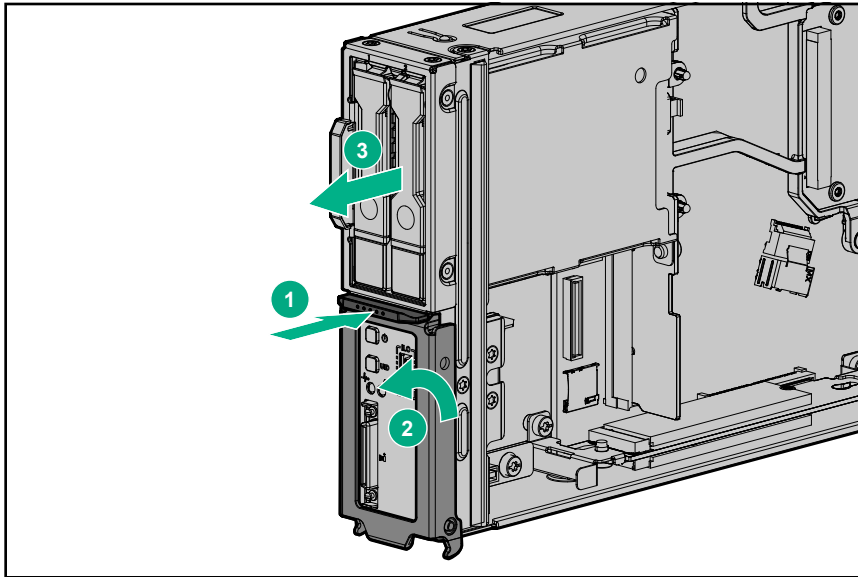
NOTE: To avoid damage to the device, do not use the removal handle to carry it.

---

3. Place the server on a flat, level work surface.

Setup

Optional service

Delivered by experienced, certified engineers, Hewlett Packard Enterprise support services help you keep your servers up and running with support packages tailored specifically for HPE ProLiant systems. Hewlett Packard Enterprise support services let you integrate both hardware and software support into a single package. A number of service level options are available to meet your business and IT needs.

Hewlett Packard Enterprise support services offer upgraded service levels to expand the standard product warranty with easy-to-buy, easy-to-use support packages that will help you make the most of your server investments. Some of the Hewlett Packard Enterprise support services for hardware, software or both are:

*   Foundation Care – Keep systems running.
    *   6-Hour Call-to-Repair[1]
    *   4-Hour 24x7
    *   Next Business Day

*   Proactive Care – Help prevent service incidents and get you to technical experts when there is one.
    *   6-Hour Call-to-Repair[1]
    *   4-Hour 24x7
    *   Next Business Day

*   Deployment service for both hardware and software

*   Hewlett Packard Enterprise Education Services – Help train your IT staff.

[1]The time commitment for this repair service might vary depending on the geographical region of site. For more service information available in your site, contact your local **Hewlett Packard Enterprise support center**.

For more information on Hewlett Packard Enterprise support services, see the **Hewlett Packard Enterprise website**.

Rack planning resources

The rack resource kit ships with all HPE Intelligent Series racks. For more information on the content of each resource, see the rack resource kit documentation.

Optimum environment

When installing the server in a rack, select a location that meets the environmental standards described in this section.

Space and airflow requirements

To enable servicing and ensure adequate airflow, observe the following spatial requirements when deciding where to install a rack:

- Leave a minimum clearance of 121.9 cm (48.0 in) in front of the rack and between rows of racks.

- Leave a minimum clearance of 76.2 cm (30.0 in) in back of the rack for a single row of racks or after the final row of racks.

Hewlett Packard Enterprise Rack products draw cool air in through the front and expel warm air through the rear of the enclosure. Therefore, the front of the rack enclosure must be adequately ventilated to enable ambient room air to enter the enclosure, and the rear of the enclosure must be adequately ventilated to enable the warm air to escape from the enclosure.

ⓘ **IMPORTANT:** Do not block the ventilation openings.

If the front of the rack is not completely filled with components, the remaining gaps between the components can cause changes in the airflow, which can adversely affect cooling within the rack. Cover these gaps with blanking panels.

⚠ **CAUTION:** Always use blanking panels to fill empty vertical spaces in the rack. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

Racks provide proper server cooling from flow-through perforations in the front and rear doors that provide a 65% open area for ventilation.

Temperature requirements

To ensure continued safe and reliable equipment operation, install or position the system in a well-ventilated, climate-controlled environment.

The maximum recommended ambient operating temperature (TMRA) for most server products is 35°C (95°F). The temperature in the room where the rack is located must not exceed 35°C (95°F).

⚠ **CAUTION:** To reduce the risk of damage to the equipment when installing third-party options:

- Do not permit optional equipment to impede airflow around the server or to increase the internal rack temperature beyond the maximum allowable limits.

- Do not exceed the manufacturer's TMRA.

Power requirements

Installation of this equipment must comply with local and regional electrical regulations governing the installation of information technology equipment by licensed electricians. This equipment is designed to operate in installations covered by NFPA 70, 1999 Edition (National Electric Code) and NFPA-75, 1992 (code for Protection of Electronic Computer/Data Processing Equipment). For electrical power ratings on options, refer to the product rating label or the user documentation supplied with that option.

⚠ **WARNING:** To reduce the risk of personal injury, fire, or damage to the equipment, do not overload the AC supply branch circuit that provides power to the chassis. Consult the electrical authority having jurisdiction over wiring and installation requirements of your facility.

⚠ **CAUTION:** Protect the server from power fluctuations and temporary interruptions with a regulating uninterruptible power supply. This device protects the hardware from damage caused by power surges and voltage spikes and keeps the system in operation during a power failure.

When installing more than one server, you might need to use additional power distribution devices to safely provide power to all devices. Observe the following guidelines:

- Balance the server power load between available AC supply branch circuits.

- Do not allow the overall system AC current load to exceed 80% of the branch circuit AC current rating.

- Do not use common power outlet strips for this equipment.

- Provide a separate electrical circuit for the server.

For more information on the hot-plug power supply and calculators to determine server power consumption in various system configurations, see the **Hewlett Packard Enterprise Power Advisor website**.

Electrical grounding requirements

The server must be grounded properly for proper operation and safety. In the United States, you must install the equipment in accordance with NFPA 70, 1999 Edition (National Electric Code), Article 250, as well as any local and regional building codes. In Canada, you must install the equipment in accordance with Canadian Standards Association, CSA C22.1, Canadian Electrical Code. In all other countries, you must install the equipment in accordance with any regional or national electrical wiring codes, such as the International Electrotechnical Commission (IEC) Code 364, parts 1 through 7. Furthermore, you must be sure that all power distribution devices used in the installation, such as branch wiring and receptacles, are listed or certified grounding-type devices.

Because of the high ground-leakage currents associated with multiple servers connected to the same power source, Hewlett Packard Enterprise recommends the use of a PDU that is either permanently wired to the building's branch circuit or includes a nondetachable cord that is wired to an industrial-style plug. NEMA locking-style plugs or those complying with IEC 60309 are considered suitable for this purpose. Using common power outlet strips for the server is not recommended.

Installing the server

The server is installed in the chassis. If the chassis is not already installed in a rack, install the chassis in a rack.

For more information, see the *HPE Apollo 4510 Gen10 chassis Setup and Installation Guide* and the *HPE Apollo 4500 4U Rail Installation Instructions* that ship with the rack hardware kit.

Install a server

△ **CAUTION:** To prevent improper cooling and thermal damage, do not operate the chassis unless all bays are populated with a component or a blank.

Procedure

1. Prepare the server for installation.
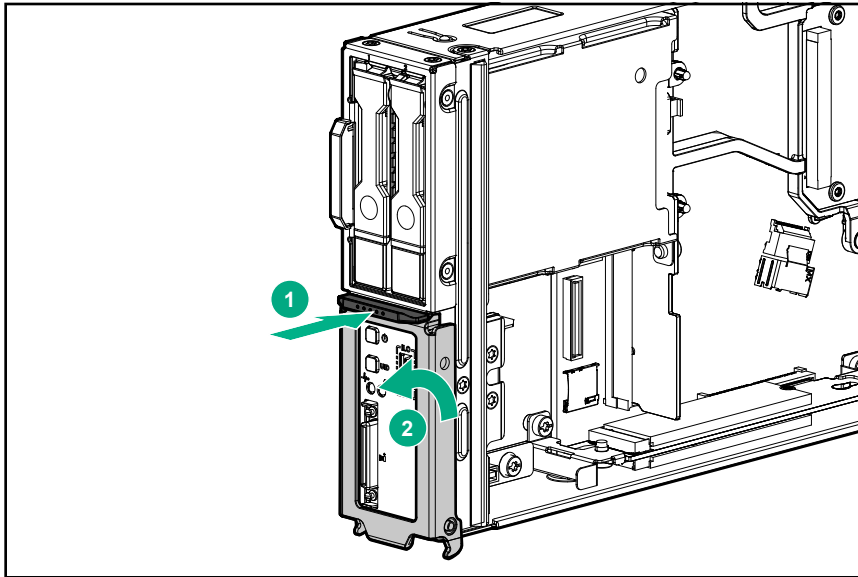
2. Install the server. When seated properly, the server will be flush with the front of the chassis and the release lever will close completely without resistance.
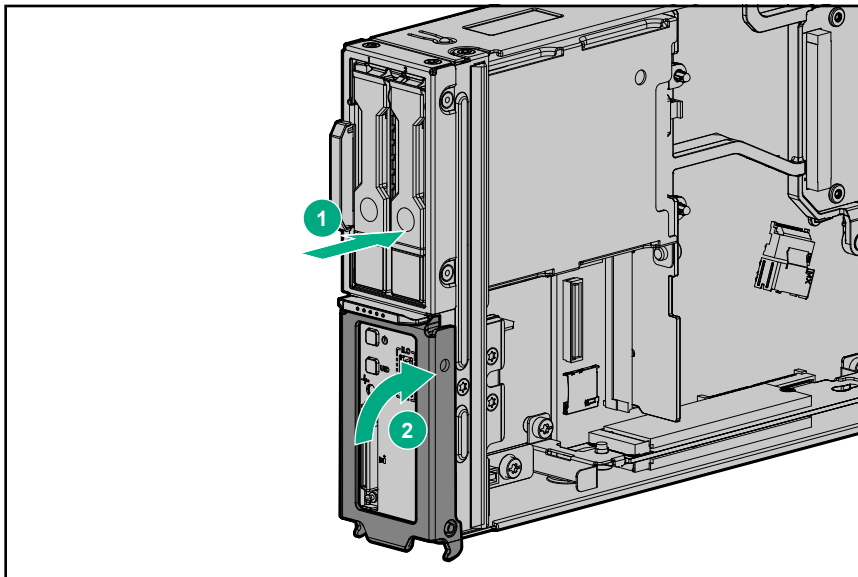
Installing hardware options

