Hewlett Packard Enterprise

HPE ProLiant XL230k Gen10 Server
User Guide

Abstract

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

Contents

Cabling..58

Software and configuration utilities..63

Component identification

Front panel components
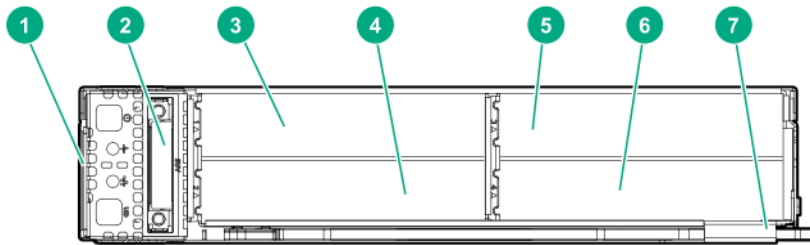
Item	Description
1	Serial number/iLO information pull tab
2	SUV connector
3	Drive bay 1
4	Drive bay 2
5	Drive bay 3
6	Drive bay 4
7	Release latch

Front panel LEDs and buttons
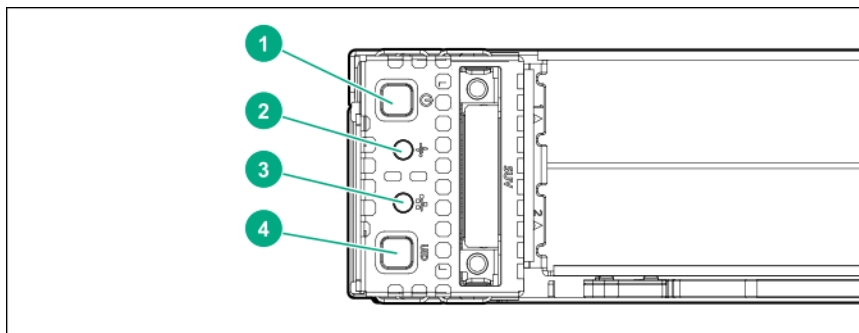
Item	Description	Status
1	Power on/Standby button and System power LED[1]	• Solid green = System on • Flashing green (1 Hz/cycle per sec) = System attempting to power on • Solid amber = System in standby • Off = No power present[2]
2	Health LED	• Solid green = Normal • Flashing green (1 Hz/cycle per sec) = iLO is rebooting. • Flashing amber = System degraded • Flashing red (1 Hz/cycle per sec) = System critical
3	NIC LED	• Solid green = Link to network • Flashing green (1 Hz/cycle per sec) = Network active • Off = No network activity
4	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 soft reboot sequence initiated ◦ 8 Hz/cycle per sec = iLO manual hard reboot sequence in progress • Off = Deactivated

[1] When all four LEDs described in this table flash simultaneously, a power fault has occurred. For more information, see "**Front panel LED power fault codes** on page 7."

[2] Facility power is not present, power cord is not attached, no power supplies are installed, power supply failure has occurred, or the power button cable is disconnected.

Front panel LED power fault codes

The following table provides a list of power fault codes, and the subsystems that are affected. Not all power faults are used by all servers.

Subsystem	LED behavior
System board	1 flash
Processor	2 flashes

Table Continued

Subsystem	LED behavior
Memory	3 flashes
Riser board PCIe slots	4 flashes
FlexibleLOM	5 flashes
Removable HPE Smart Array SR Gen10 controller	6 flashes
System board PCIe slots	7 flashes
Power backplane or storage backplane	8 flashes
Power supply	9 flashes

Hot-plug drive LED definitions
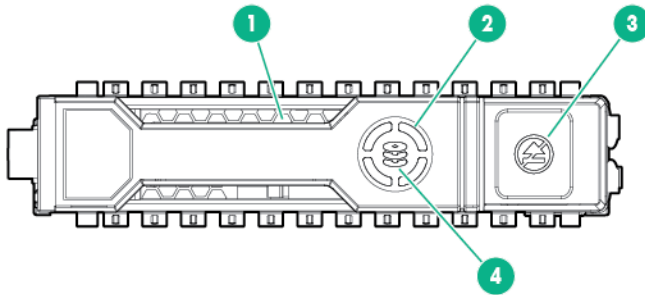
Item	LED	Status	Definition
1	Locate	Solid blue	The drive is being identified by a host application.
		Flashing blue	The drive carrier firmware is being updated or requires an update.
2	Activity ring	Rotating green	Drive activity
		Off	No drive activity
3	Do not remove	Solid white	Do not remove the drive. 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 drive components and LEDs
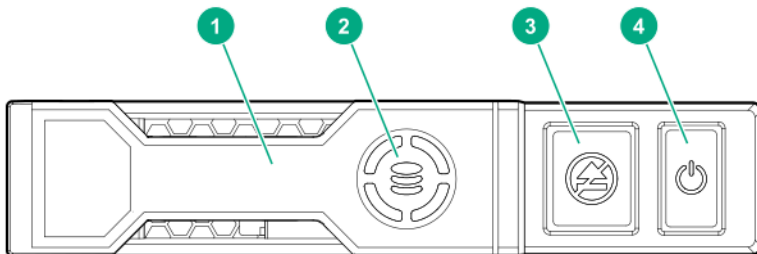
Item	Description
1	Release lever
2	Activity ring
3	Do Not Remove LED[1]
4	Request to Remove NVMe Drive button

[1]Do not remove an NVMe SSD from the drive bay while the Do Not Remove button LED is flashing. The Do Not Remove button LED flashes to indicate the device is still in use. Removal of the NVMe SSD before the device has completed and ceased signal/traffic flow can cause loss of data.

Chassis server bay numbering
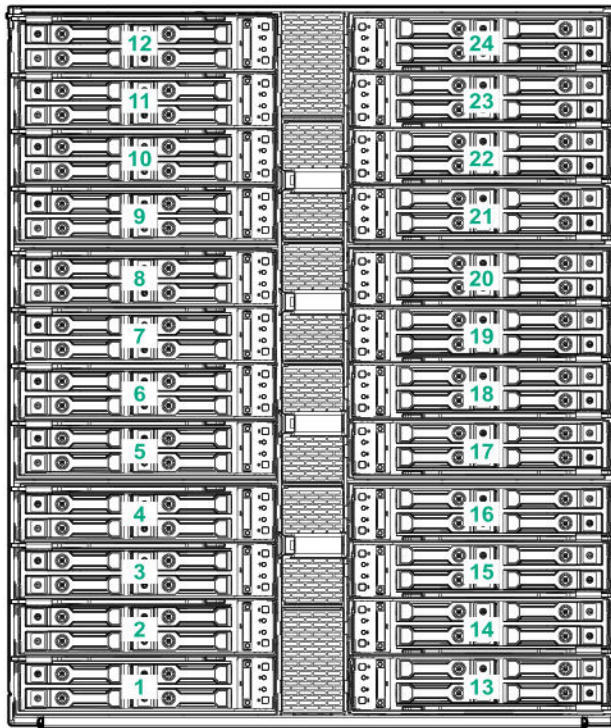
Chassis I/O module bay numbering
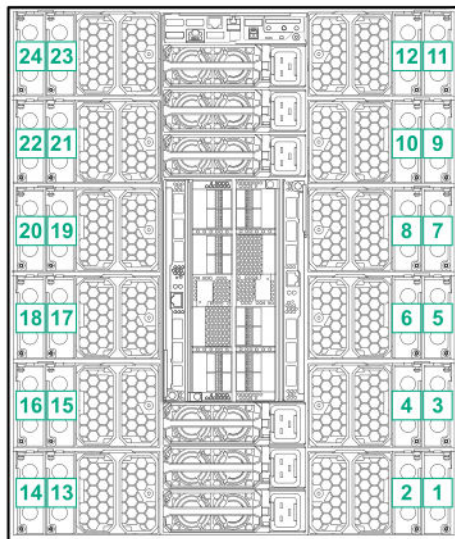
System board components
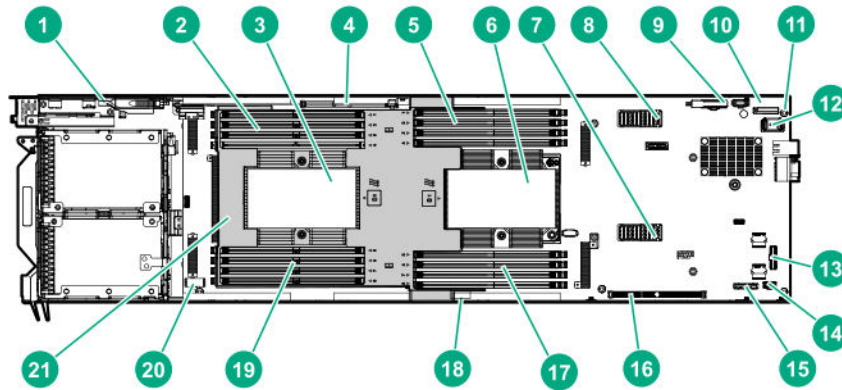
Item	Description
1	Internal USB port
2	Processor 2 DIMM slots
3	Processor 2[1]
4	NVMe riser connector[2]
5	Processor 1 DIMM slots
6	Processor 1
7	Mezzanine B connector (Processor 2)[3]
8	Mezzanine A connector (Processor 1)
9	SATA cable connector
10	Front panel USB cable connector
11	M.2 cable connector
12	Trusted Platform Module
13	Front panel SUV cable connector
14	Front panel LED cable connector
15	System battery
16	PCI riser connector
17	Processor 1 DIMM slots
18	System maintenance switch
19	Processor 2 DIMM slots
20	Drive backplane power connector
21	Required air baffle

[1] In a single processor configuration, the processor 2 socket dust cover must remain installed during operation.

[2] In a single processor configuration, NVMe is not supported.

[3] In a single processor configuration, Mezzanine B is not supported.

Processor, heatsink, and socket components
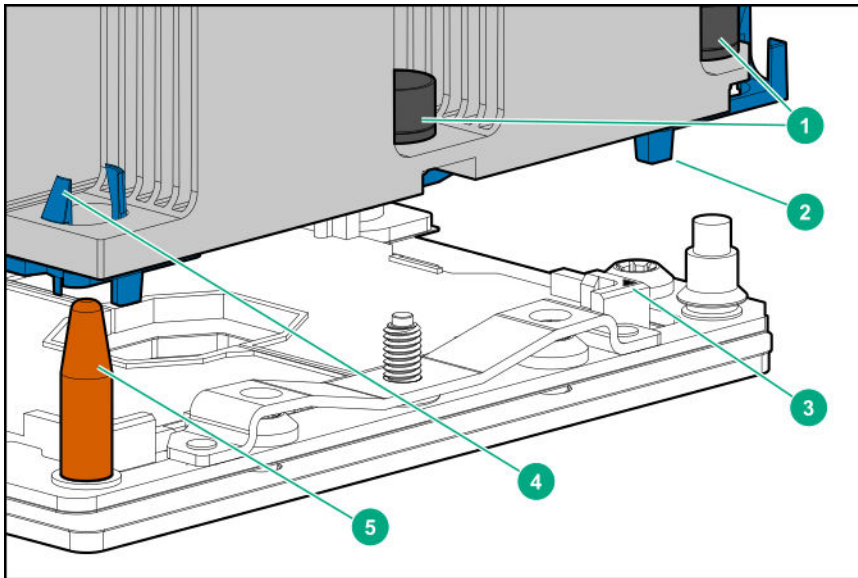
Item	Description
1	Heatsink nuts
2	Processor carrier
3	Pin 1 indicator[1]
4	Heatsink latch
5	Alignment post

[1] Symbol also on the processor and frame.

DIMM slot locations
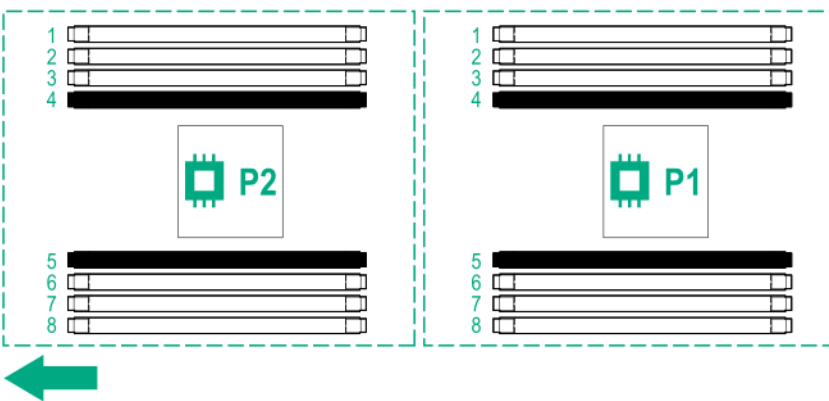
System maintenance switch descriptions

Position	Default	Function
S1 [1]	Off	Off = iLO 5 security is enabled. On = iLO 5 security is disabled.
S2	Off	Reserved
S3	Off	Reserved
S4	Off	Reserved
S5 [1]	Off	Off = Power-on password is enabled. On = Power-on password is disabled.
S6 [1, 2, 3]	Off	Off = No function On = Restore default manufacturing settings
S7	Off	Reserved
S8	—	Reserved
S9	—	Reserved
S10	—	Reserved
S11	—	Reserved
S12	—	Reserved

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

[2] When the system maintenance switch position 6 is set to the On position, the system is prepared to restore all configuration settings to their manufacturing defaults.

[3] When the system maintenance switch position 6 is set to the On position and Secure Boot is enabled, some configurations cannot be restored. For more information, see **Secure Boot** on page 68.

Setup

Setup overview

Installation of a server requires the following steps:

1. Install and configure the chassis (**Installing the chassis into a rack** on page 14).
2. Install any server options (**Installing hardware options** on page 14).
3. Install the server (**Installing the server** on page 14).
4. Power up the chassis (**Powering up the chassis** on page 15).
5. Install an operating system (**Installing the operating system** on page 15).
6. Register the product (**Registering the server** on page 15).

Installing the chassis into a rack

To install the chassis into a rack, see the *HPE Apollo k6000 Chassis User Guide* on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/Apollok6000-docs**).

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 24."

Installing the server

Always populate the chassis from bottom to top, beginning with bay 1.

> (!) **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Install the server.

   When seated properly, the server will be flush with the front of the chassis and the release lever will close easily.
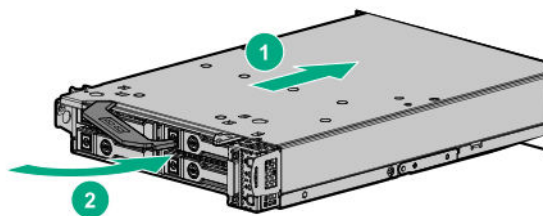
2. Press the Power On/Standby button.

   The server exits standby mode and applies full power to the system. The system power LED changes from amber to green.

Powering up the chassis

Procedure

1. Connect the AC or DC power cables, depending on the power configuration.

   When the circuit breakers are powered, the chassis and the HPE Apollo Platform Manager have power. By default, each installed component also powers up.