Install any hardware options before initializing the server. For options installation information, see the option documentation. For server-specific information, see **Hardware options installation** on page 21.

Configuring the chassis

Configure the chassis, if it is not already configured. For more information on setting up and configuring your system, see the *Apollo 4510 Gen10 Chassis Setup and Installation Guide*.

Selecting boot options in UEFI Boot Mode

On servers operating in UEFI Boot Mode, the boot controller and boot order are set automatically.

Procedure

1. Press the Power On/Standby button.

2. During the initial boot:

   - To modify the server configuration ROM default settings, press the **F9** key in the ProLiant POST screen to enter the UEFI System Utilities screen. By default, the System Utilities menus are in the English language.

   - If you do not need to modify the server configuration and are ready to install the system software, press the **F10** key to access Intelligent Provisioning.

For more information on automatic configuration, see the UEFI documentation on the **Hewlett Packard Enterprise website**.

Installing the operating system

To operate properly, the server must have a supported operating system installed. For the latest information on operating system support, see the Hewlett Packard Enterprise website (**http://www.hpe.com/info/supportos**).

> (i) **IMPORTANT:** HPE ProLiant XL servers do not support operating system installation with Intelligent Provisioning, but they do support the maintenance features. For more information, see "Performing Maintenance" in the *HPE Intelligent Provisioning User Guide* and online help.

To install an operating system on the server, use one of the following methods:

- Insert the operating system CD into the USB-attached DVD-ROM drive (user provided) and reboot the server. Download the Service Pack for ProLiant from the SPP download site (**http://www.hpe.com/servers/spp/download**) and create SPP media to install the drivers.

- Remote deployment installation — Use PXE boot into a server and deploy an operating system with a host server.

For additional system software and firmware updates, download the Service Pack for ProLiant from the Hewlett Packard Enterprise website (**http://www.hpe.com/servers/spp/download**). Software and firmware must be updated before using the node for the first time, unless any installed software or components require an older version.

For more information on using these installation methods, see the Hewlett Packard Enterprise website (**http://www.hpe.com/info/ilo**).

Registering the server

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

Hardware options installation

Introduction

Install any hardware options before initializing the server. For options installation information, see the option documentation. For server-specific information, use the procedures in this section.

If multiple options are being installed, read the installation instructions for all the hardware options to identify similar steps and streamline the installation process.

⚠ **WARNING:** To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

⚠ **CAUTION:** To prevent damage to electrical components, properly ground the server before beginning any installation procedure. Improper grounding can cause electrostatic discharge.

Installing a processor

The server supports single-processor and dual processor operations. You can install a processor in the second processor socket.

Prerequisites
Before installing this option, be sure that you have the following items:

- Processor and heatsink kit contents
- T-30 Torx screwdriver

Procedure

1. Observe the following alerts:

   ⚠ **WARNING:** To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

   ⚠ **CAUTION:** To prevent possible server malfunction and damage to the equipment, multiprocessor configurations must contain processors with the same part number.

   ⓘ **IMPORTANT:** Existing HPE ProLiant and HPE Synergy Gen10 server products containing First Generation Intel Xeon Scalable Processors may not be upgraded to Second Generation Intel Xeon Scalable Processors at this time. For more information, see the product QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/qs**).

   ⚠ **CAUTION: THE CONTACTS ARE VERY FRAGILE AND EASILY DAMAGED.** To avoid damage to the socket or processor, do not touch the contacts.

   ⚠ **CAUTION:** To prevent possible server overheating, always populate processor socket 2 with a processor and a heatsink or a processor socket cover and a heatsink blank.

⚠ CAUTION: The heatsink thermal interface media is not reusable and must be replaced if the heatsink is removed from the processor after it has been installed.

⚠ CAUTION: To prevent damage to electrical components, properly ground the server before beginning any installation procedure. Improper grounding can cause ESD.

ⓘ IMPORTANT: Processor socket 1 must be populated at all times or the server does not function.

2. Update the system ROM.

   Locate and download the latest ROM version from the Hewlett Packard Enterprise Support Center website (**http://www.hpe.com/support/hpesc**). Follow the instructions on the website to update the system ROM.

3. **Powering down the server** on page 14.

4. **Remove the server from the chassis** on page 14.

5. Place the server on a flat, level surface.

6. Remove the heatsink blank from the processor 2 location. Retain the heatsink blank for future use.
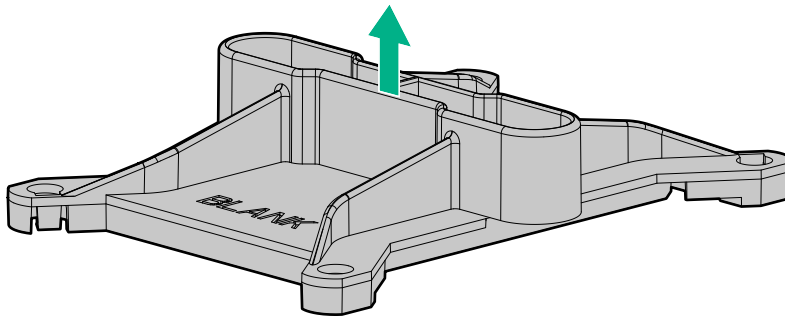
7. Install the processor-heatsink assembly:

   a. Locate and align the Pin 1 indicator on the processor frame and the socket.

   b. Align the processor-heatsink module with the heatsink alignment pins and gently lower it down until it sits evenly on the socket.
      The heatsink alignment pins are keyed. The processor will only install one way.

      Your heatsink may look different than the one shown.
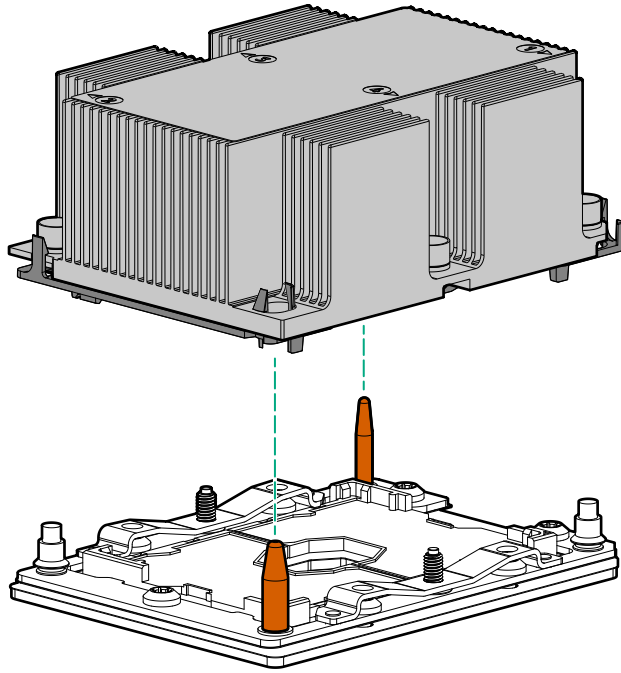
⚠ **CAUTION:** Be sure to tighten each heatsink nut fully in the order indicated. Otherwise, boot failure or intermittent shutdowns might occur.

c. Using a T-30 Torx screwdriver, fully tighten each heatsink screw in the order indicated on the heatsink label (1 -2 -3 -4) until it no longer turns.
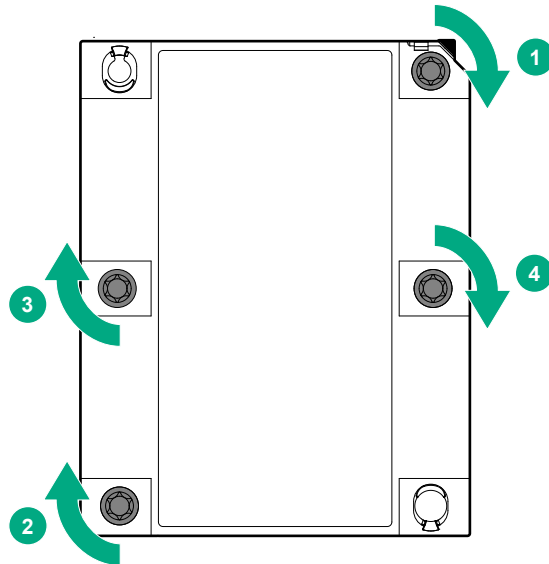
8. Install the server in the rack.

9. **Powering up the server** on page 14.

Memory options

> ⓘ **IMPORTANT:** This server does not support mixing LRDIMMs and RDIMMs. Attempting to mix any combination of these DIMMs can cause the server to halt during BIOS initialization. All memory installed in the server must be of the same type.

DIMM population information

For specific DIMM population information, see the DIMM population guidelines on the Hewlett Packard Enterprise website (**http://www.hpe.com/docs/memory-population-rules**).

DIMM-processor compatibility

The installed processor determines the type of DIMM that is supported in the server:

- First Generation Intel Xeon Scalable Processors support DDR4-2666 DIMMs.

- Second Generation Intel Xeon Scalable Processors support DDR4-2933 DIMMs.

Mixing DIMM types is not supported. Install only the supported DDR4-2666 or DDR4-2933 DIMMs in the server.

HPE SmartMemory speed information

For more information about memory speed information, see the Hewlett Packard Enterprise website (**https://www.hpe.com/docs/memory-speed-table**).

DIMM label identification

To determine DIMM characteristics, see the label attached to the DIMM. The information in this section helps you to use the label to locate specific information about the DIMM.
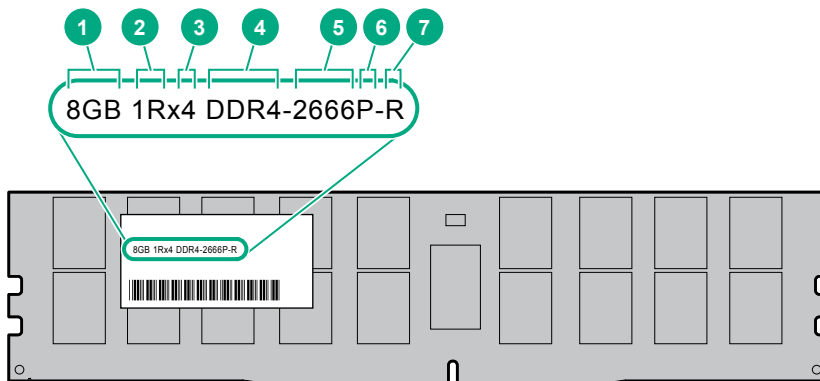
Item	Description	Example
1	Capacity	8 GB
		16 GB
		32 GB
		64 GB
		128 GB
2	Rank	1R = Single rank
		2R = Dual rank
		4R = Quad rank
		8R = Octal rank
3	Data width on DRAM	x4 = 4-bit
		x8 = 8-bit
		x16 = 16-bit
4	Memory generation	PC4 = DDR4
5	Maximum memory speed	2133 MT/s
		2400 MT/s
		2666 MT/s
		2933 MT/s
6	CAS latency	P = CAS 15-15-15
		T = CAS 17-17-17
		U = CAS 20-18-18
		V = CAS 19-19-19 (for RDIMM, LRDIMM)
		V = CAS 22-19-19 (for 3DS TSV LRDIMM)
		Y = CAS 21-21-21 (for RDIMM, LRDIMM)
		Y = CAS 24-21-21 (for 3DS TSV LRDIMM)
7	DIMM type	R = RDIMM (registered)
		L = LRDIMM (load reduced)
		E = Unbuffered ECC (UDIMM)

For more information about product features, specifications, options, configurations, and compatibility, see the HPE DDR4 SmartMemory QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/support/DDR4SmartMemoryQS**).

Installing a DIMM

⚠ CAUTION: To avoid damage to the hard drives, memory, and other system components, the air baffle, and drive blanks must be installed when the server is powered up.

Procedure

1. **Powering down the server** on page 14.

2. **Remove the server from the chassis** on page 14.

3. Open the DIMM slot latches.

4. Install the DIMM.
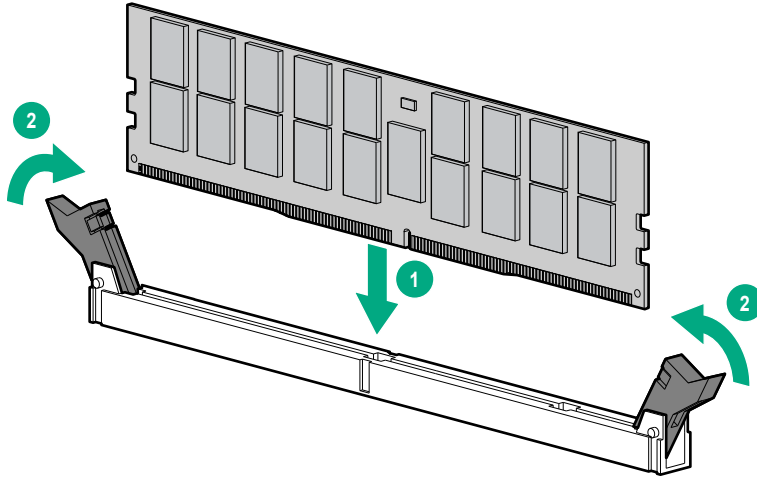
5. Install the server into the chassis (**Install a server** on page 18).

6. **Powering up the server** on page 14.

To configure the memory mode, use **UEFI System Utilities** on page 44.

Hot-plug hard drive guidelines

When adding hard drives to the server, observe the following general guidelines:

- The system automatically sets all device numbers.

- If only one hard drive is used, install it in the bay with the lowest bay number.

- Drives must be of the same capacity to provide the greatest storage space efficiency when drives are grouped into the same drive array.

Removing a drive blank

Remove the component as indicated.
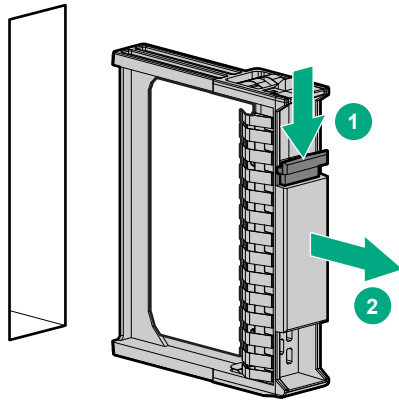
CAUTION: To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with either a component or a blank.

Installing an SFF drive

Procedure

1. Remove a drive blank (**Removing a drive blank** on page 26).
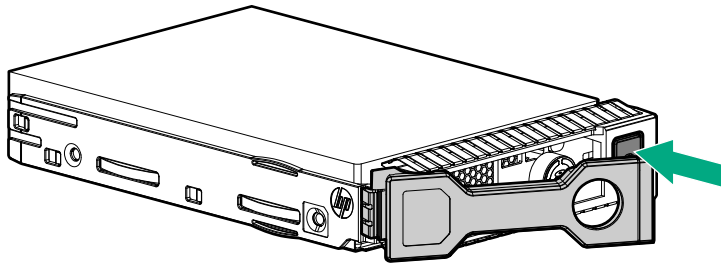
2. Prepare the drive.
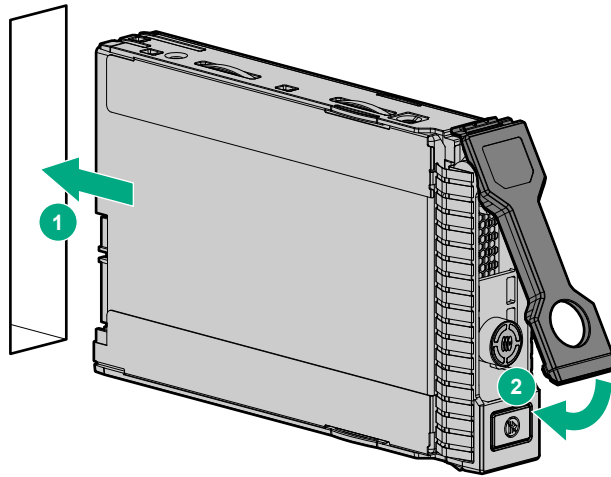
3. Install the drive.

4. Determine the status of the drive from the drive LED definitions (**Hot-plug drive LED definitions** on page 8).

Installing an NVMe drive

⚠ **CAUTION:** To prevent improper cooling and thermal damage, do not operate the chassis unless all device bays are populated with either a component or a blank.

Procedure

1. Remove a drive blank (**Removing a drive blank** on page 26).

2. Prepare the drive.
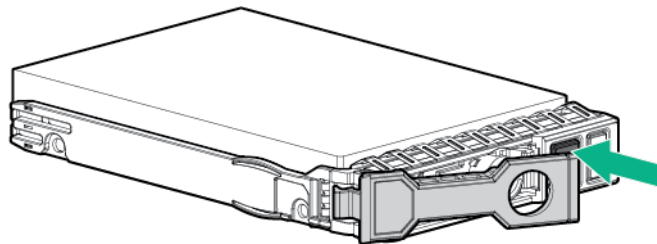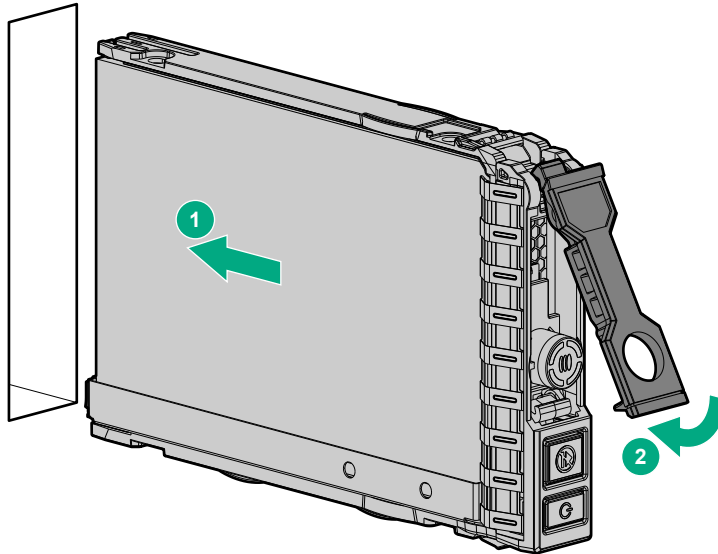
3. Install the drive.