2. Examine the APM for any errors which may prevent installed components from powering up.

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**.

Operations

Power 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 5.

  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.

Removing the hard drive blank

> △ **CAUTION:** For proper cooling, do not operate the server without the access panel, baffles, expansion slot covers, or blanks installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

> ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Remove the component as indicated.
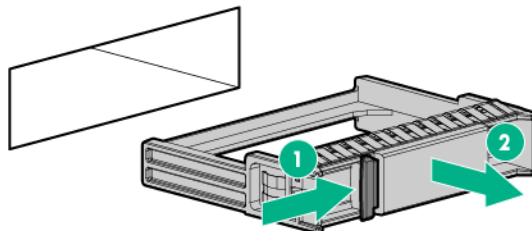
Prerequisites

Removing a hot-plug drive

△ CAUTION: For proper cooling, do not operate the server without the access panel, baffles, expansion slot covers, or blanks installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

① IMPORTANT: The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

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

2. Back up all server data on the drive.

3. Remove the drive.
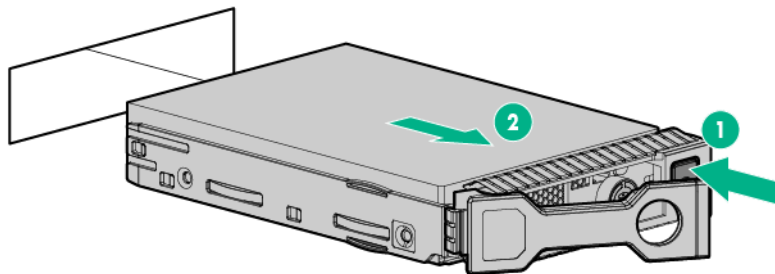
Removing the server

△ CAUTION: For proper cooling, do not operate the server without the access panel, baffles, expansion slot covers, or blanks installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

① IMPORTANT: The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server (**Power down the server** on page 16).

   The system power LED changes from green to amber.

2. Disconnect all peripheral cables from the front of the server.

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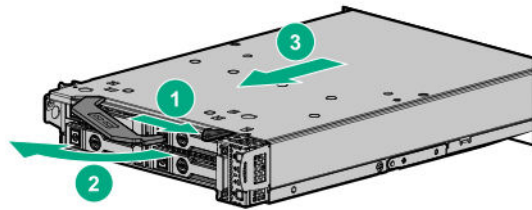
4. Place the server on a flat, level work surface.

To replace the server, reverse the removal procedure.

Removing the access panel

> **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel.
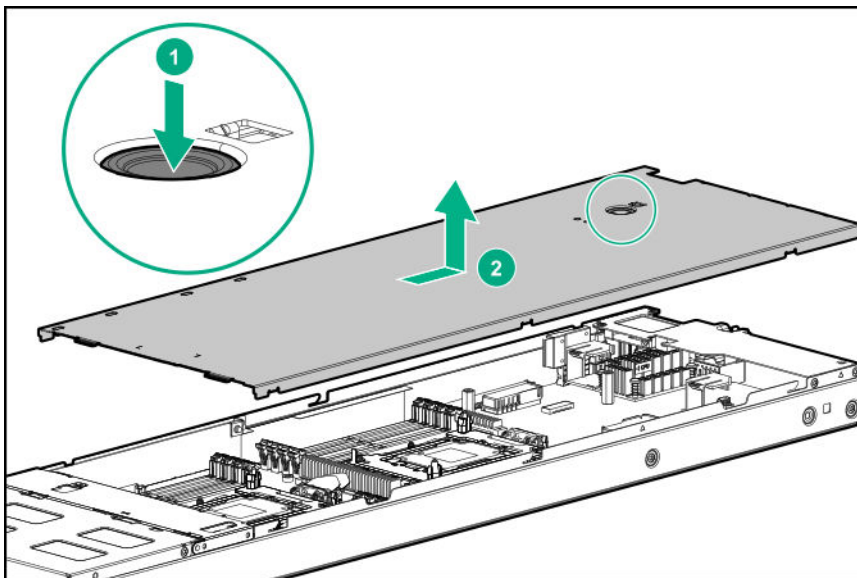
To replace the component, reverse the removal procedure.

Opening the front bracket

> **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Open the front bracket.

> **NOTE:** Depending on the server configuration, the HPE Smart Storage Battery or the M.2 enablement backplane might be installed on the front bracket.

Removing a server blank

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

> ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

Remove the component as indicated.
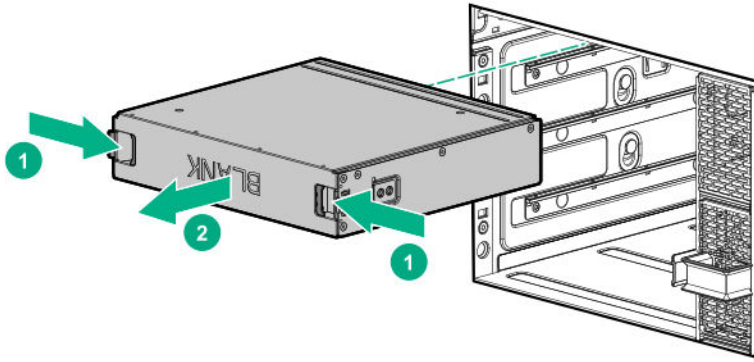
Installing a server blank

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

ⓘ IMPORTANT: The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

Install the component as indicated.
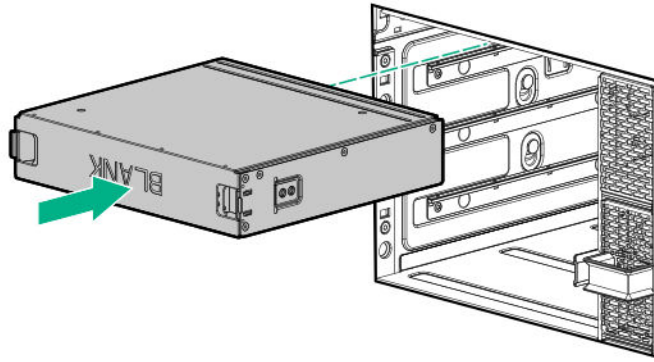
Removing the air baffle

ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Open the front bracket (**Opening the front bracket** on page 18).

6. Remove the air baffle.
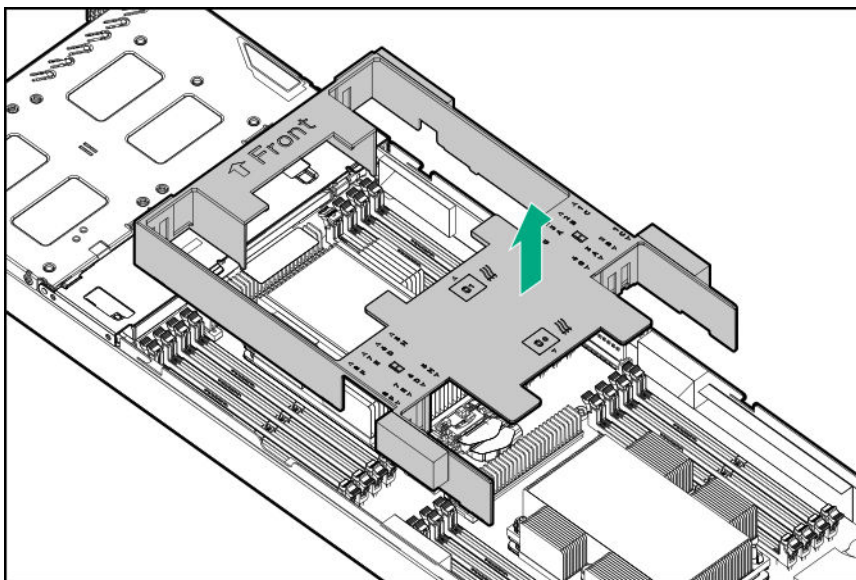
To replace the component, reverse the removal procedure.

Installing the air baffle

> ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Open the front bracket (**Opening the front bracket** on page 18).

2. Install the air baffle.
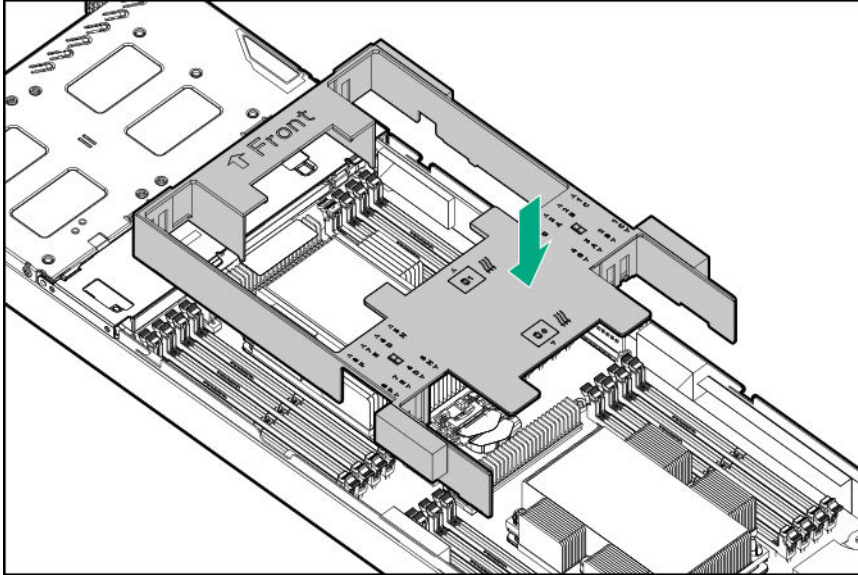
> ⓘ **IMPORTANT:** If the DIMM latches are not fully closed, the baffle will not sit properly.

> ⓘ **IMPORTANT:** Ensure that all cables are routed to the sides of the server. If the baffle will not seat properly, you may need to move the cables to their original position.

3. Close the front bracket.

4. Install the access panel.

5. Install the server into the chassis (**Installing the server** on page 14).

6. Press the Power On/Standby button.

   The server exits standby mode and applies full power to the system. The system power LED changes from amber to green.

Removing the rear support bracket
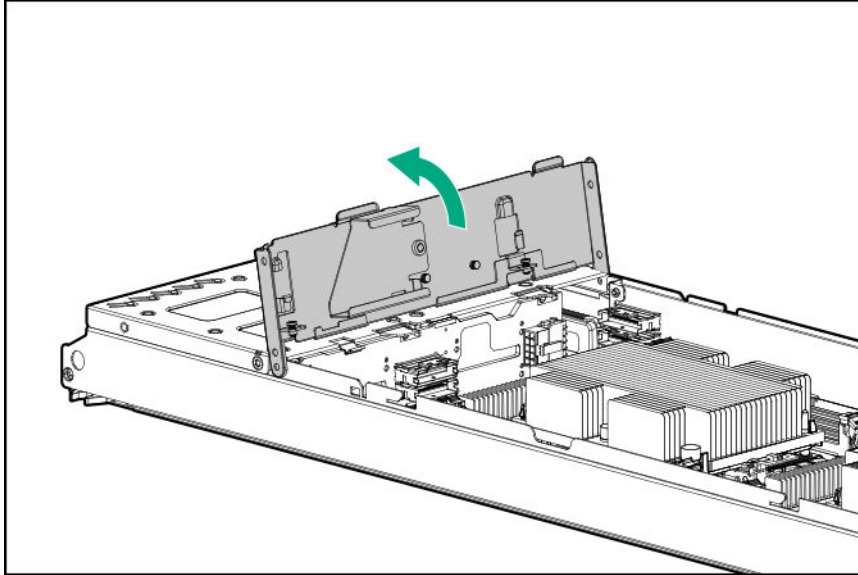
> ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Remove the rear support bracket.
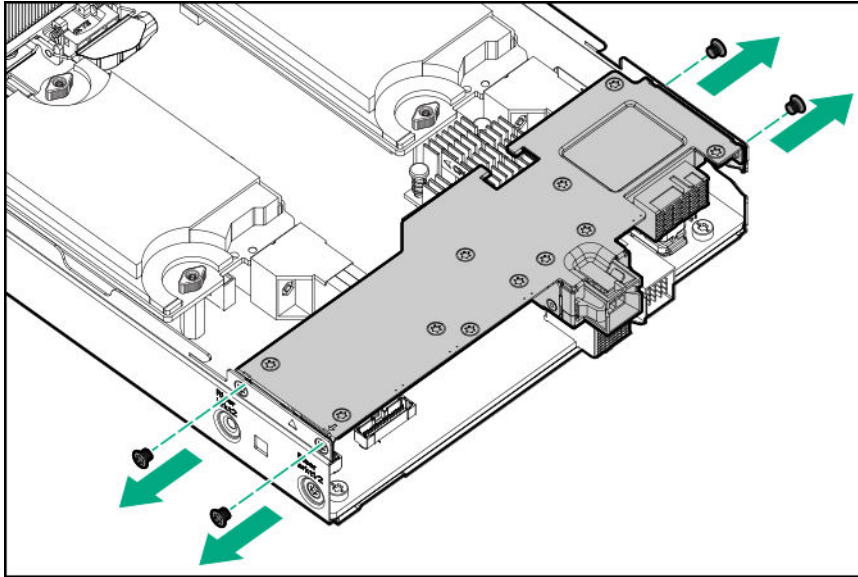
To replace the component, reverse the removal procedure.

Hardware options installation

Introduction

If more than one option is being installed, read the installation instructions for all the hardware options and identify similar steps to 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.

Drives

The server supports up to four SFF drives.

Drive guidelines

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

- The system automatically sets all device numbers.

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

- To provide the greatest storage space efficiency when drives are grouped together into the same drive array, drives must be the same capacity.

Installing a hot-plug hard drive

ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components that are installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Remove the drive blank.
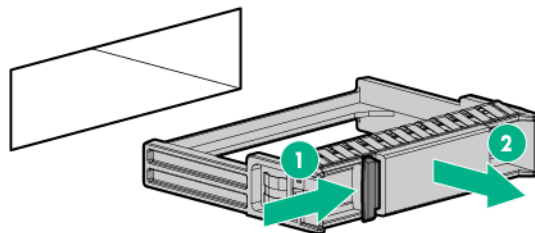
2. Prepare the drive.
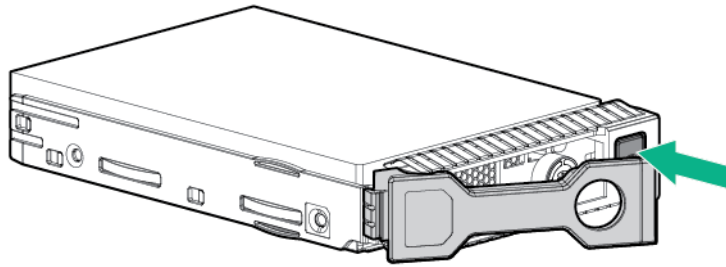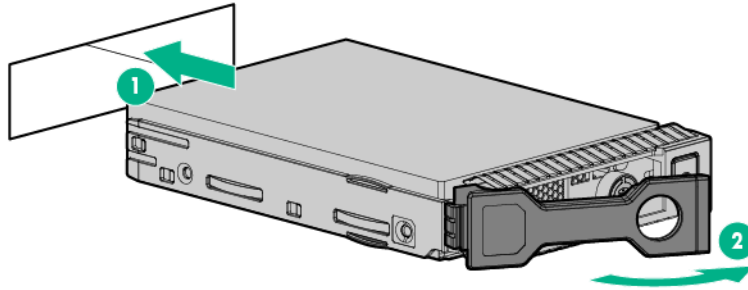
3. Install the drive.

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 server unless all drive and device bays are populated with either a component or a blank.

Procedure

1. Remove the drive blank.
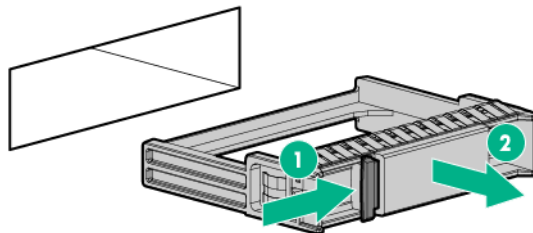
2. Prepare the drive.
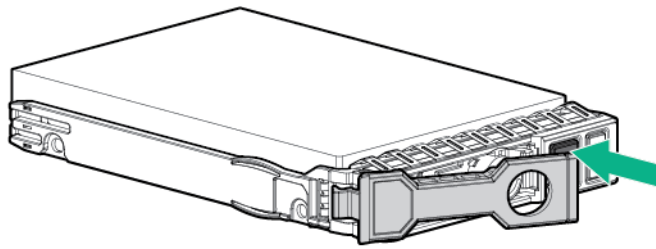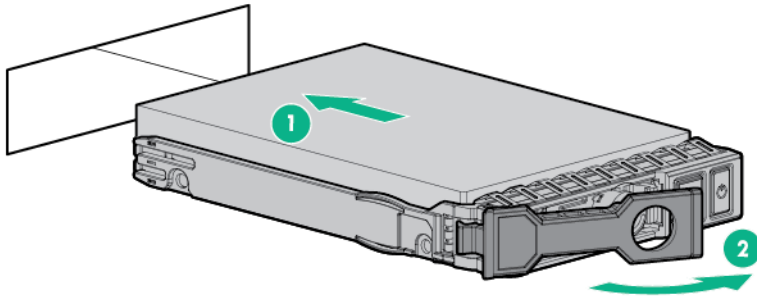
3. Install the drive.

4. Observe the LED status of the drive.

Installing a processor-heatsink assembly

Hewlett Packard Enterprise recommends identifying the processor heatsink module components before performing this procedure. See "**Processor, heatsink, and socket components** on page 12."

ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components that are installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

ⓘ **IMPORTANT:** In a single processor configuration, processor 2 is not used.

ⓘ **IMPORTANT:** HPE ProLiant and HPE Synergy Gen10 server products do not support upgrading 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**).

NOTE: Install the rear heatsink on processor 1 and the front heatsink on processor 2.

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

- The components included with the hardware option kit

- T-30 Torx screwdriver

Procedure

1. Observe the following alerts:

⚠ CAUTION: When handling the heatsink, always hold it along the top and bottom of the fins. Holding it from the sides can damage the fins.

⚠ CAUTION: To avoid damage to the processor or system board, only authorized personnel should attempt to replace or install the processor in this server.

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

⚠ CAUTION: If installing a processor with a faster speed, update the system ROM before installing the processor.

To download firmware and view installation instructions, see the **Hewlett Packard Enterprise Support Center website**.

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

2. Power down the server (**Power down the server** on page 16).

3. Remove the server (**Removing the server** on page 17).

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

5. Remove the access panel (**Removing the access panel** on page 18).

6. Open the front bracket (**Opening the front bracket** on page 18).

7. Remove the air baffle (**Removing the air baffle** on page 21).

8. Remove the processor-heatsink module:

   a. Allow the heatsink to cool.

   b. Loosen the heatsink nuts in the order specified by the label on the heatsink (4 - 3 - 2 - 1).
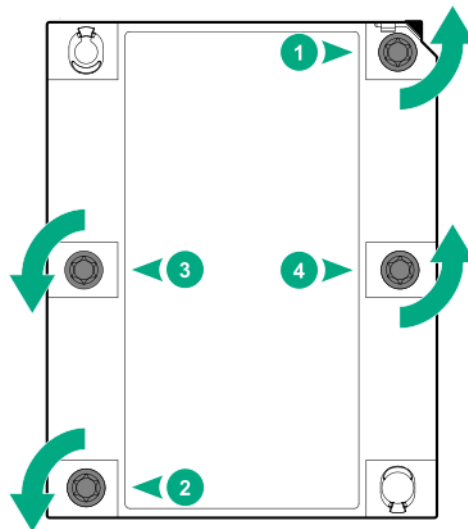
   c. Lift the processor-heatsink module, away from the system board.

d. Turn the module over and place it on a work surface with the processor facing up.

e. Install the dust cover.

9. Install the processor-heatsink assembly:

   a. Remove the dust cover.

   b. Locate the Pin 1 indicator on the processor frame and the socket.

   c. Align the processor-heatsink assembly with the 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.

   A standard heatsink is shown. Your heatsink might look different.
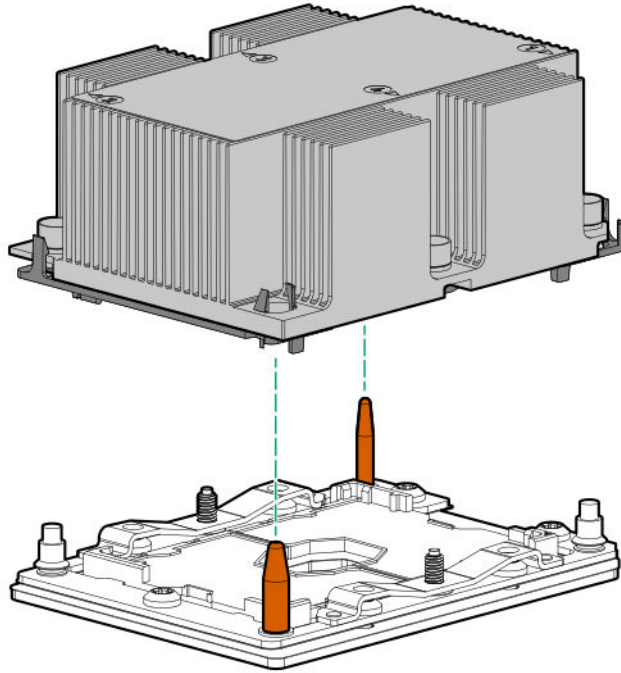
   d. Using a T-30 Torx screwdriver, tighten the nuts until they stop.
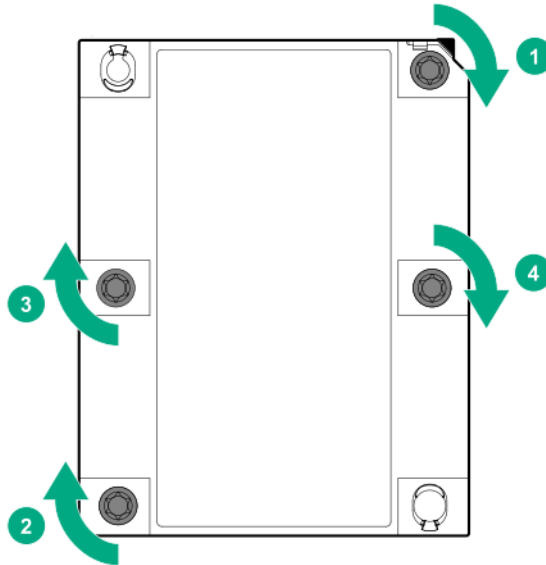
10. Install the air baffle.

11. Close the front bracket.

12. Install the access panel.

13. Install the server into the rack.

14. Connect each power cord to the server.

15. Connect each power cord to the power source.

16. Power up the server.

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.
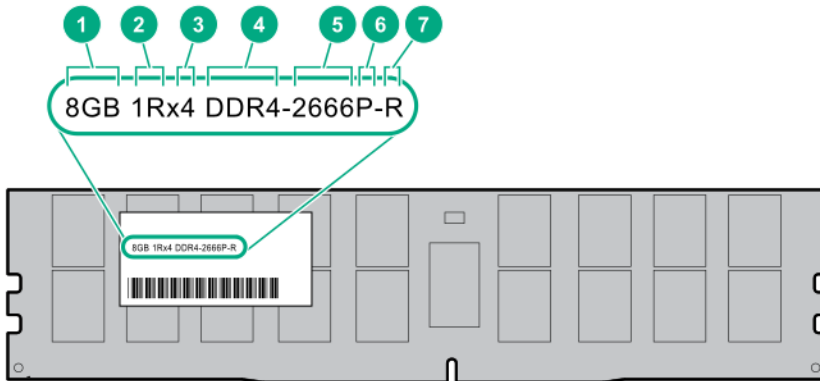
Item	Description	Example
1	Capacity	8 GB 16 GB 32 GB 64 GB 128 GB
2	Rank	1R = Single rank 2R = Dual rank 4R = Quad rank 8R = Octal rank
3	Data width on DRAM	x4 = 4-bit x8 = 8-bit x16 = 16-bit
4	Memory generation	PC4 = DDR4
5	Maximum memory speed	2133 MT/s 2400 MT/s 2666 MT/s 2933 MT/s

Table Continued

Item	Description	Example
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.

⚠ **CAUTION:** To avoid damage to the DIMM, insert it into the slot by pressing down gently on each side.

ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components that are installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Open the front bracket (**Opening the front bracket** on page 18).

6. Remove the air baffle (**Removing the air baffle** on page 21).

7. Open the DIMM slot latches.

8. Install the DIMM.
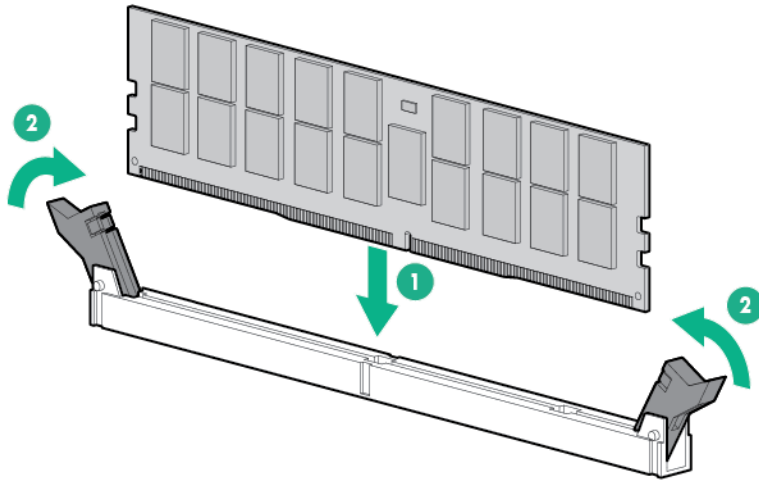
> ⓘ **IMPORTANT:** If the DIMM latches are not fully closed, the baffle will not sit properly.

9. Install the air baffle (**Installing the air baffle** on page 22).

10. Close the front bracket.

11. Install the access panel.

12. Install the server into the chassis (**Installing the server** on page 14).

13. Press the Power On/Standby button.

    The server exits standby mode and applies full power to the system. The system power LED changes from amber, to flashing green, and then to green.

To configure the memory mode, use UEFI System Utilities (see **UEFI System Utilities** on page 67).

Installing the cable retention clip

You can install an optional cable retention clip that attaches to the fabric management cable and then to the mezzanine card for additional stability.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Remove the rear support bracket (**Removing the rear support bracket** on page 22).