4. Determine the status of the drive from the drive LED definitions (**Hot-plug drive LED definitions** on page 8).

Installing the SFF flash adapter option

⚠ **CAUTION:** To prevent improper cooling and thermal damage, do not operate the server or the enclosure unless all drive and device bays are populated with either a component or a blank.

Procedure

1. Remove the drive blank.

2. Install the SFF flash adapter by pushing firmly near the left-side adapter ejection handle until the latching spring engages in the drive bay.
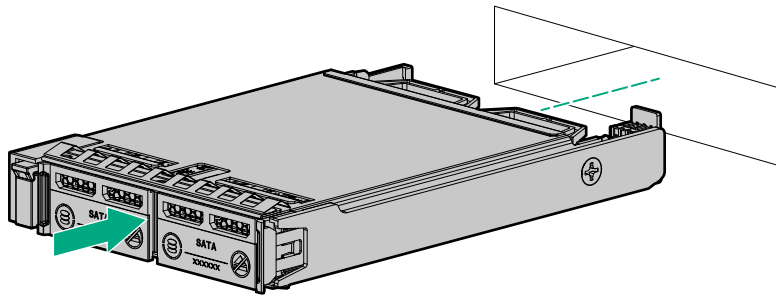
Installing a storage controller option

Prerequisites

Before installing this option, be sure that you have the following:

• The components included with the hardware option kit

• T-15 Torx screwdriver

Procedure

1. Observe the following alerts:

    ⚠ **WARNING:** To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

    ⚠ **CAUTION:** To prevent damage to electrical components, properly ground the server before beginning any installation procedure. Improper grounding can cause electrostatic discharge.

2. Back up all server data.

3. **Powering down the server** on page 14.

4. **Remove the server from the chassis** on page 14.

5. Place the server on a flat, level work surface.

6. Install the storage controller.
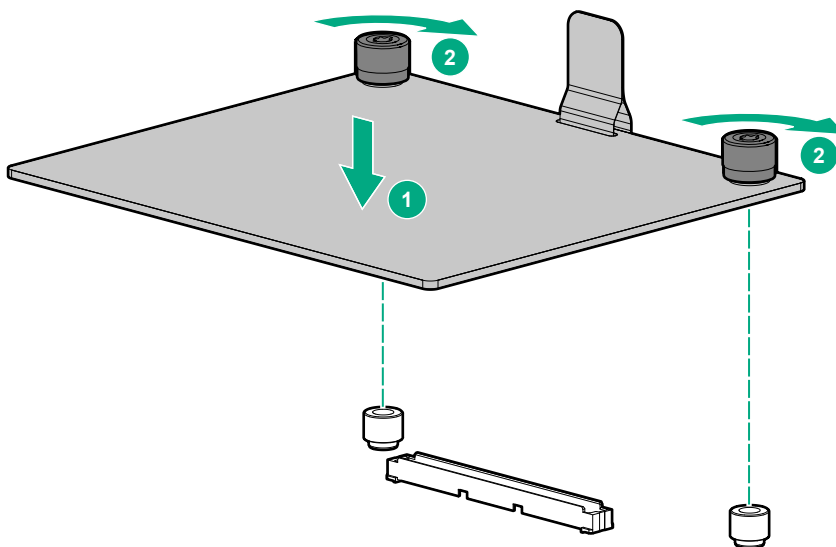
7. Connect the cable. For more information, see **Controller cabling** on page 37.

8. Install the server (**Install a server** on page 18).

9. **Powering up the server** on page 14.

HPE Trusted Platform Module 2.0 Gen10 option

Overview

Use these instructions to install and enable an HPE TPM 2.0 Gen10 Kit in a supported server. This option is not supported on Gen9 and earlier servers.

This procedure includes three sections:

1. Installing the Trusted Platform Module board.

2. Enabling the Trusted Platform Module.

3. Retaining the recovery key/password.

HPE TPM 2.0 installation is supported with specific operating system support such as Microsoft®
Windows Server® 2012 R2 and later. For more information about operating system support, see the
product QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/qs**). For more
information about Microsoft® Windows® BitLocker Drive Encryption feature, see the Microsoft website
(**http://www.microsoft.com**).

> **CAUTION:** If the TPM is removed from the original server and powered up on a different server,
> data stored in the TPM including keys will be erased.

> **IMPORTANT:** In UEFI Boot Mode, the HPE TPM 2.0 Gen10 Kit can be configured to operate as
> TPM 2.0 (default) or TPM 1.2 on a supported server. In Legacy Boot Mode, the configuration can be
> changed between TPM 1.2 and TPM 2.0, but only TPM 1.2 operation is supported.

HPE Trusted Platform Module 2.0 Guidelines

> **CAUTION:** Always observe the guidelines in this document. Failure to follow these guidelines can
> cause hardware damage or halt data access.

When installing or replacing a TPM, observe the following guidelines:

- Do not remove an installed TPM. Once installed, the TPM is bound to the system board. If an OS is
  configured to use the TPM and it is removed, the OS may go into recovery mode, data loss can occur,
  or both.

- When installing or replacing hardware, Hewlett Packard Enterprise service providers cannot enable
  the TPM or the encryption technology. For security reasons, only the customer can enable these
  features.

- When returning a system board for service replacement, do not remove the TPM from the system
  board. When requested, Hewlett Packard Enterprise Service provides a TPM with the spare system
  board.

- Any attempt to remove the cover of an installed TPM from the system board can damage the TPM
  cover, the TPM, and the system board.

- If the TPM is removed from the original server and powered up on a different server, data stored in the
  TPM including keys will be erased.

- When using BitLocker, always retain the recovery key/password. The recovery key/password is
  required to complete Recovery Mode after BitLocker detects a possible compromise of system
  integrity or system configuration.

- Hewlett Packard Enterprise is not liable for blocked data access caused by improper TPM use. For
  operating instructions, see the TPM documentation or the encryption technology feature
  documentation provided by the operating system.

Installing and enabling the HPE TPM 2.0 Gen10 Kit

Installing the Trusted Platform Module board

Preparing the server for installation

Procedure

1. Observe the following warnings:

⚠ WARNING: The front panel Power On/Standby button does not shut off system power. Portions of the power supply and some internal circuitry remain active until AC power is removed.

To reduce the risk of personal injury, electric shock, or damage to the equipment, remove power from the server:

For rack and tower servers, remove the power cord.

For server blades and compute modules, remove the server blade or compute module from the enclosure.

⚠ WARNING: To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

2. Update the system ROM.

   Locate and download the latest ROM version from the **Hewlett Packard Enterprise Support Center website**. Follow the instructions on the website to update the system ROM.

3. Power down the server (**Powering down the server** on page 14).

4. **Remove the server from the chassis** on page 14.

5. Place the server on a flat, level work surface.

6. Remove any options or cables that may prevent access to the TPM connector.

7. Proceed to **Installing the TPM board and cover** on page 32.

Installing the TPM board and cover

Procedure

1. Observe the following alerts:

   △ CAUTION: If the TPM is removed from the original server and powered up on a different server, data stored in the TPM including keys will be erased.

   △ CAUTION: The TPM is keyed to install only in the orientation shown. Any attempt to install the TPM in a different orientation might result in damage to the TPM or system board.

2. Align the TPM board with the key on the connector, and then install the TPM board. To seat the board, press the TPM board firmly into the connector. To locate the TPM connector on the system board, see the server label on the access panel.
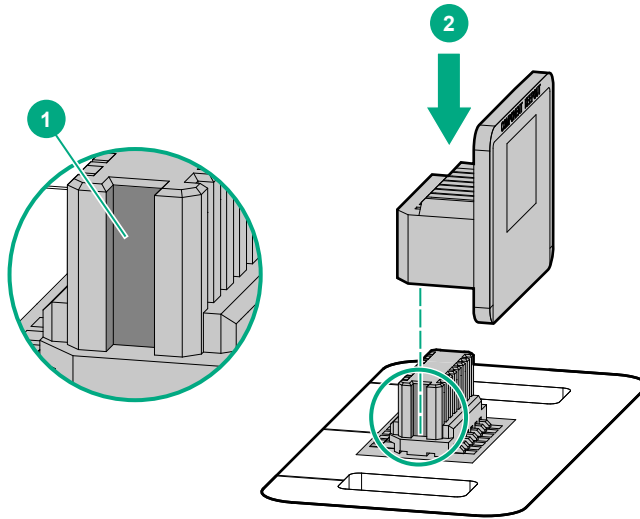
3. Install the TPM cover:

    a. Line up the tabs on the cover with the openings on either side of the TPM connector.

    b. To snap the cover into place, firmly press straight down on the middle of the cover.
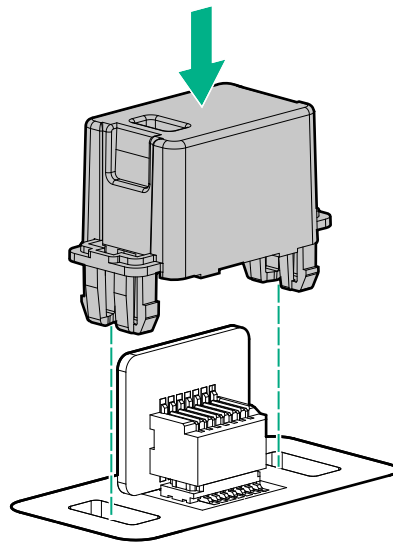
4. Proceed to **Preparing the server for operation** on page 33.

Preparing the server for operation

Procedure

1. Install any options or cables previously removed to access the TPM connector.

2. Install the server in the chassis.

Enabling the Trusted Platform Module

When enabling the Trusted Platform module, observe the following guidelines:

- By default, the Trusted Platform Module is enabled as TPM 2.0 when the server is powered on after installing it.

- In UEFI Boot Mode, the Trusted Platform Module can be configured to operate as TPM 2.0 or TPM 1.2.

- In Legacy Boot Mode, the Trusted Platform Module configuration can be changed between TPM 1.2 and TPM 2.0, but only TPM 1.2 operation is supported.

Enabling the Trusted Platform Module as TPM 2.0

Procedure

1. During the server startup sequence, press the **F9** key to access **System Utilities**.

2. From the System Utilities screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Trusted Platform Module options**.

3. Verify the following:

   - "Current TPM Type" is set to **TPM 2.0**.

   - "Current TPM State" is set to **Present and Enabled**.

   - "TPM Visibility" is set to **Visible**.

4. If changes were made in the previous step, press the **F10** key to save your selection.

5. If F10 was pressed in the previous step, do one of the following:

   - If in graphical mode, click **Yes**.

   - If in text mode, press the **Y** key.

6. Press the **ESC** key to exit System Utilities.

7. If changes were made and saved, the server prompts for reboot request. Press the **Enter** key to confirm reboot.

   If the following actions were performed, the server reboots a second time without user input. During this reboot, the TPM setting becomes effective.

   - Changing from TPM 1.2 and TPM 2.0

   - Changing TPM bus from FIFO to CRB

   - Enabling or disabling TPM

   - Clearing the TPM

8. Enable TPM functionality in the OS, such as Microsoft Windows BitLocker or measured boot.

   For more information, see the **Microsoft website**.

Enabling the Trusted Platform Module as TPM 1.2

Procedure

1. During the server startup sequence, press the **F9** key to access **System Utilities**.

2. From the System Utilities screen select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Trusted Platform Module options**.

3. Change the "TPM Mode Switch Operation" to **TPM 1.2**.

4. Verify "TPM Visibility" is **Visible**.

5. Press the **F10** key to save your selection.

6. When prompted to save the change in System Utilities, do one of the following:

   - If in graphical mode, click **Yes**.

   - If in text mode, press the **Y** key.

7. Press the **ESC** key to exit System Utilities.

   The server reboots a second time without user input. During this reboot, the TPM setting becomes effective.

8. Enable TPM functionality in the OS, such as Microsoft Windows BitLocker or measured boot.

   For more information, see the **Microsoft website**.

Retaining the recovery key/password

The recovery key/password is generated during BitLocker setup, and can be saved and printed after BitLocker is enabled. When using BitLocker, always retain the recovery key/password. The recovery key/password is required to enter Recovery Mode after BitLocker detects a possible compromise of system integrity.

To help ensure maximum security, observe the following guidelines when retaining the recovery key/password:

- Always store the recovery key/password in multiple locations.

- Always store copies of the recovery key/password away from the server.

- Do not save the recovery key/password on the encrypted hard drive.

Cabling

SUV cable connectors

⚠ **CAUTION:** Before disconnecting the SUV cable from the connector, always squeeze the release buttons on the sides of the connector. Failure to do so can result in damage to the equipment.
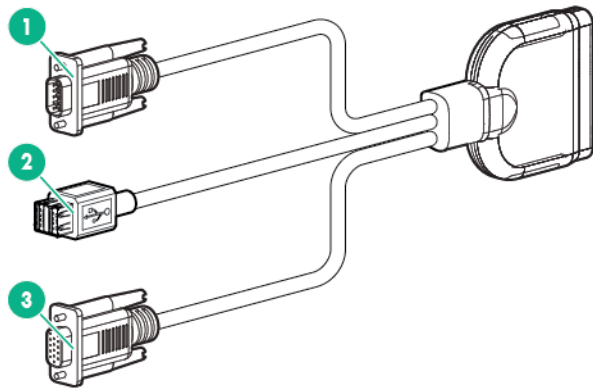
Item	Connector	Description
1	Serial	For trained personnel to connect a null modem serial cable and perform advanced diagnostic procedures
2	USB[1]	For connecting up to two USB 2.0 devices
3	Video	For connecting a video monitor

[1] The USB connectors on the SUV cable do not support devices that require greater than a 500mA power source.

Front I/O and USB board cabling
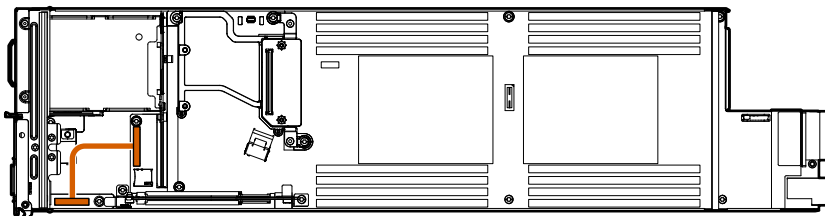
Controller cabling
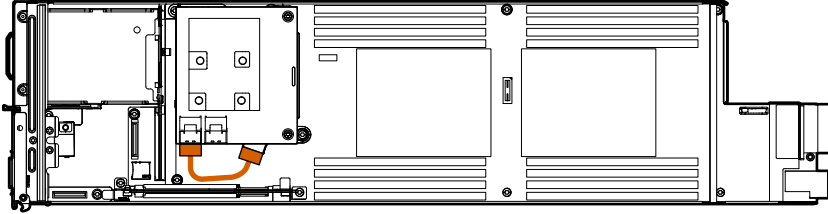
For more information about controller cabling, see the *HPE Apollo 4510 Gen10 Chassis Maintenance and Service Guide* in the **Hewlett Packard Enterprise Information Library**.

Software and configuration utilities

Server mode

The software and configuration utilities presented in this section operate in online mode, offline mode, or in both modes.

Software or configuration utility	Server mode
Active Health System on page 39	Online and Offline
HPE iLO 5 on page 39	Online and Offline
HPE Smart Storage Administrator on page 46	Online and Offline
iLO RESTful API on page 41	Online and Offline
Intelligent Provisioning on page 42	Online and Offline
Scripting Toolkit for Windows and Linux on page 43	Online
Service Pack for ProLiant on page 48	Online and Offline
Smart Update Manager on page 49	Online and Offline
UEFI System Utilities on page 44	Offline
HPE MR Storage Administrator on page 47	Offline
StorCLI on page 47	Offline

Product QuickSpecs

For more information about product features, specifications, options, configurations, and compatibility, see the product QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/qs**).

Active Health System Viewer

Active Health System Viewer (AHSV) is an online tool used to read, diagnose, and resolve server issues quickly using AHS uploaded data. AHSV provides Hewlett Packard Enterprise recommended repair actions based on experience and best practices. AHSV provides the ability to:

- Read server configuration information

- View Driver/Firmware inventory

- Review Event Logs

- Respond to Fault Detection Analytics alerts

- Open new and update existing support cases

Active Health System

The Active Health System monitors and records changes in the server hardware and system configuration.

The Active Health System provides:

- Continuous health monitoring of over 1600 system parameters

- Logging of all configuration changes

- Consolidated health and service alerts with precise time stamps

- Agentless monitoring that does not affect application performance

For more information about the Active Health System, see the iLO user guide at the following website: **http://www.hpe.com/support/ilo-docs**.

Active Health System data collection

The Active Health System does not collect information about your operations, finances, customers, employees, or partners.

Examples of information that is collected:

- Server model and serial number

- Processor model and speed

- Storage capacity and speed

- Memory capacity and speed

- Firmware/BIOS and driver versions and settings

The Active Health System does not parse or change OS data from third-party error event log activities (for example, content created or passed through the OS).

Active Health System Log

The data collected by the Active Health System is stored in the Active Health System Log. The data is logged securely, isolated from the operating system, and separate from customer data. Host resources are not consumed in the collection and logging of Active Health System data.

When the Active Health System Log is full, new data overwrites the oldest data in the log.

It takes less than 5 minutes to download the Active Health System Log and send it to a support professional to help you resolve an issue.

When you download and send Active Health System data to Hewlett Packard Enterprise, you agree to have the data used for analysis, technical resolution, and quality improvements. The data that is collected is managed according to the privacy statement, available at **http://www.hpe.com/info/privacy**.

You can also upload the log to the Active Health System Viewer. For more information, see the Active Health System Viewer documentation at the following website: **http://www.hpe.com/support/ahsv-docs**.

HPE iLO 5

iLO 5 is a remote server management processor embedded on the system boards of HPE ProLiant servers and Synergy compute modules. iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely. iLO (Standard) comes preconfigured on Hewlett Packard Enterprise servers without an additional cost or license.

Features that enhance server administrator productivity and additional new security features are licensed. For more information, see the iLO licensing guide at the following website: **http://www.hpe.com/support/ilo-docs**.