6. Remove the mezzanine card.
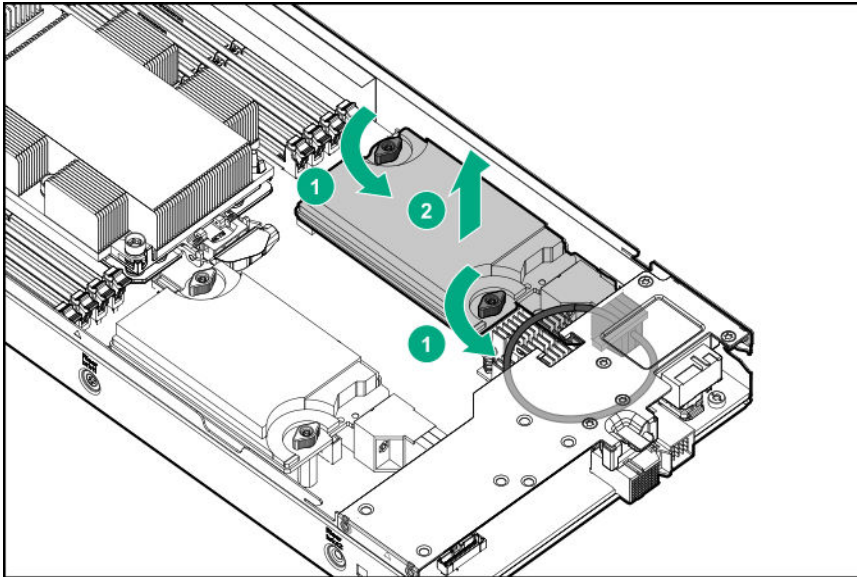
7. Center the fastener on the front edge of the cable retention clip to the cable connector.
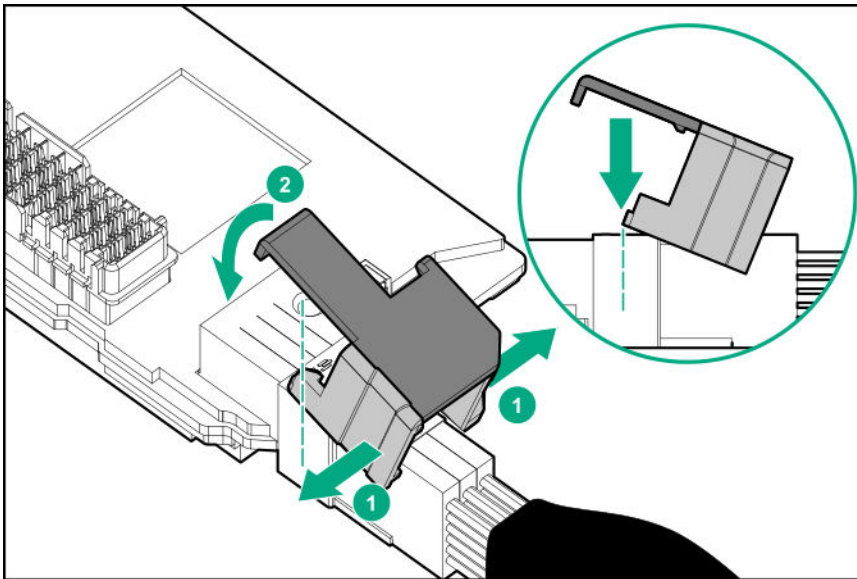
8. Slide the cable retention clip forward to lock it into place.
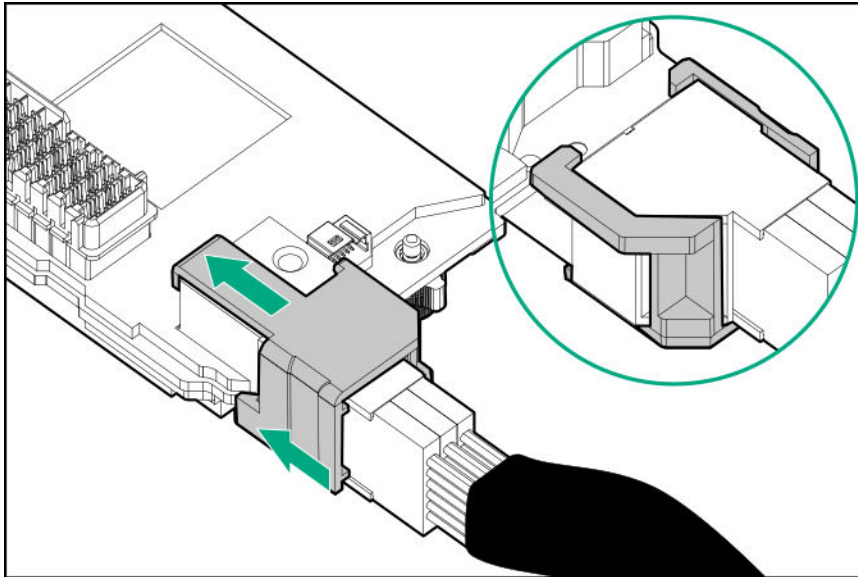
9. Ensure that the cable retention clip is aligned properly to the mezzanine card.
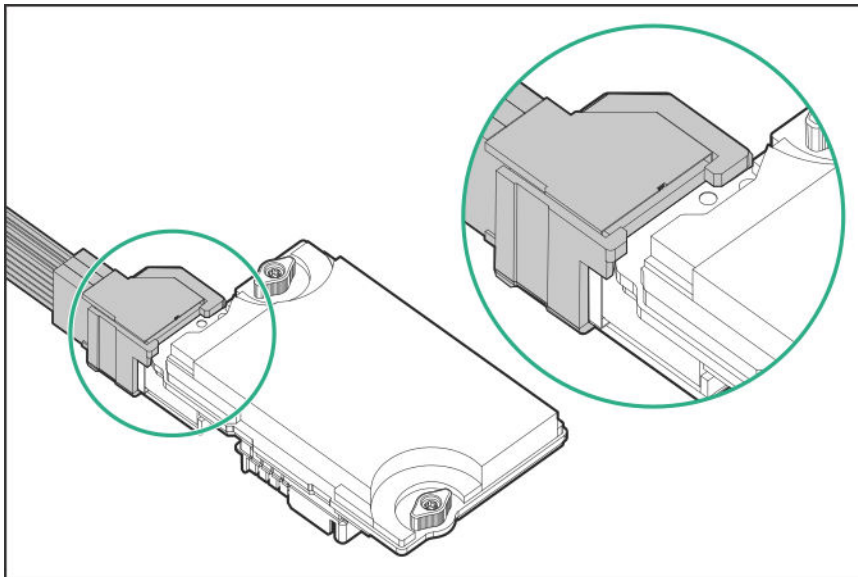
10. Install the mezzanine card (**Installing a mezzanine card** on page 34).

11. Install the rear support bracket.

12. Install the access panel (**Removing the access panel** on page 18).

13. Install the server into the chassis (**Installing the server** on page 14).

14. Press the Power On/Standby button.

   The server exits standby mode and applies full power to the system. The system power LED changes from amber, to flashing green, and then to green.

Installing a mezzanine card

ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components that are installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Observe the following requirements when installing a mezzanine card:

- Install mezzanine cards in slot A, slots A and B, or neither slot. If you are installing only one mezzanine card, install it only in slot A. See **System board components** on page 11.
- If a PCIe riser card is installed in the server, install a mezzanine card only in slot A.
- Mezzanine B is not supported in a single processor configuration.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Remove the rear support bracket (**Removing the rear support bracket** on page 22).

6. If installing the EDR mezzanine card, connect the fabric management cable to the mezzanine card.
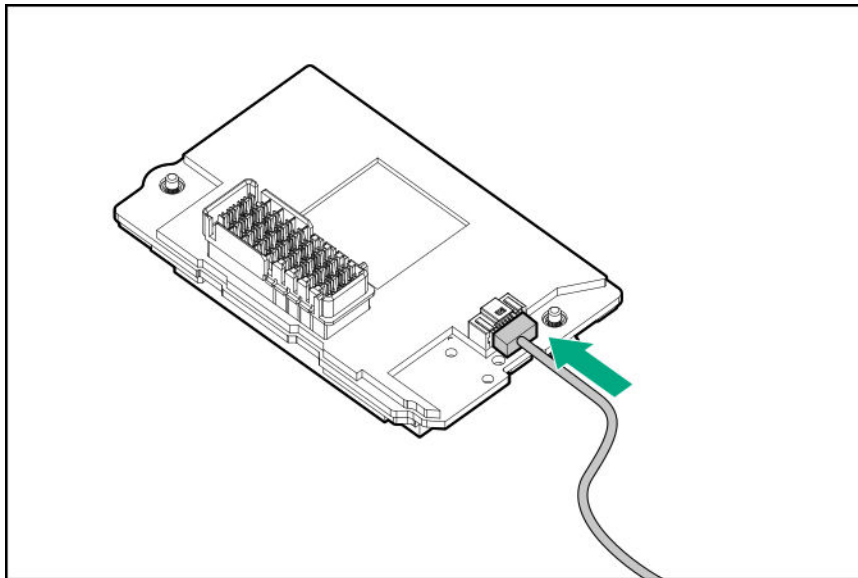
7. If you are using the cable retention clip, install it now (**Installing the cable retention clip** on page 32).

8. Install the mezzanine card.
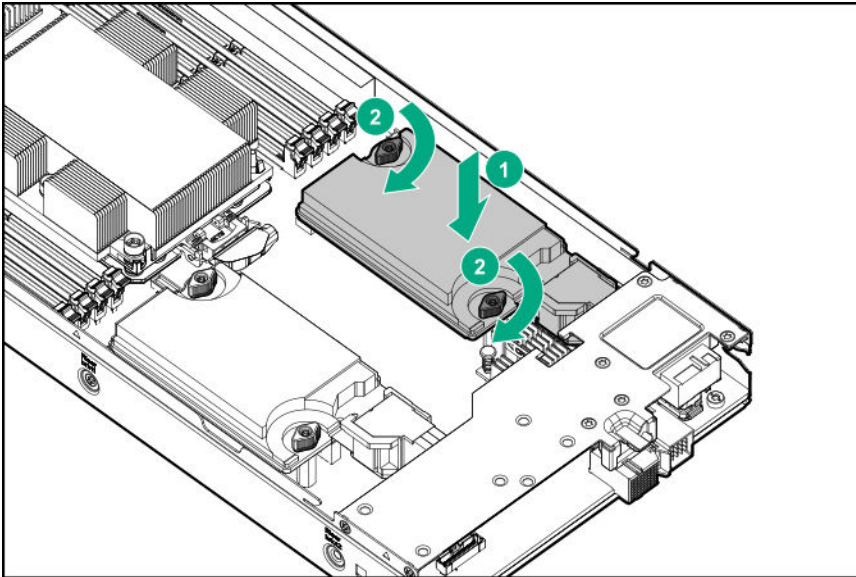
9. Route and connect the cables:

- Single mezzanine card configuration
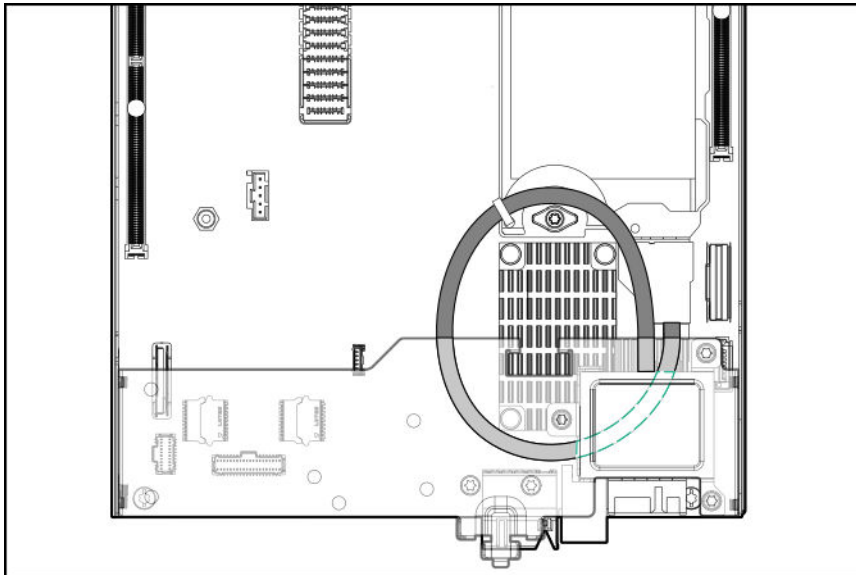
- Dual mezzanine card configuration
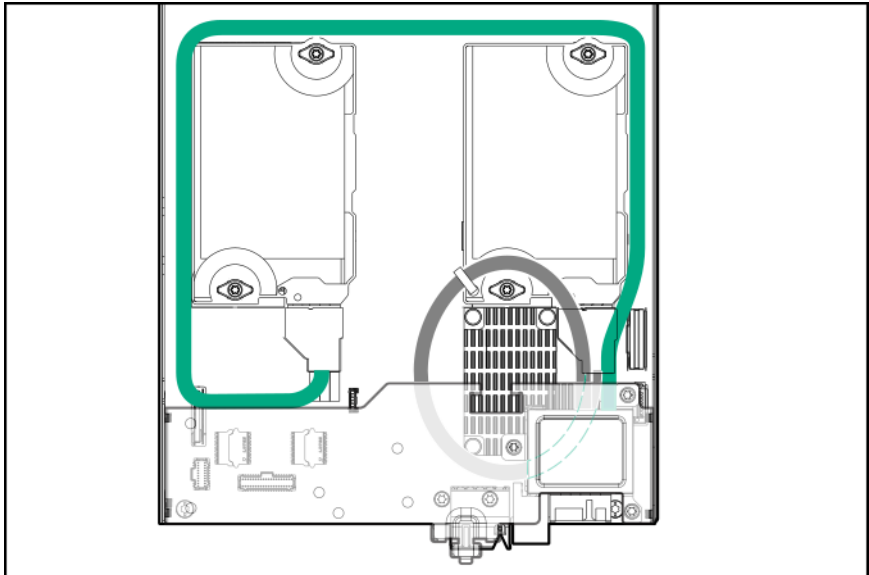
- Single EDR mezzanine with fabric management cable
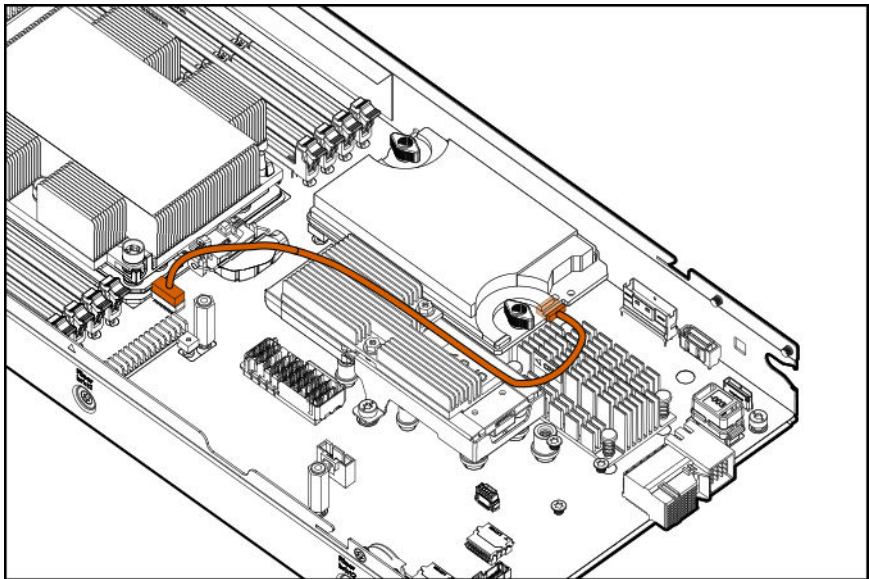
- Dual EDR mezzanines with fabric management cable
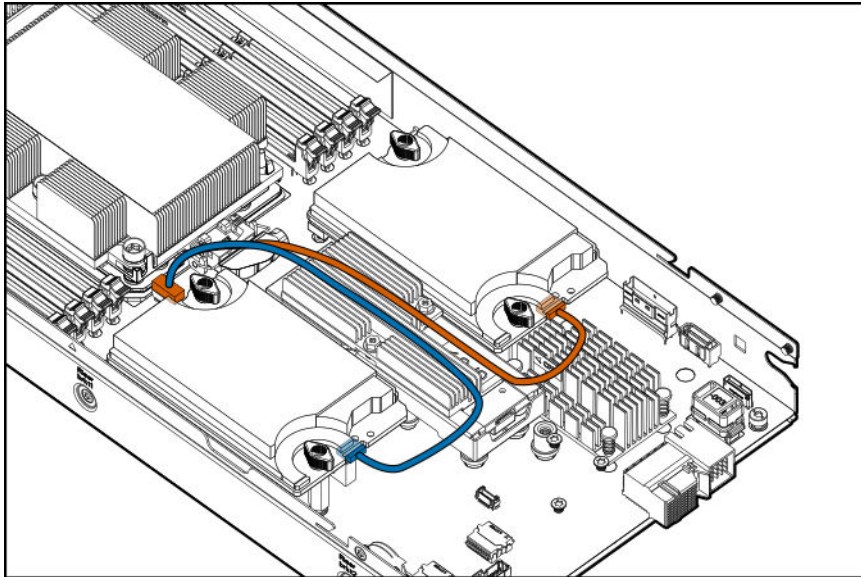
10. Install the rear support bracket.

11. Install the access panel (**Removing the access panel** on page 18).

12. Install the server into the chassis (**Installing the server** on page 14).

13. Press the Power On/Standby button.

    The server exits standby mode and applies full power to the system. The system power LED changes from amber, to flashing green, and then to green.

Installing a PCIe I/O riser card

> ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components that are installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

The server supports the following PCIe I/O riser options:

- HPE XL230k x16 LP PCIe External I/O Riser Kit

- HPE XL230k x8 PCIe Internal-External I/O Riser Kit

- HPE XL230k x8 PCIe Internal I/O Riser Kit

NOTE: When installing the HPE XL230k x16 LP PCIe External I/O Riser Kit or the HPE XL230k x8 PCIe Internal-External I/O Riser Kit, you must also install HPE XL230k External I/O Module in the chassis.