For more information about iLO, see the iLO user guide at the following website: **http://www.hpe.com/support/ilo-docs**.

iLO Federation

iLO Federation enables you to manage multiple servers from one system using the iLO web interface.

When configured for iLO Federation, iLO uses multicast discovery and peer-to-peer communication to enable communication between the systems in iLO Federation groups.

When you navigate to one of the iLO Federation pages, a data request is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all data for the selected iLO Federation group is retrieved.

iLO supports the following features:

- Group health status—View server health and model information.

- Group Virtual Media—Connect URL-based media for access by a group of servers.

- Group power control—Manage the power status of a group of servers.

- Group power capping—Set dynamic power caps for a group of servers.

- Group firmware update—Update the firmware of a group of servers.

- Group license installation—Enter a license key to activate iLO licensed features on a group of servers.

- Group configuration—Add iLO Federation group memberships for multiple iLO systems.

Any user can view information on iLO Federation pages, but a license is required for using the following features: Group Virtual Media, Group power control, Group power capping, Group configuration, and Group firmware update.

For more information about iLO Federation, see the iLO user guide at the following website: **http://www.hpe.com/support/ilo-docs**.

iLO Service Port

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

To find out if your server model supports this feature, see the server specifications document at the following website: **http://www.hpe.com/info/qs**.

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

- Download the Active Health System Log to a supported USB flash drive.

  When you use this feature, the connected USB flash drive is not accessible by the host operating system.

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

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

  Some servers, such as the XL170r, require an adapter to connect a USB to Ethernet adapter to the iLO Service Port.

Hewlett Packard Enterprise recommends the HPE Micro USB to USB Adapter (part number 789904-B21).

When you use the iLO Service Port:

- Actions are logged in the iLO Event Log.

- The server UID flashes to indicate the Service Port status.

  You can also retrieve the Service Port status by using a REST client and the iLO RESTful API.

- You cannot use the Service Port to boot any device within the server, or the server itself.

- You cannot access the server by connecting to the Service Port.

- You cannot access the connected device from the server.

For more information about the iLO Service Port, see the iLO user guide at the following website: **http://www.hpe.com/support/ilo-docs**.

iLO RESTful API

iLO includes the iLO RESTful API, which is Redfish API conformant. The iLO RESTful API is a management interface that server management tools can use to perform configuration, inventory, and monitoring tasks by sending basic HTTPS operations (GET, PUT, POST, DELETE, and PATCH) to the iLO web server.

To learn more about the iLO RESTful API, see the Hewlett Packard Enterprise website (**http://www.hpe.com/support/restfulinterface/docs**).

For specific information about automating tasks using the iLO RESTful API, see libraries and sample code at **http://www.hpe.com/info/redfish**.

 For more information, watch the **Redfish & How it works with HPE Server Management** video.

RESTful Interface Tool

The RESTful Interface Tool (iLOREST) is a scripting tool that allows you to automate HPE server management tasks. It provides a set of simplified commands that take advantage of the iLO RESTful API. You can install the tool on your computer for remote use or install it locally on a server with a Windows or Linux Operating System. The RESTful Interface Tool offers an interactive mode, a scriptable mode, and a file-based mode similar to CONREP to help decrease automation times.

For more information, see the following website: **http://www.hpe.com/info/resttool**.

iLO Amplifier Pack

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

For more information about iLO Amplifier Pack, see the *iLO Amplifier Pack User Guide* at the following website: **http://www.hpe.com/support/ilo-ap-ug-en**.

Integrated Management Log

The IML records hundreds of events and stores them in an easy-to-view form. The IML timestamps each event with one-minute granularity.

You can view recorded events in the IML in several ways, including the following:

- From within HPE SIM

- From within the UEFI System Utilities

- From within the Embedded UEFI shell

- From within the iLO web interface

Intelligent Provisioning

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

Intelligent Provisioning 3.30 and later includes HPE SMB Setup. When you launch F10 mode from the POST screen, you are prompted to select whether you want to enter the Intelligent Provisioning or HPE SMB Setup mode.

NOTE: After you have selected a mode, you must reprovision the server to change the mode that launches when you boot to F10.

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

ⓘ **IMPORTANT:** HPE ProLiant XL servers do not support operating system installation with Intelligent Provisioning, but they do support the maintenance features. For more information, see "Performing Maintenance" in the Intelligent Provisioning user guide and online help.

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

To access Intelligent Provisioning:

- Press **F10** from the POST screen and enter either Intelligent Provisioning or HPE SMB Setup.

- From the iLO web interface using **Always On**. **Always On** allows you to access Intelligent Provisioning without rebooting your server.

Intelligent Provisioning operation

Intelligent Provisioning includes the following components:

- Critical boot drivers

- Active Health System (AHS)

- Erase Utility

- Deployment Settings

> **IMPORTANT:**
>
> - Although your server is preloaded with firmware and drivers, Hewlett Packard Enterprise recommends updating the firmware upon initial setup. Also, downloading and updating the latest version of Intelligent Provisioning ensures the latest supported features are available.
>
> - For ProLiant servers, firmware is updated using the Intelligent Provisioning Firmware Update utility.
>
> - Do not update firmware if the version you are currently running is required for compatibility.

NOTE: Intelligent Provisioning does not function within multihomed configurations. A multihomed host is one that is connected to two or more networks or has two or more IP addresses.

Intelligent Provisioning provides installation help for the following operating systems:

- Microsoft Windows Server

- Red Hat Enterprise Linux

- SUSE Linux Enterprise Server

- VMware ESXi/vSphere Custom Image

- ClearOS

Not all versions of an OS are supported. For information about specific versions of a supported operating system, see the OS Support Matrix on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/ossupport**).

Management Security

HPE ProLiant Gen10 servers are built with some of the industry's most advanced security capabilities, out of the box, with a foundation of secure embedded management applications and firmware. The management security provided by HPE embedded management products enables secure support of modern workloads, protecting your components from unauthorized access and unapproved use. The range of embedded management and optional software and firmware available with the iLO Advanced and iLO Advanced Premium Security Edition licenses provides security features that help ensure protection, detection, and recovery from advanced cyber-attacks. For more information, see the *HPE Gen10 Server Security Reference Guide* on the Hewlett Packard Enterprise Information Library at **http://www.hpe.com/support/gen10-security-ref-en**.

For information about the iLO Advanced Premium Security Edition license, see **http://www.hpe.com/servers/ilopremium**.

Scripting Toolkit for Windows and Linux

The STK for Windows and Linux is a server deployment product that delivers an unattended automated installation for high-volume server deployments. The STK is designed to support ProLiant servers. The toolkit includes a modular set of utilities and important documentation that describes how to apply these tools to build an automated server deployment process.

The STK provides a flexible way to create standard server configuration scripts. These scripts are used to automate many of the manual steps in the server configuration process. This automated server configuration process cuts time from each deployment, making it possible to scale rapid, high-volume server deployments.

For more information or to download the STK, see the **Hewlett Packard Enterprise website**.

UEFI System Utilities

The UEFI System Utilities is embedded in the system ROM. Its features enable you to perform a wide range of configuration activities, including:

- Configuring system devices and installed options.

- Enabling and disabling system features.

- Displaying system information.

- Selecting the primary boot controller or partition.

- Configuring memory options.

- Launching other preboot environments.

HPE servers with UEFI can provide:

- Support for boot partitions larger than 2.2 TB. Such configurations could previously only be used for boot drives when using RAID solutions.

- Secure Boot that enables the system firmware, option card firmware, operating systems, and software collaborate to enhance platform security.

- UEFI Graphical User Interface (GUI)

- An Embedded UEFI Shell that provides a preboot environment for running scripts and tools.

- Boot support for option cards that only support a UEFI option ROM.

Selecting the boot mode

This server provides two **Boot Mode** configurations: UEFI Mode and Legacy BIOS Mode. Certain boot options require that you select a specific boot mode. By default, the boot mode is set to **UEFI Mode**. The system must boot in **UEFI Mode** to use certain options, including:

- Secure Boot, UEFI Optimized Boot, Generic USB Boot, IPv6 PXE Boot, iSCSI Boot, and Boot from URL

- Fibre Channel/FCoE Scan Policy

NOTE: The boot mode you use must match the operating system installation. If not, changing the boot mode can impact the ability of the server to boot to the installed operating system.

Prerequisite

When booting to **UEFI Mode**, leave **UEFI Optimized Boot** enabled.

Procedure

1. From the **System Utilities** screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **Boot Mode**.

2. Select a setting.

- **UEFI Mode** (default)—Configures the system to boot to a UEFI compatible operating system.

- **Legacy BIOS Mode**—Configures the system to boot to a traditional operating system in Legacy BIOS compatibility mode.

3. Save your setting.

4. Reboot the server.

Secure Boot

Secure Boot is a server security feature that is implemented in the BIOS and does not require special hardware. Secure Boot ensures that each component launched during the boot process is digitally signed and that the signature is validated against a set of trusted certificates embedded in the UEFI BIOS. Secure Boot validates the software identity of the following components in the boot process:

- UEFI drivers loaded from PCIe cards

- UEFI drivers loaded from mass storage devices

- Preboot UEFI Shell applications

- OS UEFI boot loaders

When Secure Boot is enabled:

- Firmware components and operating systems with boot loaders must have an appropriate digital signature to execute during the boot process.

- Operating systems must support Secure Boot and have an EFI boot loader signed with one of the authorized keys to boot. For more information about supported operating systems, see **http://www.hpe.com/servers/ossupport**.

You can customize the certificates embedded in the UEFI BIOS by adding or removing your own certificates, either from a management console directly attached to the server, or by remotely connecting to the server using the iLO Remote Console.