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**).

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Open the front bracket (**Opening the front bracket** on page 18).

6. Remove the air baffle (**Removing the air baffle** on page 21).

7. Remove the rear support bracket (**Removing the rear support bracket** on page 22).

8. Install the PCIe riser assembly onto the rear bracket.

9. Align the arrows on the PCIe riser assembly with the arrows on the server tray, and then install the assembly.
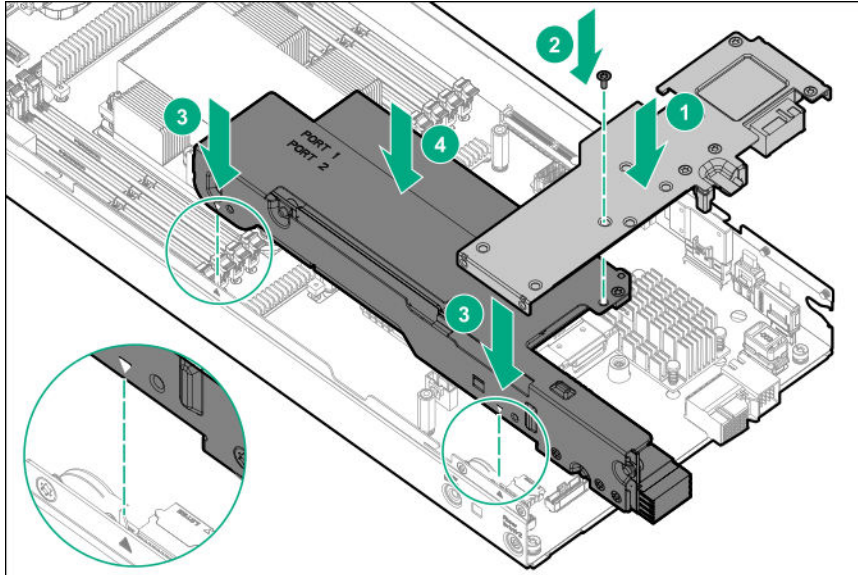
10. Install the screws to secure the PCIe riser assembly to the server tray, and then install the rear support bracket screws.
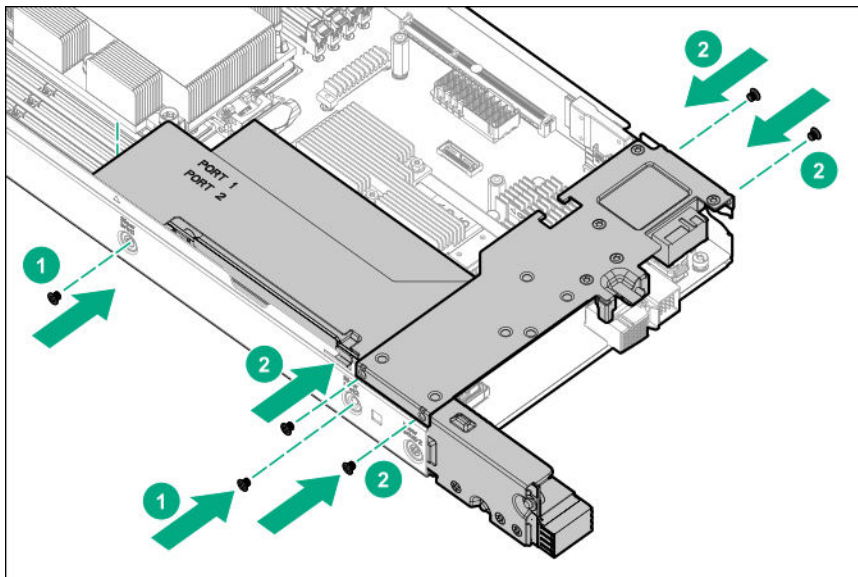
11. Install the air baffle.

12. Close the front bracket.

13. Install the access panel.

14. Install the server into the chassis (**Installing the server** on page 14).

15. Press the Power On/Standby button.

   The server exits standby mode and applies full power to the system. The system power LED changes from amber, to flashing green, and then to green.

16. If applicable, install an I/O module into the chassis (**Installing an I/O riser module** on page 40).

Installing an I/O riser module

I/O modules are specific to each server and are installed in the rear of the chassis.

The server supports the HPE XL230k External I/O Module when one of the following options are installed:

• HPE XL230k x16 LP PCIe External I/O Riser Kit

• HPE XL230k x8 PCIe Internal-External I/O Riser Kit

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**).

⚠ **CAUTION:** To prevent electrical damage, always power down the server associated with the I/O module before installing the I/O module.

⚠ **CAUTION:** Remove the server from the chassis before installing the I/O module. Failure to do so can result in damage to both components. After the I/O module is installed, install the server.

ⓘ **IMPORTANT:** Microsoft Windows does not include native support for certain expansion cards that can be installed in the I/O module. For more information about enabling support, see the Hewlett Packard Enterprise website (**http://www.hpe.com/support/XL230k-io**).

ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components that are installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server associated with the I/O module.

2. Remove the server from the chassis.
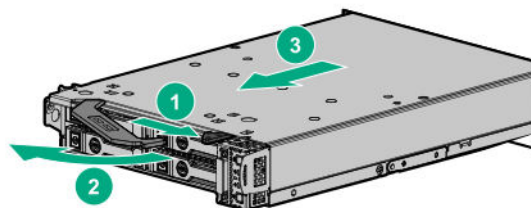
3. At the rear of the chassis, remove the I/O module riser blanks.
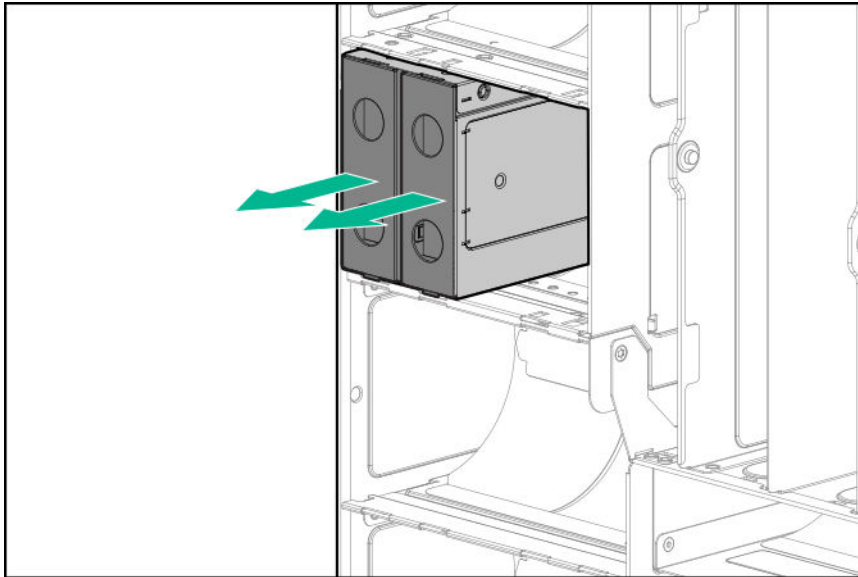
4. Install the I/O module risers into the bays that correspond to the server bays. For more information, see "**Chassis I/O module bay numbering** on page 10."
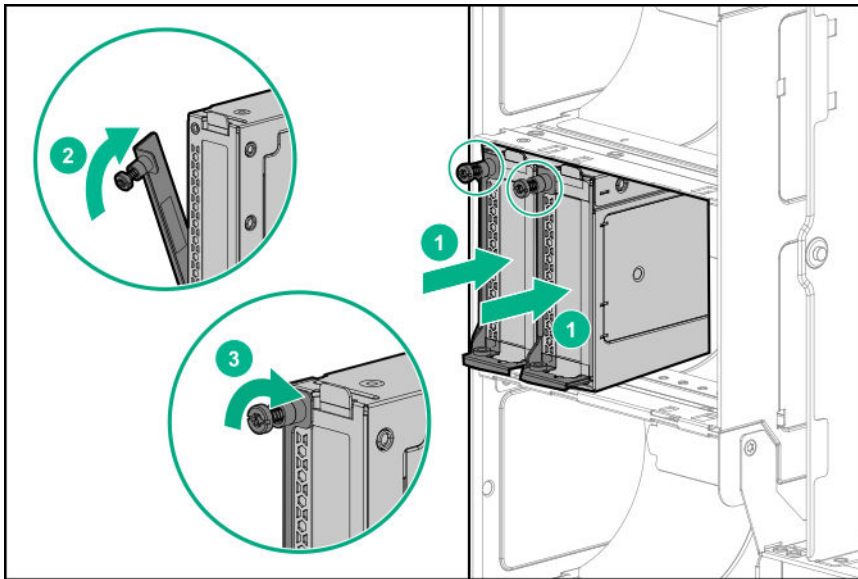
5. If there is a card installed in the I/O module, install the cable for that card.

Installing an expansion board into an I/O module

> ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components that are installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

> ⓘ **IMPORTANT:** Microsoft Windows does not include native support for certain expansion cards that can be installed in the I/O module. For more information about enabling support, see the Hewlett Packard Enterprise website (**http://www.hpe.com/support/XL230k-io**).

Procedure

1. If installed, remove the I/O module from the chassis.
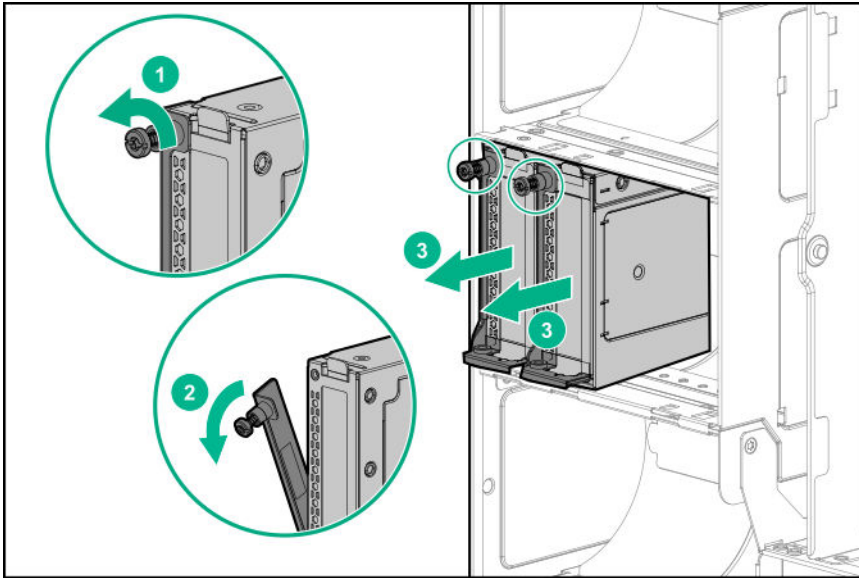
2. Remove the riser cover.
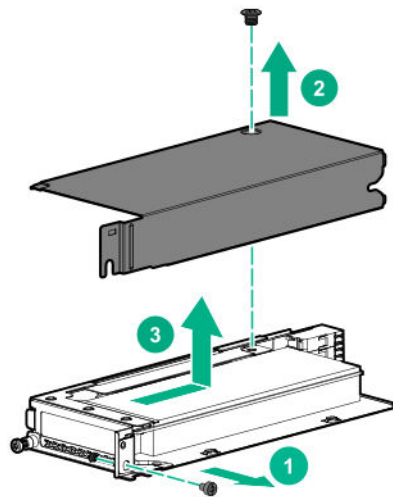
3. Install the expansion board.
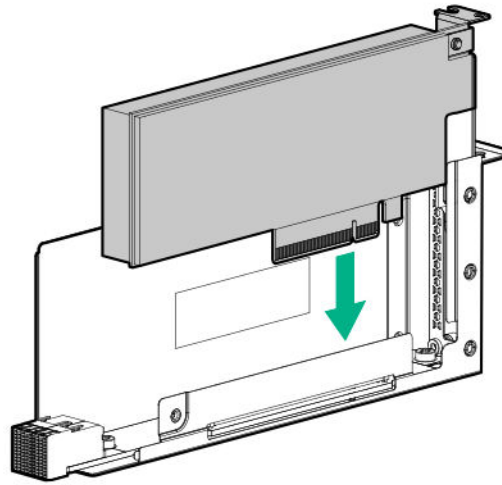
4. Install the riser cover.
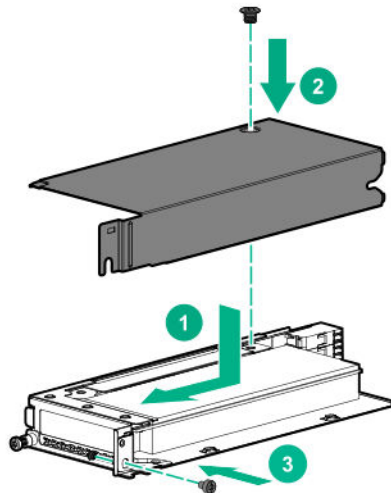
5. Install the riser into the I/O module.
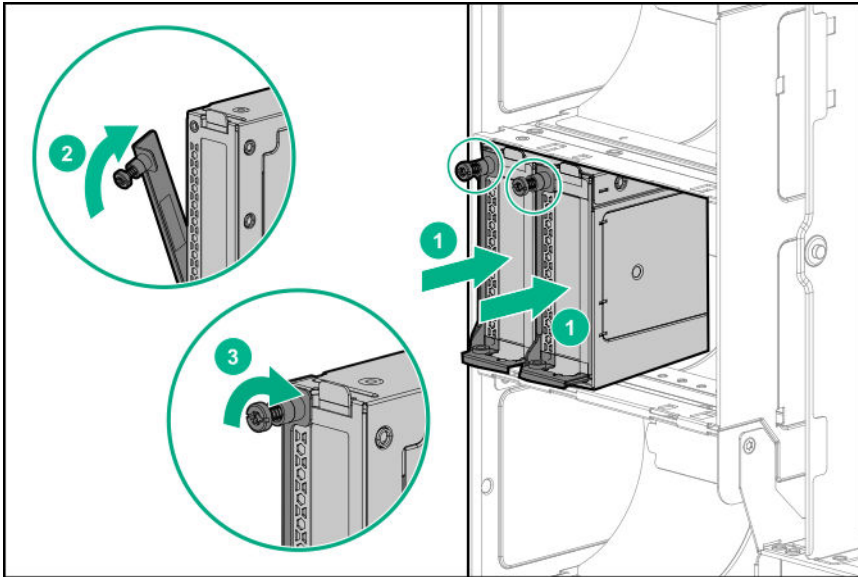
Installing the M.2 SSD enablement option

ⓘ **IMPORTANT:** The left and right sides of the chassis are oriented 180° from each other. Components installed on one side of the chassis must be turned 180° when they are installed on the opposite side.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Open the front bracket (**Opening the front bracket** on page 18).