You can configure Secure Boot:

- Using the **System Utilities** options described in the following sections.

- Using the iLO RESTful API to clear and restore certificates. For more information, see the Hewlett Packard Enterprise website (**http://www.hpe.com/info/redfish**).

- Using the `secboot` command in the Embedded UEFI Shell to display Secure Boot databases, keys, and security reports.

Launching the Embedded UEFI Shell

Use the **Embedded UEFI Shell** option to launch the Embedded UEFI Shell. The Embedded UEFI Shell is a preboot command-line environment for scripting and running UEFI applications, including UEFI boot loaders. The Shell also provides CLI-based commands you can use to obtain system information, and to configure and update the system BIOS.

Prerequisites

Embedded UEFI Shell is set to **Enabled**.

Procedure

1. From the **System Utilities** screen, select **Embedded Applications** > **Embedded UEFI Shell**.

   The **Embedded UEFI Shell** screen appears.

2. Press any key to acknowledge that you are physically present.

   This step ensures that certain features, such as disabling **Secure Boot** or managing the **Secure Boot** certificates using third-party UEFI tools, are not restricted.

3. If an administrator password is set, enter it at the prompt and press **Enter**.

   The `Shell>` prompt appears.

4. Enter the commands required to complete your task.

5. Enter the `exit` command to exit the Shell.

HPE Smart Storage Administrator

HPE SSA is the main tool for configuring arrays on HPE Smart Array SR controllers. It exists in three interface formats: the HPE SSA GUI, the HPE SSA CLI, and HPE SSA Scripting. All formats provide support for configuration tasks. Some of the advanced tasks are available in only one format.

The diagnostic features in HPE SSA are also available in the standalone software HPE Smart Storage Administrator Diagnostics Utility CLI.

During the initial provisioning of the server or compute module, an array is required to be configured before the operating system can be installed. You can configure the array using SSA.

HPE SSA is accessible both offline (either through HPE Intelligent Provisioning or as a standalone bootable ISO image) and online:

- Accessing HPE SSA in the offline environment

  (!) **IMPORTANT:** If you are updating an existing server in an offline environment, obtain the latest version of HPE SSA through Service Pack for ProLiant before performing configuration procedures.

  Using one of multiple methods, you can run HPE SSA before launching the host operating system. In offline mode, users can configure or maintain detected and supported devices, such as optional Smart Array controllers and integrated Smart Array controllers. Some HPE SSA features are only available in the offline environment, such as setting the boot controller and boot volume.

- Accessing HPE SSA in the online environment

  This method requires an administrator to download the HPE SSA executables and install them. You can run HPE SSA online after launching the host operating system.

For more information, see *HPE Smart Array SR Gen10 Configuration Guide* at the **Hewlett Packard Enterprise website**.

HPE MR Storage Administrator

HPE MR Storage Administrator is a web-based application that enables you to monitor, maintain, troubleshoot, and configure the HPE Smart Array MR controller. MR Storage Administrator helps you to view, create, and manage storage configurations.

- **Monitoring and Configuring**: MR Storage Administrator enables you to monitor the controllers and configure the drives on the controller. It displays the status of the controller cards, logical drives, and drives on the controller. The device status icons notify you if there are drive failures and other events that require your immediate attention. Email notifications about the status of the server are sent based on your alert settings. The system errors and events are recorded and displayed in an event log file. You can also import or clear foreign configurations.

- **Maintaining**: Using MR Storage Administrator, you can perform system maintenance tasks, such as updating the controller firmware.

- **Troubleshooting**: MR Storage Administrator displays information related to drive failures, device failures, and other issues. It also provides recommendations and displays contextual links, helping you to locate the drives/devices that have issues and troubleshoot them. You can also download a report of the devices and their configurations, properties, and settings and send it to Hewlett Packard Enterprise Support for further troubleshooting.

Obtain MR Storage Administrator installation files through the Service Pack for ProLiant, or SPP, which you can download from **http://www.hpe.com/servers/spp/download**. Be sure to use the latest SPP version for the server.

For more information about the MR Storage Administrator, see *MR Storage Administrator User Guide* on the Hewlett Packard Enterprise website **http://www.hpe.com/info/P824i-pdocs**.

HPE InfoSight for servers overview

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

HPE InfoSight for servers:

- Combines the machine learning and predictive analytics of HPE InfoSight with the health and performance monitoring of Active Health System (AHS) and HPE iLO to optimize performance and predict and prevent problems

- Provides automatic collection and analysis of the sensor and telemetry data from AHS to derive insights from the behaviors of the install base to provide recommendations to resolve problems and improve performance

For more information on getting started and using HPE InfoSight for servers, go to: **https://www.hpe.com/support/infosight-servers-docs.**

StorCLI

The Storage Command Line Interface (StorCLI) tool is the command line management software designed for the HPE Smart Array MR controller. StorCLI is a command line interface that is designed to be easy to use, consistent, and easy to script.

Obtain StorCLI through the Service Pack for ProLiant, or SPP, which you can download from **http://www.hpe.com/servers/spp/download**. Be sure to use the latest SPP version for the server.

For more information about StorCLI, see *StorCLI User Guide* on the Hewlett Packard Enterprise website **http://www.hpe.com/info/P824i-pdocs**.

USB support

Hewlett Packard Enterprise Gen10 servers support all USB operating speeds depending on the device that is connected to the server.

External USB functionality

Hewlett Packard Enterprise provides external USB support to enable local connection of USB devices for server administration, configuration, and diagnostic procedures.

For additional security, external USB functionality can be disabled through USB options in UEFI System Utilities.

Redundant ROM support

The server enables you to upgrade or configure the ROM safely with redundant ROM support. The server has a single ROM that acts as two separate ROM images. In the standard implementation, one side of the ROM contains the current ROM program version, while the other side of the ROM contains a backup version.

NOTE: The server ships with the same version programmed on each side of the ROM.

Safety and security benefits

When you flash the system ROM, the flashing mechanism writes over the backup ROM and saves the current ROM as a backup, enabling you to switch easily to the alternate ROM version if the new ROM becomes corrupted for any reason. This feature protects the existing ROM version, even if you experience a power failure while flashing the ROM.

Keeping the system current

Updating firmware or system ROM

To update firmware or system ROM, use one of the following methods:

- The **Firmware Update** option in the System Utilities.
- The `fwupdate` command in the **Embedded UEFI Shell**.
- Service Pack for ProLiant (SPP)
- HPE online flash components
- Moonshot Component Pack

Service Pack for ProLiant

SPP is a systems software and firmware solution delivered as a single ISO file download. This solution uses SUM as the deployment tool and is tested and supports HPE ProLiant, HPE BladeSystem, HPE Synergy, and HPE Apollo servers and infrastructure.

SPP, along with SUM and iSUT, provides Smart Update system maintenance tools that systematically update HPE ProLiant, HPE BladeSystem, HPE Synergy, and HPE Apollo servers and infrastructure.

SPP can be used in an online mode on a server running Windows, Linux, or VMware vSphere ESXi, or in an offline mode where the server is booted to an operating system included in the ISO file.

The preferred method for downloading an SPP is using the SPP Custom Download at **https://www.hpe.com/servers/spp/custom**.

The SPP is also available for download from the SPP download page at **https://www.hpe.com/servers/spp/download**.

Smart Update Manager

SUM is an innovative tool for maintaining and updating the firmware, drivers, and system software of HPE ProLiant, HPE BladeSystem, HPE Synergy, and HPE Apollo servers, infrastructure, and associated options.

SUM identifies associated nodes you can update at the same time to avoid interdependency issues.

Key features of SUM include:

- Discovery engine that finds installed versions of hardware, firmware, and software on nodes.
- SUM deploys updates in the correct order and ensures that all dependencies are met before deploying an update.
- Interdependency checking.
- Automatic and step-by-step Localhost Guided Update process.
- Web browser-based user interface.
- Ability to create custom baselines and ISOs.
- Support for iLO Repository (Gen10 iLO 5 nodes only).
- Simultaneous firmware and software deployment for multiple remote nodes.
- Local offline firmware deployments with SPP deliverables.
- Extensive logging in all modes.

NOTE: SUM does not support third-party controllers, including flashing hard drives behind the controllers.

Integrated Smart Update Tools

Integrated Smart Update Tools (iSUT) is a software utility used with iLO 4, iLO 5, iLO Amplifier Pack, Service Pack for ProLiant (SPP), and Smart Update Manager (SUM) to stage, install, and activate firmware and driver updates.

- **iSUT**: Polls iLO to check for requests from SUM or iLO Amplifier Pack for updates through the management network and orchestrates staging, deploying, and activating updates. You can adjust the polling interval by issuing the appropriate command-line option provided by iSUT. Performs inventory on target servers, stages deployment, deploys updates, and then reboots the servers.
- **iLO 5 with integrated Smart Update** (Gen10 servers only): Performs iLO Repository-based updates by downloading the components from iLO Repository when iLO Installation Queue has the components which can be updated by iSUT.
- **iLO Amplifier Pack**: Displays available updates for servers. Communicates with iSUT (or SUT 1.x) to initiate updates using the iLO Redfish interface. iSUT reports the status of updates to iLO Amplifier Pack via iLO Restful Interface.
- **SPP**: A comprehensive systems software and firmware update solution, which is delivered as a single ISO image.
- **SUM**: A tool for firmware and driver maintenance for HPE ProLiant servers and associated options.

NOTE: SUM and iLO Amplifier Pack should not manage the same nodes.