6. Remove the air baffle (**Removing the air baffle** on page 21).

7. Remove the HPE Smart Storage Battery bracket.
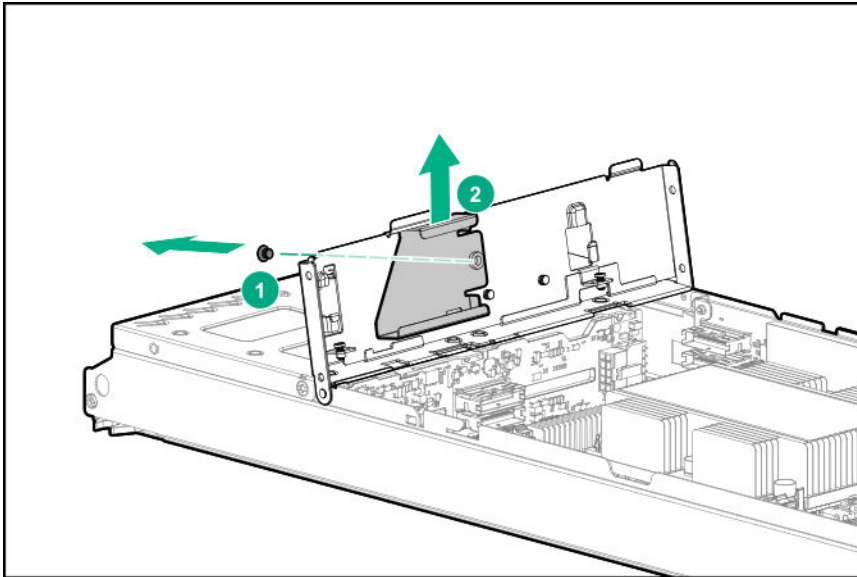
8. Align the M.2 backplane adapter, and then secure it with T-10 flat head screws.
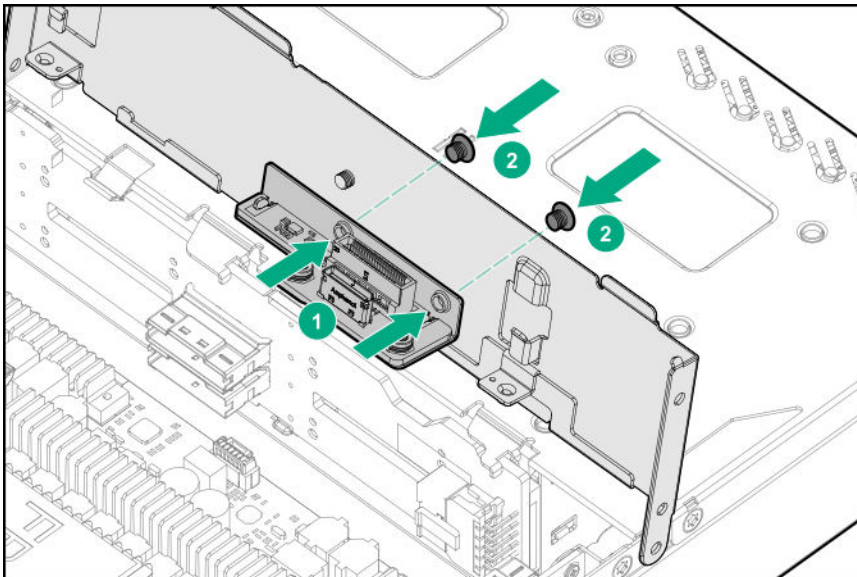
9. Align the guide brackets so that each bracket faces the other, and then secure the brackets with pan head screws.
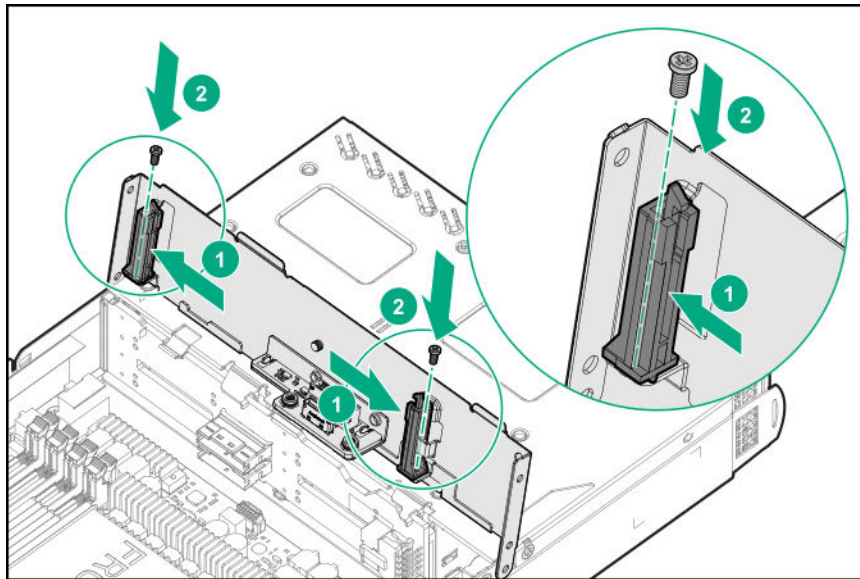
10. Install up to two M.2 SSD drives onto the backplane.
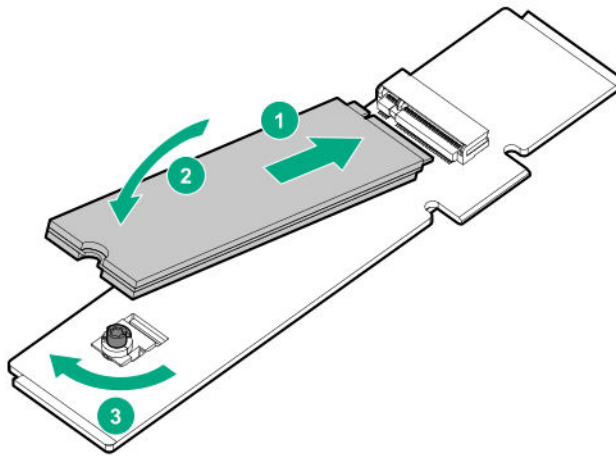
11. Install the M.2 backplane. Be sure that the backplane is fully seated and that the guide brackets are closed.
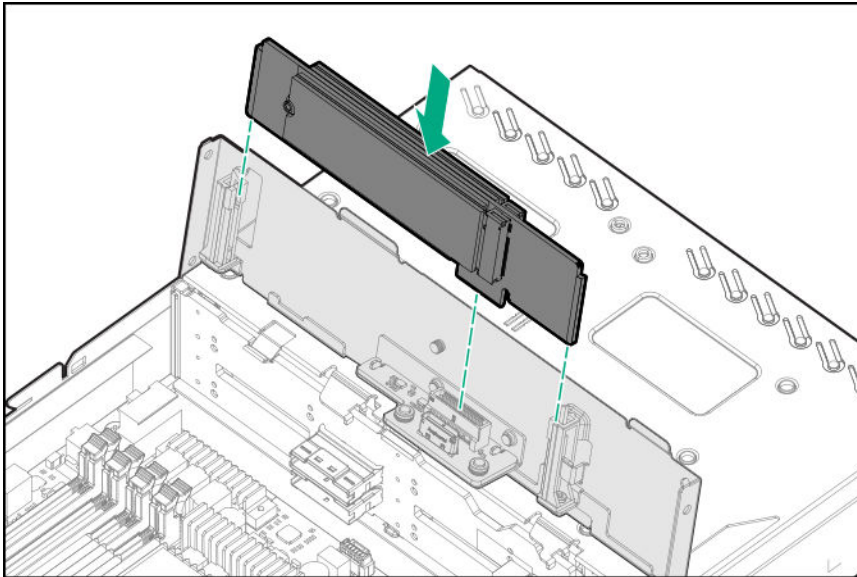
12. Connect the cable to the adapter, and then close the bracket.
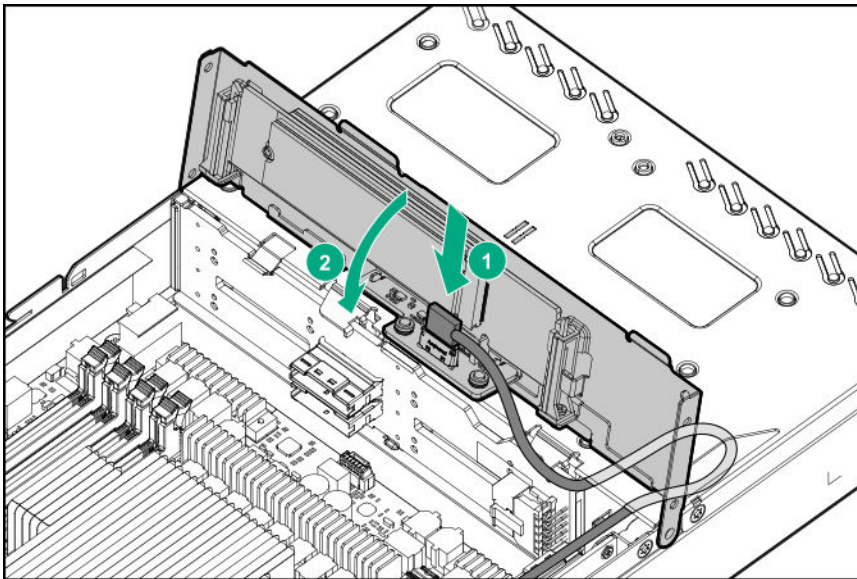
13. Remove the rear support bracket screws.
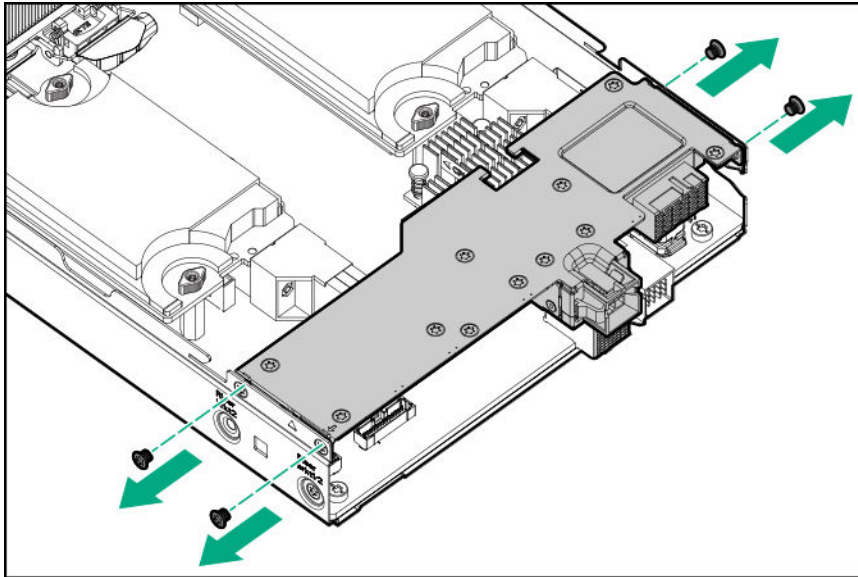
14. Remove the rear support bracket.

   a. If a mezzanine card is installed in slot A, remove the mezzanine card while maintaining the cable connection between the mezzanine card and the rear support bracket.
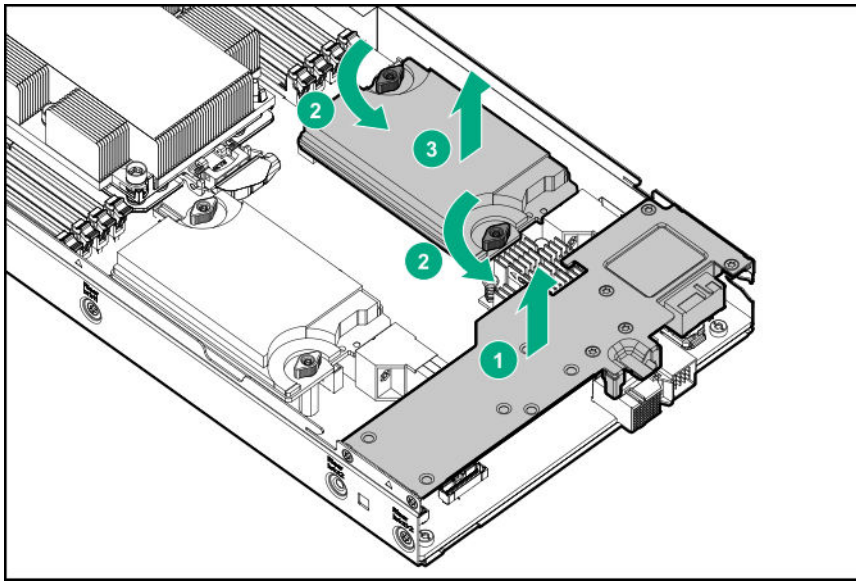
   b. If the PCIe riser is installed, remove the screw securing the rear support bracket to the PCIe riser bracket, and then remove the rear support bracket.
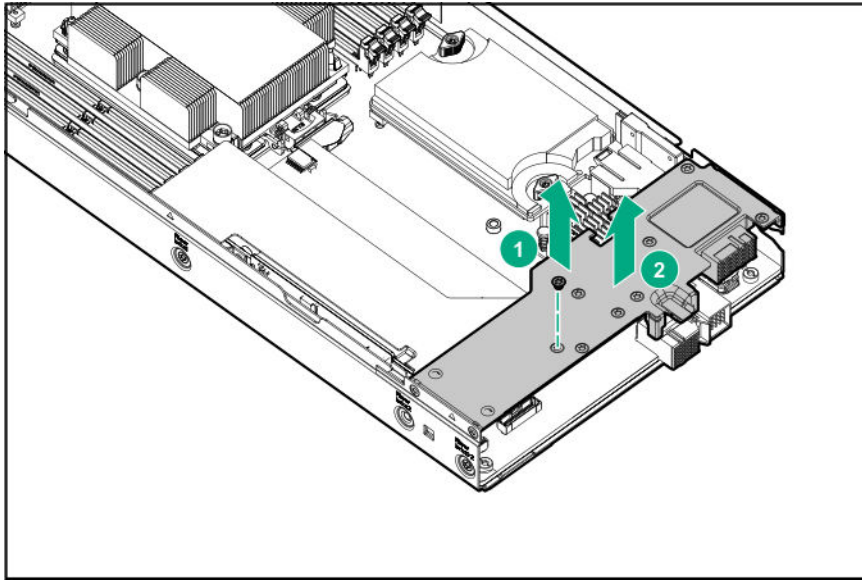
15. Route and connect the cable to the system board.
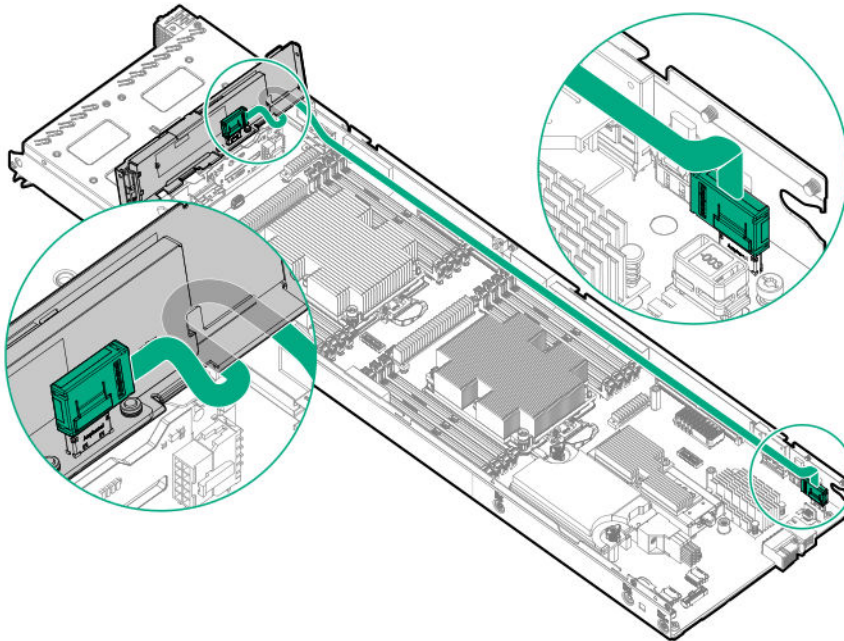
16. Install the mezzanine card.
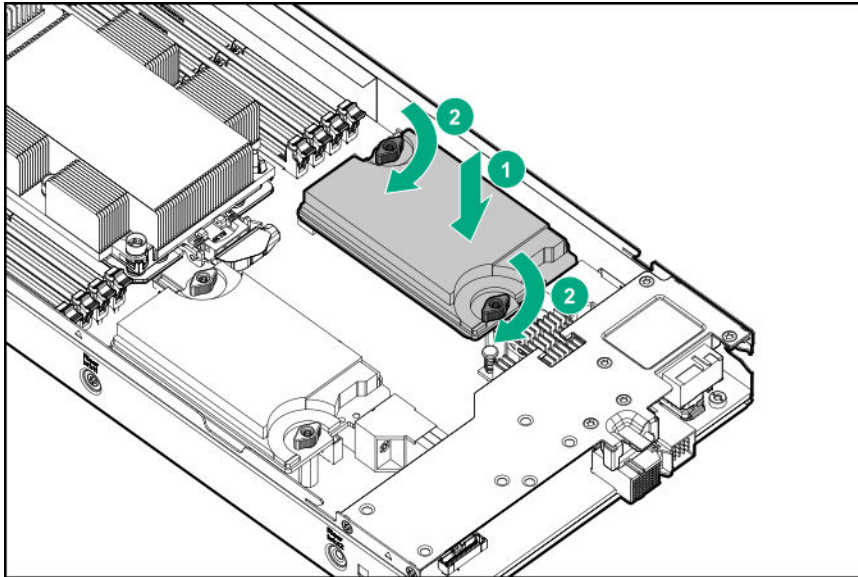
17. Install the rear support bracket.

> ⓘ **IMPORTANT:** To prevent damage to the cable when installing the rear support bracket, route the mezzanine cables as pictured.
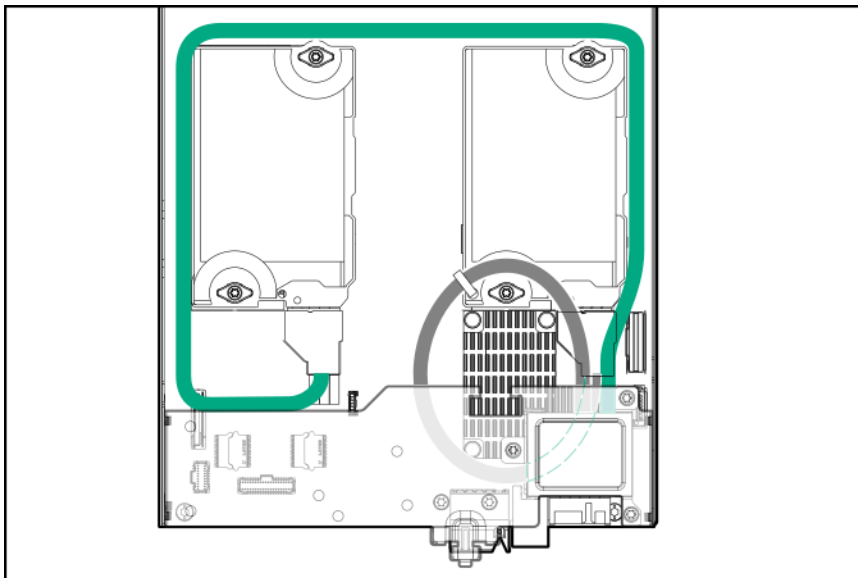
18. Install the air baffle (**Installing the air baffle** on page 22).

19. Close the front bracket.

20. Install the access panel.

21. Install the server into the chassis (**Installing the server** on page 14).

22. Press the Power On/Standby button.

    The server exits standby mode and applies full power to the system. The system power LED changes from amber, to flashing green, and then to green.

Installing an HPE Smart Storage Battery

NOTE: System ROM and firmware messages may display "energy pack" in place of "Smart Storage Battery." Energy pack refers to both HPE Smart Storage Batteries and HPE Smart Storage Hybrid Capacitors.

Procedure

1. Power down the server (**Power down the server** on page 16).

2. Remove the server (**Removing the server** on page 17).

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

4. Remove the access panel (**Removing the access panel** on page 18).

5. Open the front bracket (**Opening the front bracket** on page 18).

6. Remove the air baffle (**Removing the air baffle** on page 21).

7. Remove the HPE Smart Storage Battery bracket.
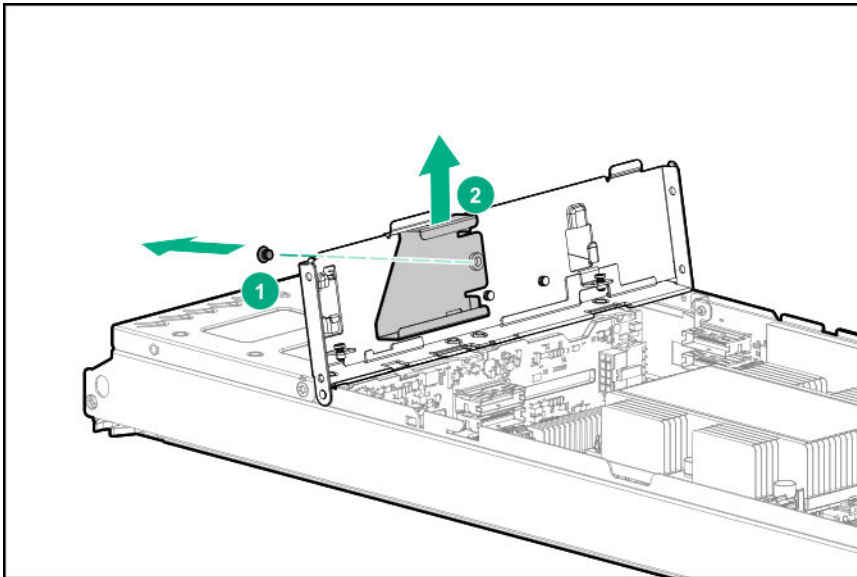
8. Install the HPE Smart Storage Battery:

   a. Slide the HPE Smart Storage Battery into the bracket.

   b. Secure the assembly to the front bracket.
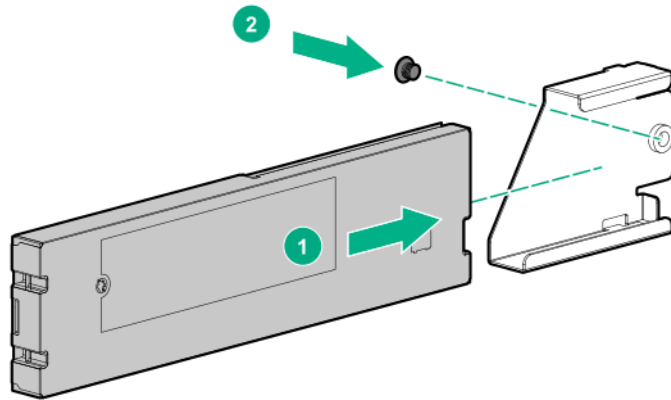
9. Reattach the HPE Smart Storage Battery bracket to the front bracket.

10. Close the front bracket.

11. Route and connect the cable to the controller.
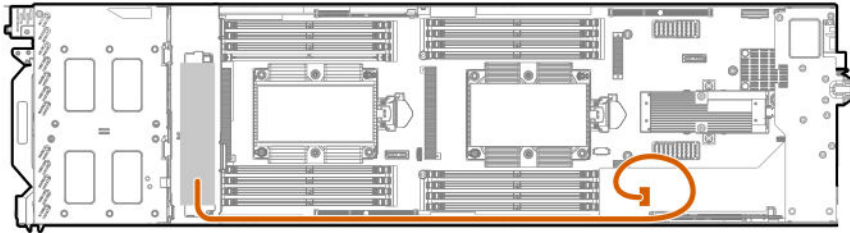
HPE Trusted Platform Module 2.0 Gen10 option

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

   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. 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**). To update the system ROM, follow the instructions on the website.

4. Power down the server.

   a. Shut down the OS as directed by the OS documentation.

   b. To place the server in standby mode, press the Power On/Standby button. When the server enters standby power mode, the system power LED changes to amber.

   c. Disconnect the power cords (rack and tower servers).

5. Do one of the following:

   • Remove the server from the rack, if necessary.

   • Remove the server or server blade from the chassis.

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

7. Remove the access panel.

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

9. Proceed to **Installing the TPM board and cover** on page 54.

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.
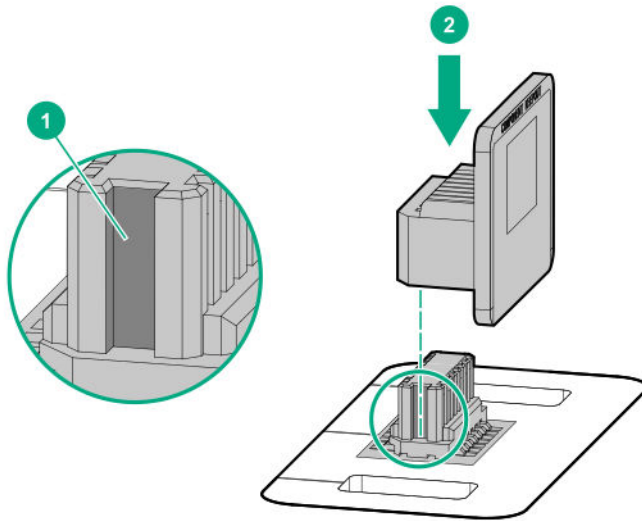
3. Install the TPM cover:

   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.
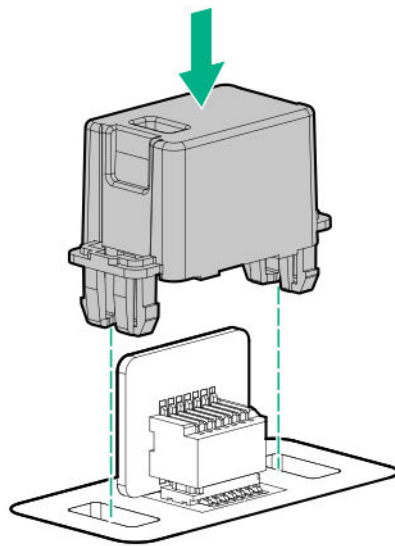
4. Proceed to **Preparing the server for operation** on page 55.

Preparing the server for operation

Procedure

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

2. Install the access panel.

3. Do one of the following:

a. Install the server in the rack, if necessary.

b. Install the server in the enclosure.

4. Power up the server.

a. Connect the power cords (rack and tower servers).

b. Press the Power On/Standby button.

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

Front panel LED board assembly cabling
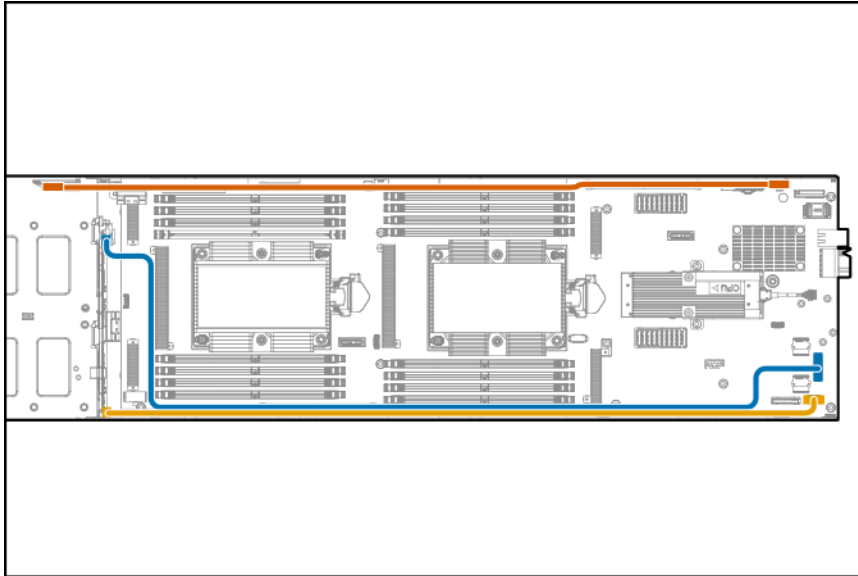
SATA drive cabling