Updating firmware from the System Utilities

Use the **Firmware Updates** option to update firmware components in the system, including the system BIOS, NICs, and storage cards.

Procedure

1. Access the System ROM Flash Binary component for your server from the Hewlett Packard Enterprise Support Center.

2. Copy the binary file to a USB media or iLO virtual media.

3. Attach the media to the server.

4. Launch the **System Utilities**, and select **Embedded Applications** > **Firmware Update**.

5. Select a device.

   The **Firmware Updates** screen lists details about your selected device, including the current firmware version in use.

6. Select **Select Firmware File**.

7. Select the flash file in the **File Explorer** list.

   The firmware file is loaded and the **Firmware Updates** screen lists details of the file in the **Selected firmware file** field.

8. Select **Image Description**, and then select a firmware image.

   A device can have multiple firmware images.

9. Select **Start firmware update**.

Updating the firmware from the UEFI Embedded Shell

Procedure

1. Access the System ROM Flash Binary component for your server from the Hewlett Packard Enterprise Support Center (**http://www.hpe.com/support/hpesc**).

2. Copy the binary file to a USB media or iLO virtual media.

3. Attach the media to the server.

4. Boot to the UEFI Embedded Shell.

5. To obtain the assigned file system volume for the USB key, enter `map -r`.

6. Change to the file system that contains the System ROM Flash Binary component for your server. Enter one of the `fsx` file systems available, such as `fs0:` or `fs1:`, and press **Enter**.

7. Use the `cd` command to change from the current directory to the directory that contains the binary file.

8. Flash the system ROM by entering `fwupdate -d BIOS -f` *filename*.

9. Reboot the server. A reboot is required after the firmware update in order for the updates to take effect and for hardware stability to be maintained.

Online Flash components

This component provides updated system firmware that can be installed directly on supported operating systems. Additionally, when used in conjunction with SUM, this Smart Component allows the user to

update firmware on remote servers from a central location. This remote deployment capability eliminates the need for the user to be physically present at the server to perform a firmware update.

Drivers

ⓘ **IMPORTANT:** Always perform a backup before installing or updating device drivers.

Update drivers using any of the following **Smart Update Solutions**:

- Download the latest Service Pack for ProLiant (includes Smart Update Manager)
- Create a custom SPP download
- Download Smart Update Manager for Linux
- Download specific drivers

  To locate the drivers for a server, go to the **Hewlett Packard Enterprise Support Center website**, and then search for the product name/number.

Software and firmware

Update software and firmware before using the server for the first time, unless any installed software or components require an older version.

For system software and firmware updates, use one of the following sources:

- Download the SPP from the Hewlett Packard Enterprise website (**http://www.hpe.com/servers/spp/download**).
- Download individual drivers, firmware, or other system software components from the server product page in the Hewlett Packard Enterprise Support Center website (**http://www.hpe.com/support/hpesc**).

Operating system version support

For information about specific versions of a supported operating system, refer to the **operating system support matrix**.

HPE Pointnext Portfolio

HPE Pointnext delivers confidence, reduces risk, and helps customers realize agility and stability. Hewlett Packard Enterprise helps customers succeed through Hybrid IT by simplifying and enriching the on-premise experience, informed by public cloud qualities and attributes.

Operational Support Services enable you to choose the right service level, length of coverage, and response time to fit your business needs. For more information, see the Hewlett Packard Enterprise website:

https://www.hpe.com/us/en/services/operational.html

Utilize the Advisory and Transformation Services in the following areas:

- Private or hybrid cloud computing
- Big data and mobility requirements

- Improving data center infrastructure

- Better use of server, storage, and networking technology

For more information, see the Hewlett Packard Enterprise website:

http://www.hpe.com/services/consulting

Proactive notifications

30 to 60 days in advance, Hewlett Packard Enterprise sends notifications to subscribed customers on upcoming:

- Hardware, firmware, and software changes

- Bulletins

- Patches

- Security alerts

You can subscribe to proactive notifications on the **Hewlett Packard Enterprise website**.

Troubleshooting

Troubleshooting resources

Troubleshooting resources are available for HPE Gen10 server products in the following documents:

- *Troubleshooting Guide for HPE ProLiant Gen10 servers* provides procedures for resolving common problems and comprehensive courses of action for fault isolation and identification, issue resolution, and software maintenance.

- *Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy* provides a list of error messages and information to assist with interpreting and resolving error messages.

- *Integrated Management Log Messages and Troubleshooting Guide for HPE ProLiant Gen10 and HPE Synergy* provides IML messages and associated troubleshooting information to resolve critical and cautionary IML events.

To access the troubleshooting resources, see the Hewlett Packard Enterprise Information Library (**http://www.hpe.com/info/gen10-troubleshooting**).
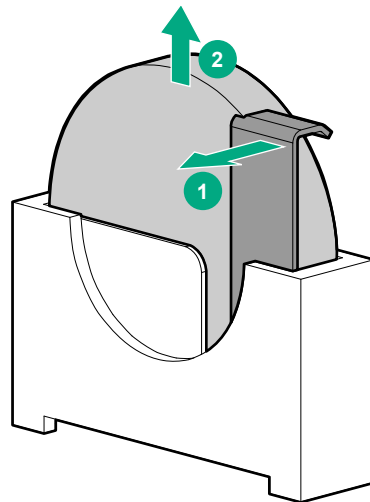
Removing and replacing the system battery

If the server no longer automatically displays the correct date and time, then replace the battery that provides power to the real-time clock. Under normal use, battery life is 5 to 10 years.

> ⚠ **WARNING:** The computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. A risk of fire and burns exists if the battery pack is not properly handled. To reduce the risk of personal injury:
>
> - Do not attempt to recharge the battery.
> - Do not expose the battery to temperatures higher than 60°C (140°F).
> - Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.
> - Replace only with the spare designated for this product.

Procedure

1. **Powering down the server** on page 14.
2. **Remove the server from the chassis** on page 14.
3. Place the server on a flat, level work surface.
4. Identify the battery location.

   For more information, see **Server components** on page 11.
5. Remove the battery.

> ⓘ **IMPORTANT:** Replacing the system board battery resets the system ROM to its default configuration. After replacing the battery, reconfigure the system through UEFI System Utilities.

To replace the component, reverse the removal procedure.

For more information about battery replacement or proper disposal, contact an authorized reseller or an authorized service provider.

Electrostatic discharge

Preventing electrostatic discharge

To prevent damaging the system, be aware of the precautions you must follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

Procedure

- Avoid hand contact by transporting and storing products in static-safe containers.

- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.

- Place parts on a grounded surface before removing them from their containers.

- Avoid touching pins, leads, or circuitry.

- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding methods to prevent electrostatic discharge

Several methods are used for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ±10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.

- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.

- Use conductive field service tools.

- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

For more information on static electricity or assistance with product installation, contact the Hewlett Packard Enterprise Support Center.

Specifications

Environmental specifications

Specification	Value
Temperature range[1]	
Operating	10°C to 35°C (50°F to 95°F)
Shipping	-40°C to 70°C (-40°F to 158°F)
Maximum wet bulb temperature	28°C (82.4°F)
Relative humidity (noncondensing)[2]	
Operating	10% to 90%
Nonoperating	5% to 95%

[1] All temperature ratings shown are for sea level. An altitude derating of 1°C per 300 m (1.8°F per 1,000 ft) to 3,048 m (10,000 ft) is applicable. No direct sunlight allowed.

[2] Storage maximum humidity of 95% is based on a maximum temperature of 45°C (113°F). Altitude maximum for storage corresponds to a pressure minimum of 70 kPa.

Server specifications

Specification	Value
Height	4.36 cm (1.72 in)
Depth	66.89 cm (26.34 in)
Width	16.56 cm (6.52 in)
Weight (fully loaded)	4.92 kg (10.85 lbs)
Weight (empty)	3.62 kg (7.9 lbs)

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Subscription Service/Support Alerts

www.hpe.com/support/e-updates

Insight Remote Support

www.hpe.com/info/insightremotesupport/docs

For additional websites, see **Support and other resources**.

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

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

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

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

Information to collect

- Technical support registration number (if applicable)

- Product name, model or version, and serial number

- Operating system name and version

- Firmware version

- Error messages

- Product-specific reports and logs

- Add-on products or components

- Third-party products or components

Accessing updates

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

- To download product updates:

  Hewlett Packard Enterprise Support Center
    www.hpe.com/support/hpesc
  Hewlett Packard Enterprise Support Center: Software downloads
    www.hpe.com/support/downloads
  Software Depot
    www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

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

  www.hpe.com/support/AccessToSupportMaterials

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

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

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

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

Remote support and Proactive Care information
HPE Get Connected
> **www.hpe.com/services/getconnected**

HPE Proactive Care services
> **www.hpe.com/services/proactivecare**

HPE Proactive Care service: Supported products list
> **www.hpe.com/services/proactivecaresupportedproducts**

HPE Proactive Care advanced service: Supported products list
> **www.hpe.com/services/proactivecareadvancedsupportedproducts**

Proactive Care customer information
Proactive Care central
> **www.hpe.com/services/proactivecarecentral**

Proactive Care service activation
> **www.hpe.com/services/proactivecarecentralgetstarted**

Warranty information

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

HPE ProLiant and IA-32 Servers and Options
> **www.hpe.com/support/ProLiantServers-Warranties**

HPE Enterprise and Cloudline Servers
> **www.hpe.com/support/EnterpriseServers-Warranties**

HPE Storage Products
> **www.hpe.com/support/Storage-Warranties**

HPE Networking Products
> **www.hpe.com/support/Networking-Warranties**

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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