M.2 SSD cabling
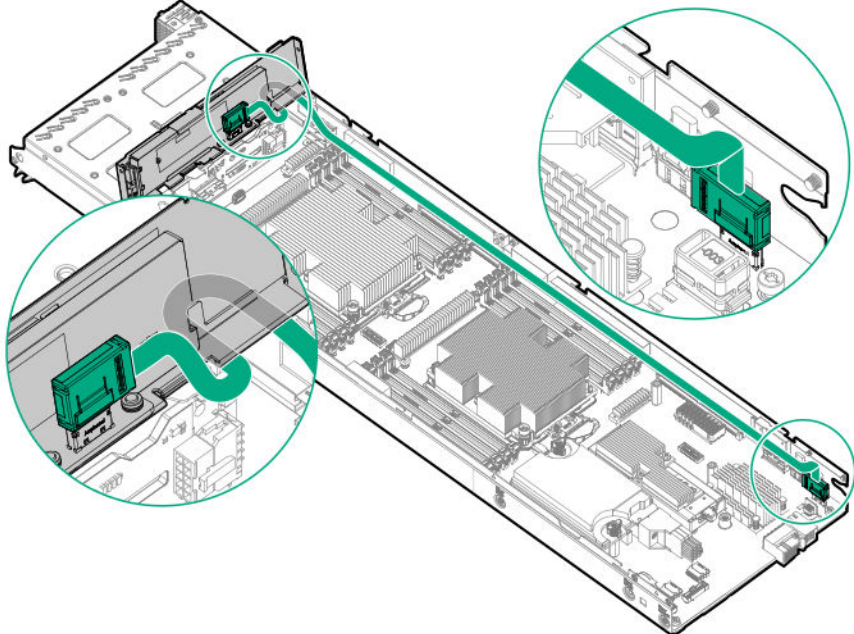
Mezzanine card cabling

Single mezzanine configuration
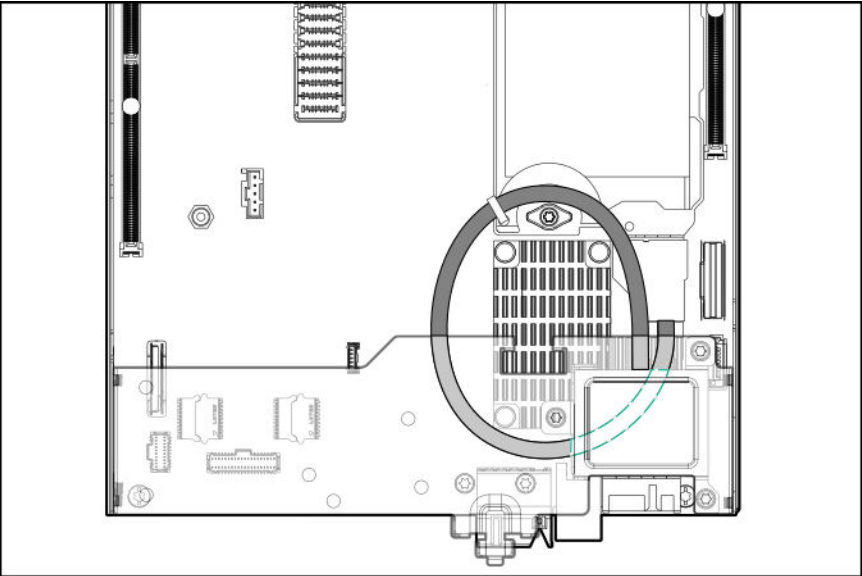
Dual mezzanine configuration

NOTE: Mezzanine B is not supported in a single processor configuration.
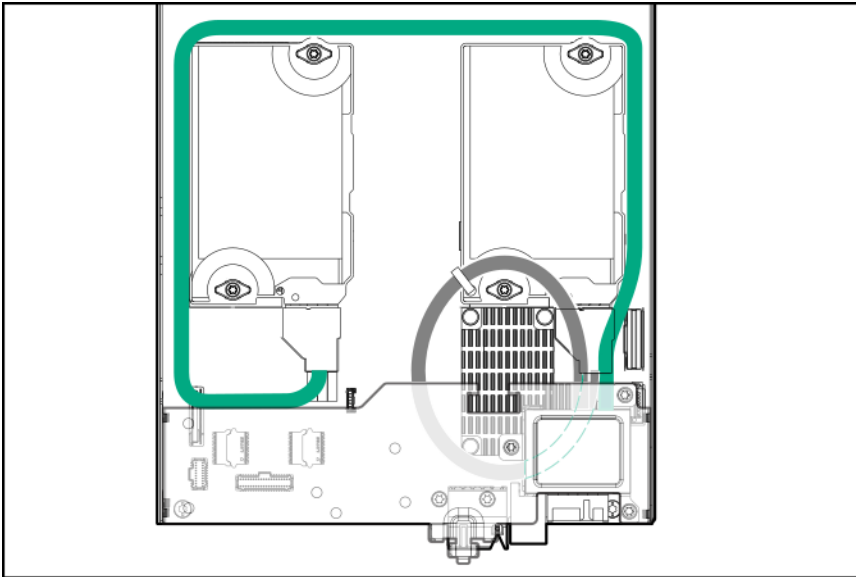
Single EDR mezzanine with fabric management cable
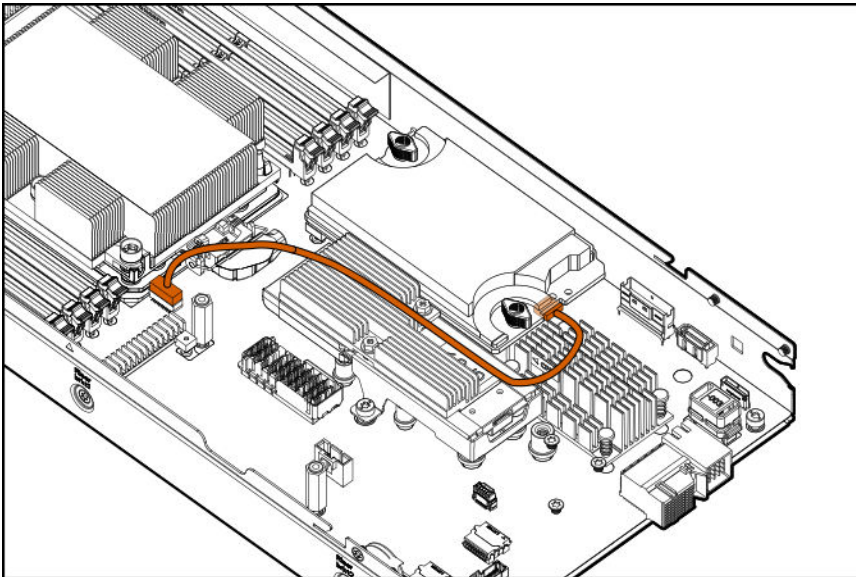
Dual EDR mezzanines with fabric management cable

NOTE: Mezzanine B is not supported in a single processor configuration.
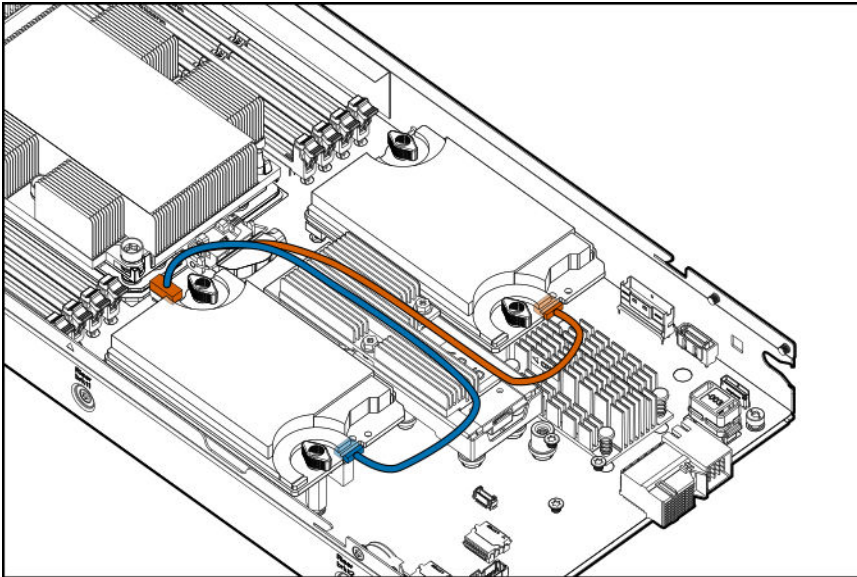
NVMe backplane cabling

NOTE: NVMe is not supported in a single processor configuration.
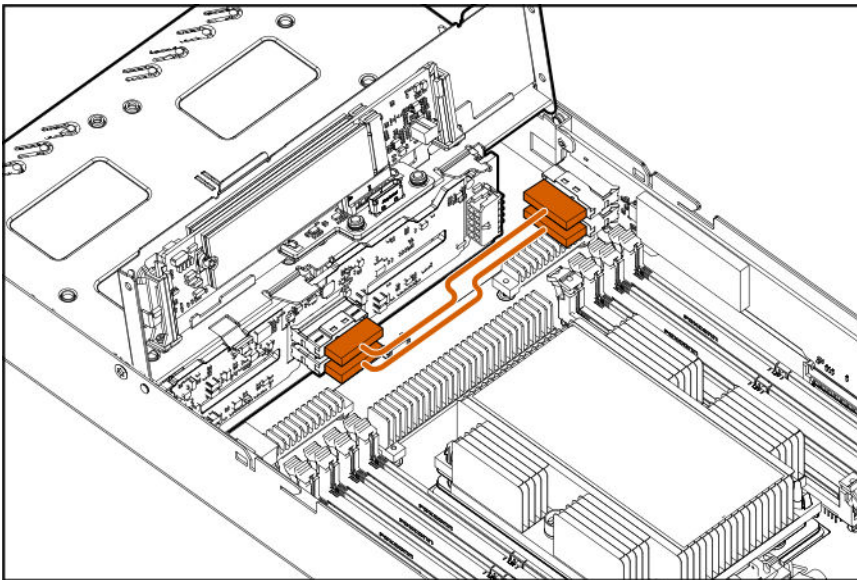
HPE Smart Storage Battery cabling

NOTE: This server supports only the HPE Smart Storage Battery.
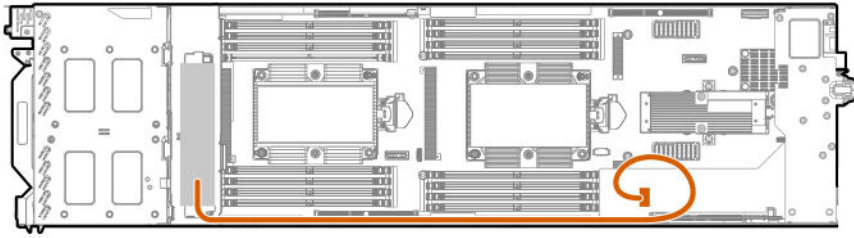
SUV cable connectors

⚠ **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.
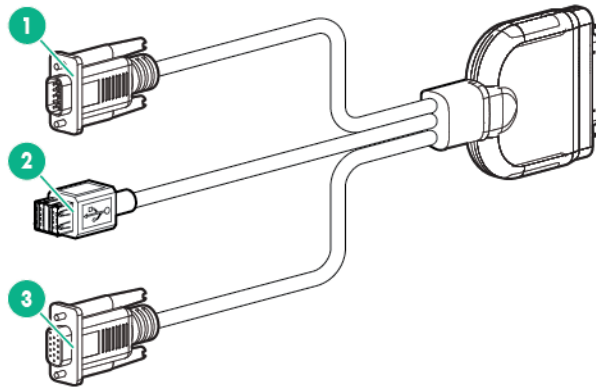
Item	Connector	Description
1	Serial	For trained personnel to connect a null modem serial cable and perform advanced diagnostic procedures
2	USB[1]	For connecting up to two USB 2.0 devices
3	Video	For connecting a video monitor

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

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 63	Online and Offline
HPE iLO 5 on page 64	Online and Offline
HPE Smart Storage Administrator on page 69	Online and Offline
iLO RESTful API on page 66	Online and Offline
Intelligent Provisioning on page 66	Offline
Scripting Toolkit for Windows and Linux on page 67	Online
Service Pack for ProLiant on page 71	Online and Offline
Smart Update Manager on page 71	Online and Offline
UEFI System Utilities on page 67	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 on the Hewlett Packard Enterprise website.

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.

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 on the Hewlett Packard Enterprise website.

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 an iLO Federation group.

When an iLO Federation page loads, 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 the servers in an iLO Federation group.

- Group power control—Manage the power status of the servers in an iLO Federation group.

- Group power capping—Set dynamic power caps for the servers in an iLO Federation group.

- Group firmware update—Update the firmware of the servers in an iLO Federation group.

- Group license installation—Enter a license key to activate iLO licensed features on the servers in an iLO Federation group.

- 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 on the Hewlett Packard Enterprise website.

iLO Service Port

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

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

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

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

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

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

When you use the iLO Service Port:

- Actions are logged in the iLO Event Log.

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

  You can also retrieve the 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 on the Hewlett Packard Enterprise website.

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/ info/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**.

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 and firmware and driver update solution that enables rapid discovery, detailed inventory reporting, and 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**.

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 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.

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

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/info/EIL**.

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 pre-boot 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**.

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 on supported ProLiant servers.

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

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

To download the SPP, see the SPP download page at **https://www.hpe.com/servers/spp/download**.

Smart Update Manager

SUM is an innovative tool for maintaining the firmware, drivers, and system software of HPE ProLiant, HPE Synergy, HPE BladeSystem and HPE Moonshot infrastructures and associated options up to date and secure.

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 mode.

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

- **SUT**: Polls iLO to check for requests from HPE OneView, 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 SUT. 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 SUT.

- **iLO Amplifier Pack**: Displays available updates for servers. Communicates with SUT (or SUT 1.x) to initiate updates using the iLO Redfish interface. SUT reports the status of updates to iLO Amplifier Pack via iLO Restful Interface.

- **HPE OneView**: Displays available updates for servers. Communicates with SUT (or SUT 1.x) to initiate updates, reports the status on the **Firmware** section of the **Server Profile** page of HPE OneView. HPE OneView provides automated compliance reporting in the dashboard.

- **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, iLO Amplifier Pack, and HPE OneView 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 systems 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**).

Battery replacement

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. Power down the server (**Power down the server** on page 16).
2. Remove the server (**Removing the server** on page 17).
3. Place the server on a flat, level work surface.
4. Remove the access panel (**Removing the access panel** on page 18).
5. Open the front bracket (**Opening the front bracket** on page 18).
6. Remove the air baffle (**Removing the air baffle** on page 21).
7. Remove the rear support bracket (**Removing the rear support bracket** on page 22).
8. Identify the battery location (**System board components** on page 11).
9. Remove the battery.
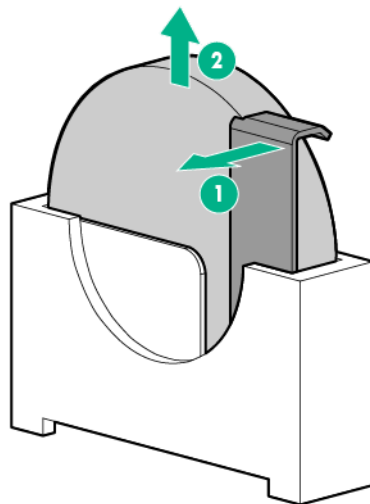
> **(!) IMPORTANT:** Replacing the system board battery resets the system ROM to its default configuration. After replacing the battery, reconfigure the system through UEFI System Utilities (**UEFI System Utilities** on page 67).

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.

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 is 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.

For certain approved hardware configurations, the supported system inlet temperature range is extended.

The approved hardware configurations for this system are listed on the Hewlett Packard Enterprise website (**http://www.hpe.com/servers/ASHRAE**).

Server specifications

Specification	Value
Height	4.33 cm (1.70 in)
Depth	71.12 cm (28.00 in)
Width	19.05 cm (7.50 in)
Maximum weight	6.80 kg (15.00 lb)

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

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 for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

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

Additional warranty information
HPE ProLiant and x86 Servers and Options
> **www.hpe.com/support/ProLiantServers-Warranties**

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

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

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

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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